स्वाध्याय स्वमन्थन स्वावलम्बन

UTTAR PRADESH RAJARSHI TANDON OPEN UNIVERSITY

(Established vide U.P. Govt. Act No. 10, of 1999)

Indira Gandhi National Open University

UP Rajarshi Tandon Open University

UGMM-06

Abstract Algebra

FIRST BLOCK

Elementary Group Theory

Shantipuram (Sector-F), Phaphamau, Allahabad - 211013

UTTAR PRADESH
RAJARSHI TANDON OPEN UNIVERSITY

UGMM – 06
Abstract Algebra

Block

1

ELEMENTARY GROUP THEORY

ABSTRACT ALGEBRA

lgebra is a word that you all are familiar with. You may also know that it is derived from ıe Arabic word 'al-jabr'. Classically, algebra was concerned with obtaining solutions of quations. Then came modern algebra, a term used to describe detailed investigations within lassical algebra. And now we have abstract algebra, a generalisation of modern algebra. In ostract algebra we study algebraic systems that are defined by axioms alone. These axioms ormally evolve from concrete situations. From the Linear Algebra course, you are already ware of one such algebraic system, namely, a vector space. As you know, the axioms that efine a vector space were developed by keeping the Euclidean space R^n in mind.

this course we will deal with three other basic algebraic systems, namely; groups, rings id fields. In the first two blocks of this course we will introduce you to groups and their operties. In the remaining two blocks we discuss rings and fields. To start with, in Unit 1, e give a summary of basic definitions and results on sets, functions and properties of visibility of integers. This will help you to grasp the concepts that come later, more sily.

ou may wonder why you should study this course. As you read this course you will realise at the methods of abstract algebra allow us to deal with several similar algebraic systems just dealing with one representative system. This helps us to be concise and to understand structure of several systems more quickly.

ere are several practical applications of what you will study in this course. Let us start th some applications of group theory. This theory is used by physicists and chemists in ystallography, spectroscopy, general relativity, solid state physics and the modern theory of mentary particles. In fact, using group theory, scientists predicted the existence of the ega minus particle, which was identified in 1964, much after the prediction.

w let us look at some applications of rings and fields. Polynomial rings and matrix rings used in quantum mechanics. Field theory is being used to construct efficient error ecting and correcting codes in the area of data communication. Of course, finite fields are y useful in statistics too.

would like to say a few words about the way we have presented the material. **We have sented this course with the assumption that you have already studied material given in our Elementary Algebra and Linear Algebra courses.** As you know, enever we introduce concepts, we give a lot of concrete examples to help you understand Quite a few examples are taken from linear algebra. We also assume a knowledge of the perties of the basis of a vector space in Block 4 of this course.

s course is divided into four blocks. In each block we give a block introduction, a list of ibols that are used in the block and then, the units of the block. Every unit has exercises rspersed with the text. They are meant to help you check your progress. The solutions or wers to the exercises in a unit are given at the end of the unit. **After you finish dying a unit, please go back to the objectives of the unit (given in the oduction), and see if they have been achieved.**

v a word about our notation. Each unit has been divided into sections. Since the material ie different units is heavily interlinked, we will be doing a lot of cross-referencing. For we will be using **the notation Sec. x.y. to mean Section y of Unit x.**

ing your study of this course we will send you two assignments. They are also meant to eaching aids. Your academic counsellors will assess them and return them to you with able detailed remarks

u may also like to view our video programme, "Groups of Symmetries". In it we have l to concretise some concepts of group theory that you have studied in the first two blocks is course. The notes of this programme are in Block 2.

ou feel like reading more than what this course contains, **you may consult the owing books:**

University Algebra by N.S. Gopalakrishnan (Wiley - Eastern Ltd.)

Topics in Algebra by I.N. Herstein (Vikas)

A Text Book of Modern Abstract Algebra by Shanti Narayan

ie books will be available at your study centre.

NOTATIONS AND SYMBOLS

$\{x \mid x \text{ satisfies } P\}$	the set of all x such that x satisfies the property P.
$\mathbf{N}$	the set of natural numbers
$\mathbf{Z}$ $(\mathbf{Z}^*)$	the set of integers (non-zero integers)
$\mathbf{Q}$ $(\mathbf{Q}^*)$	the set of rational numbers (non-zero rational numbers)
$\mathbf{R}$ $(\mathbf{R}^*)$	the set of real numbers (non-zero real numbers)
$\mathbf{C}$ $(\mathbf{C}^*)$	the set of complex numbers (non-zero complex numbers)
$\mathbf{Z}_n$	the set of integers modulo n.
ϕ	the empty set
$\in$	belongs to
$\notin$	does not belong to
$\subseteq$ $(\subsetneq)$	is contained in (is properly contained in)
$\not\subseteq$	is not contained in
$A \cup B$	union of the sets A and B
$A \cap B$	intersection of the sets A and B
$A \setminus B$	the set of elements of A that are not in B
A^c	complement of A
$A \times B$	Cartesian product of A and B
$\exists$	there exists
$\forall$	for all
$\Rightarrow$	implies
$\Leftrightarrow$	implies and is implied by
iff	if and only if
$[a], \bar{a}$	the equivalence class of a
$f : A \to B$	a function f from a set A into a set B
$f(S)$ $(f^{-1}(S))$	image (inverse image) of the set S under the function f
$f \circ g$	composition of the functions f and g
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a \equiv b \pmod n$	a is congruent to b modulo n
$\pm a$	a or $-a$
x^{-1} or $-x$	inverse of the element x
S_n	symmetric group on n symbols
$(i_1\ i_2\ \ldots\ i_r)$	an r-cycle
$H \leq G$	H is a subgroup of G
$H \not\leq G$	H is not a subgroup of G
$\langle S \rangle$	group generated by the set S
$\langle a \rangle$	cyclic group generated by a
Hx, $H+x$	right coset of the subgroup H
A_n	alternating group on n symbols
Q_8	quaternion group
$Z(G)$	centre of the group G
$o(G)$	order of the group G
$o(x)$	order of the element x
$\therefore$	therefore
i.e.	that is

Greek Alphabets

α	Alpha
β	Beta
γ	Gamma
δ	Delta
ϵ	Epsilon
ζ	Zeta
η	Eta
θ	Theta
ι	Iota
κ	Kappa
λ	Lambda
μ	Mu
ν	Nu
ξ	Xi
o	Omicron
π, Π	Pi (capital pi)
ρ	Rho
σ, Σ	Sigma (capital sigma)
τ	Tau
υ	Upsilon
ϕ	Phi
χ	Chi
ψ	Psi
ω	Omega

BLOCK 1 ELEMENTARY GROUP THEORY

A group is an algebraic system consisting of a set, along with one binary operation defined on it. Groups have been studied by mathematicians for over two hundred years. Throughout the nineteenth century, group theory was a study of permutations and substitutions. It slowly evolved into its present abstract form.

Group theory, in its present form, helps in analysing basic mathematical structures. Mathematicians working in a variety of branches of mathematics can borrow methods and tools from group theory to make progress in their own field. Not only mathematicians, but chemists and physicists also use group theory to analyse the structures of molecules and crystals, or to study the "solid circuits" of sophisticated electronics. It was a group of algebraic transformations, devised by a Dutch physicist Lorentz, which Einstein used for analysing Special Relativity. It is the basics of this interesting and useful theory that we want to share with you in this block.

In the first unit of this block we summarise some of the basic ideas concerning sets, functions and number theory. We also establish certain notation that is used throughout the course.

We start the study of group theory in Unit 2. In this unit you will see what a group is. You will also discover that a lot of familiar sets, like the sets of integers and rational numbers, are groups with respect to addition.

We also introduce you to three groups that you will come across off and on, throughout the course: the group of integers modulo n, permutation groups and the group of complex numbers.

In Unit 3 you will study subsets of groups that are groups in their own right. They are appropriately called subgroups.

In the last unit we discuss a very elementary theorem about groups with a finite number of elements. This result is named after the mathematician Lagrange.

In the next block you will go a little deeper into group theory and you will need everything that you learn in this block. So go through this block carefully. Try every exercise, and go further only after solving it.

UNIT 1 SETS AND FUNCTIONS

Structure

1.1 INTRODUCTION

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

In the last section we discuss some elementary number theory. The primary aim of this section is to assemble a 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.

Objectives

After reading 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 and use the principle of induction;
- use the division algorithm and unique prime factorisation theorem.

1.2 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 being is rich or not.

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

The Greek letter, $\in$, denotes 'belongs to'. It is the abbreviation of the Greek word meaning 'is'

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

There are usually two way of describing a non-empty set:
(1) roster method, and (2) set builder method.

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

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

Convention 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 $1\frac{1}{2}$ 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 $\mathbf{Z}$ = {0, ±1, ±2, ...}.

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, and which no other objects 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 of all x such that x has property P". For example, the set of all integers can also be written as

$\mathbf{Z}$ = {x | x is an integer}.

Some other sets that you may be familiar with are

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

$\mathbf{R}$, the set of real numbers

$\mathbf{C}$, the set of complex numbers = {a+ib | a, b ∈ $\mathbf{R}$}. (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 an element of A. In such a case, that is, when every element of a set B is an element of a set A, we say that B is a **subset of A**, and we write this as $B \subseteq A$.

It is obvious that if A is any set, then every element of A is certainly an element of A. So, for every set A, $A \subset A$.

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

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

'∃' 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 '$\exists\ x \in B$ such that $x \notin A$'.

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

Try the following exercise now.

E 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 set is called their union. Formally, we define the **union of A and B** to be the set of all those elements of S which are in A or in B. We denote the union of A and B by $A \cup B$. 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 $A \cup B = \{1, 2, 4, 6, 7\}$.

Again, if $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8\}$, then $A \cup B = \{1, 2, 3, 4, 6, 8\}$. Observe that 2 and 4 are in both A and B, but when we write $A \cup B$, 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 $A \subseteq B$ you need to show that $x \in A \Rightarrow x \in B$.

E 2) Let A, B, C be subsets of a set S such that $A \subseteq C$ and $B \subseteq C$. Then show that

a) $A \cup B \subseteq C$

b) $A \cup B = B \cup A$

c) $A \cup \phi = A$

Now we 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 $A_1 \cup A_2 \cup \ldots\ldots \cup A_k$ is the set of elements which belong to at least one of these sets. That is,

$A_1 \cup A_2 \cup \ldots\ldots \cup A_k = \{x \in S \mid x \in A_i \text{ for some } i = 1, 2, \ldots\ldots, k\}$.

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

If $\mathcal{P}$ is a collection of subsets of a set S, then we can define the union of all members of $\mathcal{P}$ by

$\bigcup_{A \in \mathcal{P}} A = \{x \in S \mid x \in A \text{ for some } A \in \mathcal{P}\}$.

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

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

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

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

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

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

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

Try this exercise now.

'⇒' denotes 'implies'.

E 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) $A \cap \phi = \phi$

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

$A_1 \cap A_2 \cap \ldots\ldots \cap A_k = \{ x \in S \mid x \in A_i \text{ for each } i = 1,2,\ldots\ldots,k\}$.

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

In general, if $\wp$ is a collection of subsets of a set S, then we can define the intersection of all the members of $\wp$ by

'$\forall$' denotes 'for every'.

$$\bigcap_{A \in \wp} A = \{x \in S \mid x \in A \; \forall \; A \in \wp\}$$

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

E 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) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

E 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) $B \subseteq A \cup B$

e) 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** $A \setminus B$. Similarly, the difference $B \setminus A$ 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,

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

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 $X \setminus A$. 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.

E 6) Why are the following statements true?

a) A and A^c are disjoint, i.e., $A \cap A^c = \phi$.

b) $A \cup A^c = X$, where X is the universal set.

c) $(A^c)^c = A$.

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

1.3 CARTESIAN PRODUCT

An interesting set that can be formed from two given sets is their **Cartesian product**, named after the 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 the 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** $A \times B$, 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 $A = \{1, 2, 3\}$ and $B = \{4, 6\}$, then
$A \times B = \{ (1, 4), (1, 6), (2, 4), (2, 6), (3, 4), (3, 6) \}$.
Also note that
$B \times A = \{ (4, 1), (4, 2), (4, 3), (6, 1), (6, 2), (6, 3) \}$ and $A \times B \neq B \times A$.

Let us make some remarks about the Cartesian product here.

Remark : i) $A \times B = \phi$ iff $A = \phi$ or $B = \phi$.

ii) If A has m elements and B has n elements, then $A \times B$ has mn elements. $B \times A$ also has mn elements. But the elements of $B \times A$ need not be the same as the elements of $A \times B$, 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

$R \times R = \{(a_1, a_2) \mid a_1 \in R, a_2 \in R \}$
$R \times R \times R = \{ (a_1, a_2, a_3) \mid a_i \in R \text{ for } i = 1, 2, 3 \}$, and so on. It is customary to write R^2 for $R \times R$ and R^n for $R \times \ldots\ldots \times R$ (n times).

Now, you know that every point in a plane has two coordinates, x and y. Also, every ordered pair (x,y) of real numbers defines the coordinates of a point in the plane. So, we can say that R^2 represents a plane. In fact, R^2 is the Cartesian product of the x-axis and the y-axis. In the same way R^3 represents three-dimensional space, and R^n represents n-dimensional space, for any $n \geq 1$. Note that R represents a line.

Try the following exercises now.

E 7) If $A = \{2, 5\}$, $B = \{2, 3\}$, find $A \times B$, $B \times A$ and $A \times A$.

E 8) If $A \times B = \{ (7, 2), (7, 3), (7, 4), (2, 2), (2, 3), (2, 4) \}$, determine A and B.

E 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.

1.4 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, a 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 this relation, we write a R b or $(a,b) \in R$. From the latter notation we see that $R \subseteq S \times S$. And this is exactly how we define a relation on a set.

Definition : A relation R on a set S is a subset of $S \times S$.

For example, if N is the set of natural numbers 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 $R \subseteq N \times N$.

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.

E 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 $\mathbb{Z}$ given by 'aRb if 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, R is not 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 subsets of S, i.e., $\wp(S) = \{A \mid A \subseteq S\}$. We call $\wp(S)$ the **power set of S.**

Define the relation R on $\wp(S)$ by

$R = \{(A, B) \mid A, B \in \wp(S) \text{ and } A \subseteq B\}$.

Check whether R is reflexive, symmetric or transitive.

'$\Leftrightarrow$' denotes 'implies and is implied by'.

Solution : Since $A \subseteq A \; \forall A \in \wp(S)$, R is reflexive.
If $A \subseteq B$, B need not be contained in A. (In fact, $A \subseteq B$ and $B \subseteq A \Leftrightarrow A = B$.) Thus, R is not symmetric.
If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C \; \forall A, B, C \in \wp(S)$. Thus, R is transitive.

You may like to try the following exercises now.

E 11) The relation $R \subseteq N \times N$ is defined by $(a,b) \in R$ iff 5 divides $(a - b)$. Is R reflexive? symmetric? transitive?

E 12) Give examples to show why the relation in E 10 is not reflexive, symmetric or transitive.

The relationship in E 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 $\{b \in S \mid aRb\}$ 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 E 11?

This is

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

Similarly,

$[2] = \{n \mid n \in N \text{ and } 5 \text{ divides } n-2\}$
$= \{2, 7, 12, 17, 22,.....\},$

$[3] = \{3, 8, 13, 18, 23,.....\},$

$[4] = \{4, 9, 14, 19, 24,.....\},$

$[5] = \{5, 10, 15, 20, 25,.....\},$

$[6] = \{1, 6, 11, 16, 21,.....\},$

$[7] = \{2; 7, 12, 17, 22,.....\},$

Note that

i) [1] and [6] are not disjoint. In fact, [1] = [6]. Similarly, [2] = [7], and so on.

ii) $N = [1] \cup [2] \cup [3] \cup [4] \cup [5]$, and the sets on the right hand side are mutually disjoint.

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

Theorem 1 : Let R be an equivalence relation on a set S. For $a \in S$, 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 $b \in [b] = [a]$. $\therefore b \in [a]$.

c) Since $[a] \subseteq S \; \forall \; a \in S$, $\bigcup_{a \in S} [a] \subseteq S$ (see E 2).

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

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

Example 3 : Let S be the set of straight lines in $R \times R$. Consider the relation on S given by '$L_1 \; R \; L_2$ iff $L_1 = L_2$ 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).

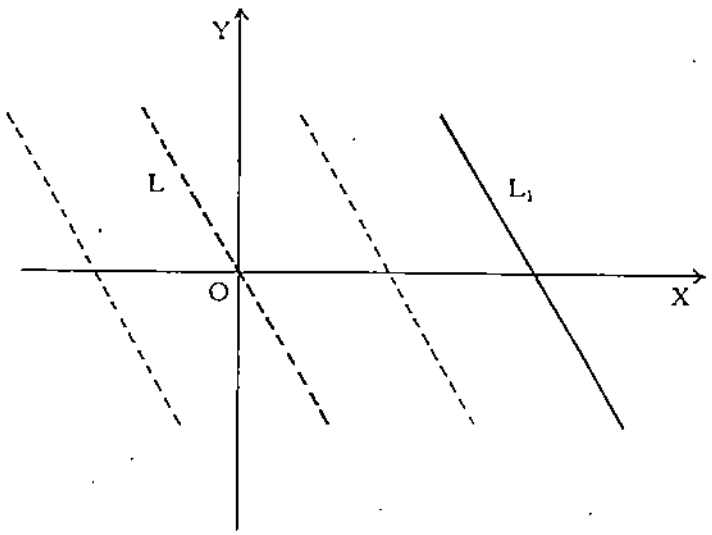


Fig.1 : The equivalence class of L_1

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 lines through (0,0) give distinct equivalence classes into which S is partitioned. Each equivalence class [L] consists of all the lines in the plane that are parallel to L.

Now for a nice exercise!

E 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.

1.5 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 one element of B. This is written as $f : A \to B$. 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 $f(A) = \{f(a) \mid a \in A\}$ 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 $f : A \to B$ 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 $f(x) = x^2$ for each $x \in A$ or $f : A \to B : f(x) = x^2$. We will often use this notation for defining any function.

If we define $g : A \to B$ 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 $f : A \to B$ to be the subset $\{(a, f(a)) \mid a \in A\}$ of $A \times B$.

Now let us look at functions with special properties.

'f is one-one' can also be written as 'f is 1-1'

Definition : A function $f : A \to B$ 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 $f : A \to B$ 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 $f : A \to B$ 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 $\pi_1 : A \times B \to A : \pi_1((a, b)) = a$. π_1 is called the **projection** of $A \times B$ onto A. You can see that the range of π_1 is the whole of A. Therefore, π_1 is onto. Similarly, $\pi_2 : A \times B \to B : \pi_2((a, b)) = b$, the projection of $A \times B$ 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 $I_A : A \to A : I_A(a) = a$ 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 1-1 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 $f : A \to B$ 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 ϕ is assumed to be finite.

Try the following exercises now.

E 14) Let $f : N \to N$ be defined by f(n) = n+5. Prove that f is one-one but not onto.

E 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.

E 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 E 14,

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

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

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 E 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 E 17.

E 17) Prove (b) of Theorem 2.

E 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 $g \circ f$. 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 $f : R \to R$ and $g : R \to R$ 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, $\forall\, x \in R$, $g \circ f(x) = g(f(x)) = f(x) + 1 = x^2 + 1$.

$f : A \to B$ and $g : C \to D$ are equal if $A = C$ and $f(a) = g(a)\ \forall\, a \in A$.

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 $g \circ f \neq f \circ g$. (For example, $g \circ f(1) \neq f \circ g(1)$.)

Example 6: Let $A = \{1, 2, 3\}$, $B = \{p, q, r\}$ and $C = \{x, y\}$. Let $f : A \to B$ be defined by $f(1) = p$, $f(2) = p$, $f(3) = r$. Let $g : B \to C$ 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 $g \circ f : A \to C$ 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.

E 19) In each of the following questions, both f and g are functions from $R \to R$. Define f o g and g o 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 $1 \in R$ 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 exercise on the lines of this theorem.

E 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 $f \circ g(x) = f(g(x)) = g(x) + 3 = (x-3)+3 = x \ \forall\, x \in R$. 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 finding the inverse of a given function is : try to retrieve x from f(x).

For example, let $f : R \to R$ 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, $f \circ g(x) = 3(g(x)) + 5 = 3\left[\frac{(x-5)}{3}\right] + 5 = x \ \forall\, x \in R$.

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

E 21) What is the inverse of $f : R \to R : f(x) = \frac{x}{3}$?

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

Example 7 : Let $f : R \to R$ be the constant function given by $f(x) = 1 \ \forall\, x \in R$. What is the inverse of f ?

Solution : If f has an inverse $g : R \to R$, we have $f \circ g = I_R$, i.e., $\forall\, x \in R$, $f \circ g(x) = x$. Now take $x = 5$. We should have $f \circ g(5) = 5$, i.e., $f(g(5)) = 5$. But $f(g(5)) = 1$, since $f(x) = 1 \ \forall\, x$. 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 $g : B \to A$ and prove that $g = f^{-1}$.

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

Note that, since f is onto, $B = \{f(a) \mid a \in A\}$. Then, we are simply defining $g : B \to A$ 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.

g o f is 1-1 $\Rightarrow$ f is 1-1.

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.

g o f is onto $\Rightarrow$ g is onto.

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 exercise now.

E 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) $f(x) = x^2 \; \forall \; x \in R$.

b) $f(x) = 0 \; \forall \; x \in R$.

c) $f(x) = 11x + 7 \; \forall \; x \in R$.

Let us now discuss some elementary number theory.

1.6 SOME NUMBER THEORY

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

1.6.1 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 $a \leq b \; \forall \; b \in S$. For example, N has a least element, namely, 1. But Z has no least element. In fact, many subsets of Z, like 2Z, $\{-1, -2, -3, \ldots\}$, 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 $S \subseteq N$ 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 $m \in S \; \forall \; m < k$, 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 Theorems 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 equivalent 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 $1^3 + 2^3 + \ldots\ldots\ldots + n^3 = \frac{n^2(n+1)^2}{4}$ for every $n \in N$.

Solution : Let $S_n = 1^3 + \ldots\ldots\ldots + n^3$, and let P(n) be the statement that $S_n = \frac{n^2(n+1)^2}{4}$.

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

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

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

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

$= \frac{(n-1)^2 n^2}{4} + n^3$, 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.

E 23) For $a, b \in R$ and $n \in N$, prove that $(ab)^n = a^n . b^n$.

Let us now look at some factorisation properties of integers.

1.6.2 Divisibility in Z

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

Definition : Let $a, b \in \mathbf{Z}$, $a \neq 0$. Then, we say that **a divides b** if there exists an integer c such that $b = ac$. We write this as $a \mid b$ 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 $a \nmid b$.

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

E 24) Let a, b, c be non-zero integers. Then

a) $a \mid 0, \pm 1 \mid a, \pm a \mid a$.

b) $a \mid b \Rightarrow ac \mid bc$.

c) $a \mid b$ and $b \mid c \Rightarrow a \mid c$.

d) $a \mid b$ and $b \mid a \Leftrightarrow a = \pm b$.

e) $c \mid a$ and $c \mid b \Rightarrow c \mid (ax+by)\ \forall x, y \in \mathbf{Z}$.

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

Theorem 7 (Division Algorithm) : Let $a, b \in \mathbf{Z}$, $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \leq r < b$.

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

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

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

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

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

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

So, P(1) is true.

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

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

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

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 E 24 (a) you know that 1 and –1 are common divisors of a and b, for any $a, b \in \mathbf{Z}$. Thus, a pair of integers do 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 E 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 $m, n \in \mathbf{Z}$.

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

Since $a^2+b^2 > 0$, $a^2+b^2 \in S$, i.e., $S \neq \phi$. But then, by the well-ordering principle, S has a least element, say $d = ma+nb$ for some $m, n \in \mathbf{Z}$. We show that $d = (a, b)$.

Now $d \in S$. Therefore, $d > 0$. So, by the division algorithm we can write

$a = qd + r$, $0 \leq r < d$. Thus,

$r = a - qd = a - q(ma+nb) = (1 - qm)a + (-qn)b$.

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., $d \mid a$. We can similarly show that $d \mid b$. Thus, d is a common divisor of a and b.

Now, let c be an integer such that $c \mid a$ and $c \mid b$.

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

But then $d = ma+nb = ma_1c + nb_1c = (ma_1 + nb_1)c$. Thus, $c \mid d$. 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. of 2 and 10 is $2 = 1.2 + 0.10$, and the g.c.d. of 2 and 3 is $1 = (-1)2 + 1(3)$.

Pairs 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 **coprime**) to each other.

Using Theorem 8, we can say that **a and b are coprime to each other iff there exist $m, n \in \mathbf{Z}$ such that $1 = ma+nb$.**

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

Theorem 9 : If $a,b \in \mathbf{Z}$, such that $(a,b) = 1$ and $b \mid ac$, then $b \mid c$.

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

Now, $b \mid ac$ and $b \mid bc$. $\therefore b \mid (mac+nbc)$ (by E 24(c)). Thus, $b \mid c$.

Let us now discuss prime factorisation.

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 $a \in \mathbf{Z}$ such that $p \nmid a$, then $(p,a) = 1$.

Try the following exercises now.

E 25) If p is a prime and $p \mid ab$, then show that $p \mid a$ or $p \mid b$.

E 26) If p is a prime and $p \mid a_1a_2 \ldots\ldots a_n$, then show that $p \mid a_i$ for some $i = 1, \ldots\ldots, n$.

Now consider the number 50. We can write $50 = 2 \times 5 \times 5$ 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 factorisation theorem says.

Theorem 10 (Unique Prime Factorisation Theorem) : 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 factorisation. 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,

$k+1 = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$, 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 $n = p_1 p_2 \dots p_t = q_1 q_2 \dots q_s$, where

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

If $t = 1$, then $p_1 = q_1 q_2 ..... q_s$. 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 $p_1 \mid q_1q_2.....q_s$ and hence, by E 26, $p_1 \mid q_i$ for some i. By re-ordering $q_1, ..., q_s$ we can assume that $p_1 \mid q_1$. But both p_1 and q_1 are primes. Therefore, $p_1 = q_1$. But then $p_2 ..... p_t = q_2.....q_s$. So, by induction, $t-1 = s-1$ and $p_2, ..., p_t$ are the same as $q_2, ..., q_s$, 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, just as 5 is repeated in the factorisation $50 = 2 \times 5 \times 5$. By collecting the same primes together we can give the following corollary to Theorem 10.

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

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
$P = \{ p_1, p_2, ..., p_n\}$. Consider the natural number
$n = (p_1p_2 .....p_n) + 1$

Now, suppose some $p_i \mid n$. Then $p_i \mid (n - p_1p_2 .....p_n)$, 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 exercise now.

E 27) Prove that $\sqrt{p}$ is irrational for any prime p.

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

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

1.7 SUMMARY

In this unit we have covered the following points.

1) Some properties of sets and subsets.
2) The union, intersection, difference and complements of sets.
3) The Cartesian product of sets.
4) Relations in general, and equivalence relations in particular.
5) The definition of a function, a 1-1 function, an onto function and a bijective function.
6) The composition of functions.
7) The well-ordering principle, which states that every subset of N has a least element.
8) The principle of finite induction, which states that : If P(n) is a statement about some $n \in N$ 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 every $n \in N$.
9) The principle of finite induction can also be stated as :

   If P(n) is a statement about some $n \in N$ such that
   i) P(1) is true, and
   ii) 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 the well-ordering principle is equivalent to the principle of finite induction.
10) Properties of divisibility in Z, like the division algorithm and unique prime factorisation.

1.8 SOLUTIONS/ANSWERS

E 1) a) T b) F c) F d) T.

E 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 $x \in A \Leftrightarrow x \in B \cup A$. $\therefore A \cup B = B \cup A$.

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

E 3) a) You can do it on the lines of E 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 $\phi \subseteq A$.

E 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).

E 5) a) T

b) F. For example, if $A = \{0,1\}$ and $B = \{0,2\}$, then $A \not\subseteq B$, $B \not\subseteq A$ and $A \cap B = \{0\} \neq \phi$.

c) F. In fact, for any set A, $A \subseteq A \cup B$.

d) T.

e) T.

'iff' denotes 'if and only if'.

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

E 7) $A \times B = \{ (2, 2), (2, 3), (5, 2), (5, 3) \}$
$B \times A = \{ (2, 2), (3, 2), (2, 5), (3, 5) \}$
$A \times A = \{ (2, 2), (2, 5), (5, 2), (5, 5) \}$

E 8) The set of the first coordinates is A. $\therefore A = \{7, 2\}$.
The set of the second coordinates is B. $\therefore B = \{2, 3, 4\}$.

E 9) $(x,y) \in (A \cup B) \times C \Leftrightarrow x \in A \cup B$ and $y \in C$
$\Leftrightarrow x \in A$ or $x \in B$ and $y \in C$
$\Leftrightarrow x \in A$ and $y \in C$ or $x \in B$ and $y \in C$
$\Leftrightarrow (x, y) \in A \times C$ or $(x, y) \in B \times C$
$\Leftrightarrow (x, y) \in (A \times C) \cup (B \times C)$.

You can similarly show that
$(A \cap B) \times C = (A \times C) \cap (B \times C)$.

E 10) a) F b) T c) F

E 11) Since 5 divides $(a-a) = 0 \; \forall \; a \in N$, R is reflexive.
If $5 \mid (a-b)$, then $5 \mid (b-a)$. $\therefore$, R is symmetric.
If $5 \mid (a-b)$ and $5 \mid (b-c)$, then $5 \mid \{(a-b) + (b-c)\}$, i.e.,
$5 \mid (a-c)$. $\therefore$, R is transitive.

E 12) 2 R 2 is false.
$(2, 4) \in R$, but $(4,2) \notin R$.
$(2, 4) \in R$, $(4,16) \in R$, but $(2, 16) \notin R$.

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

E 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.

E 15) f is 1-1 (as in E 14).
For any $z \in Z$, $f(z-5) = z$. $\therefore$, f is surjective, and hence, bijective.

E 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.

E 17) $x \in X \Rightarrow f(x) \in f(X) \Rightarrow x \in f^{-1}(f(X))$. $\therefore$, $X \subseteq f^{-1}(f(X))$.

E 18) a) $x \in f^{-1}(S) \Rightarrow f(x) \in S \subseteq T$.
$\Rightarrow f(x) \in T$
$\Rightarrow x \in f^{-1}(T)$.
$\therefore$, $f^{-1}(S) \subseteq f^{-1}(T)$.

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).

E 19) $f \circ g$ and $g \circ f$ are functions from R to R in all the 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) $f \circ g(x) = x^2 = g \circ f(x) \; \forall \; x \in R$.

E 20) Show that $I_A \circ g(b) = g(b)$ and $g \circ I_B(b) = g(b) \; \forall \; b \in B$.

E 21) $g : R \to R : g(x) = 3x$.

E 22) a) f is not 1-1, since $f(1) = f(-1)$.
$\therefore$, f^{-1} doesn't exist.

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

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

E 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 $\forall \; n \in N$.

E 24) a) Since $a.0 = 0$, $a \mid 0$.
$(\pm 1)(\pm a) = a$. $\therefore \pm 1 \mid a$ and $\pm a \mid a$.

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

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

d) $a \mid b \Rightarrow b = ad$, for some $d \in \mathbf{Z}$
$b \mid a \Rightarrow a = be$, for some $e \in \mathbf{Z}$.
$\therefore a = ade \Rightarrow de = 1$, 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 $d, e \in \mathbf{Z}$.
$\therefore$ for any $x, y \in \mathbf{Z}$, $ax+by = c(dx+ey)$.
$\therefore c \mid (ax+by)$.

E 25) Suppose $p \nmid a$. Then $(p,a) = 1$. $\therefore$, by Theorem 9, $p \mid b$.

E 26) Let P(n) be the statement that $p \mid a_1 a_2 \ldots\ldots a_n$
$\Rightarrow p \mid a_i$ for some $i = 1,2, \ldots\ldots, n$.
P(1) is true.
Suppose P (m–1) is true.
Now, let $p \mid a_1 a_2 \ldots\ldots a_m$. Then $p \mid (a_1 \ldots\ldots a_{m-1})a_m$.
By E 25, $p \mid (a_1 a_2 \ldots\ldots a_{m-1})$ 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 $\forall\, n \in \mathbf{N}$.

E 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.

UNIT 2 GROUPS

Structure

2.1 INTRODUCTION

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

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

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

Objectives

After reading this unit, you should be able to

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

2.2 BINARY OPERATIONS

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

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

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

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

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

Let us look at some examples.

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

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

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

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

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

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

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

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

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

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

Try the following exercise now.

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

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

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

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

for all $x, y \in R$.

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

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

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

$= ab * ac$, and

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

Hence, multiplication is distributive over $+$.

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

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

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

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

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

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

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

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

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

Then $e = e * e'$, since e' is an identity element.

$= e'$, since e is an identity element.

That is, $e = e'$. Hence, the identity element is unique.

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

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

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

$= e * b = b$.

That is, $a = b$.

Hence, the inverse of s is unique.

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

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

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

Let us consider the following examples now.

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

Solution : We are looking for some $e \in \mathbf{R}$ such that $a \oplus e = a = e \oplus a \; \forall \; a \in \mathbf{R}$. So we want $e \in \mathbf{R}$ such that $a + e - 1 = a \; \forall \; a \in \mathbf{R}$. Obviously, $e = 1$ will satisfy this. Also, $1 \oplus a = a \; \forall \; a \in \mathbf{R}$. Hence, 1 is the identity element of $\oplus$.

For $x \in \mathbf{R}$, 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 $\mathcal{P}(S)$, the set of all subsets of S. Are $\cup$ and $\cap$ commutative or associative operations on $\mathcal{P}(S)$? Do identity elements and inverses of elements of $\mathcal{P}(S)$ exist with respect to these operations?

Solution : Since $A \cup B = B \cup A$ and $A \cap B = B \cap A \; \forall \; A, B \in \mathcal{P}(S)$, the operations of union and intersection are commutative. E 4 of Unit 1 also says that both operations are associative. You can see that the empty set ϕ and the set S are the identities of the operations of union and intersection, respectively. Since $S \neq \phi$, there is no $B \in \mathcal{P}(S)$ such that $S \cup B = \phi$. In fact, for any $A \in \mathcal{P}(S)$ 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 exercise now.

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

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

Fig. 1 : Arthur Cayley

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

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

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

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

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

From this table we see that, for instance, $1 * 2 = 2$ and $2 * 3 = 2$.
Now $2 * 1 = 3$ and $1 * 2 = 2$. $\therefore 2 * 1 \neq 1 * 2$. That is, * is not commutative.

Again, $(2 * 1) * 3 = 3 * 3 = 1$ and $2 * (1 * 3) = 2$.

$\therefore (2 * 1) * 3 \neq 2 * (1 * 3)$. $\therefore$, * is not associative.

See how much information a mere table can give !

The following exercise will give you some practice in drawing Cayley tables.

E 3) Draw the operation table for the set $\wp(S)$ (ref. Example 2), where

$S = \{0,1\}$ and the operation is $\cap$.

Now consider the following definition.

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

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

We use this definition in the following result.

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

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

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

If n = 1, our definition above gives us

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

Now, assume that

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

Then

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

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

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

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

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

Hence, the result holds for all n.

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

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

2.3 WHAT IS A GROUP ?

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

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

G 1) $*$ is associative,

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

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

$(G, *)$ is called a **semigroup** if $*$ satisfies the property G1. Thus, every group is a semigroup.

We will now give some examples of groups.

Example 3 : Show that $(\mathbf{Z}, +)$ is a group, but $(\mathbf{Z}, .)$ is not.

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

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

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

The following exercise gives you two more examples of groups.

E 4) Show that $(\mathbf{Q}, +)$ and $(\mathbf{R}, +)$ are groups.

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

G 1') $*$ is associative.

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

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

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

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

In fact, these axioms are also equivalent to

G 1") $*$ is associative.

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

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

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

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

To prove this theorem, we need the following result.

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

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

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

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

Now we will use this lemma to prove Theorem 3.

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

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

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

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

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

That is, G2 also holds.

Thus, $(G, *)$ satisfies G1, G2 and G3.

Now consider some more examples of groups.

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

Solution : The table of the operation is

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	1	1	-1

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

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

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

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

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

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

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

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

Now let us look at an example of a non-commutative (or non-abelian) group. Before doing this example recall that an $m \times n$ 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 2×2 matrices with non-zero determinant. That is,

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

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

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

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

Show that (G, ·) is a group.

Solution : First we show that . is a binary operation, that is, $A, P \in G \Rightarrow A.P \in G$.
Now,
det (A.P) = det A. det P ≠ 0, since det A ≠ 0, det P ≠ 0.
Hence, A.P ∈ G for all A, P in G.

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

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

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

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

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

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

we see that this group is not commutative.

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

And now another example of an abelian group.

Example 6 : Consider the set of all translations of R^2,

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

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

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

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

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

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

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

b) $(R^*, .)$ is a finite abelian group.

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

d) $(Q^*, .)$, $(R^*, .)$ and $(Z^*, .)$ are semigroups.

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

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

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

2.4 PROPERTIES OF GROUPS

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

Convention : Henceforth, for convenience, we will denote a group $(G,*)$ by G, if there is no danger of confusion. We will also denote $a * b$ by **ab**, for $a, b \in G$, 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, $a\, a^{-1} = a^{-1} a = e$ also. Thus, by Theorem 1 (b), $(a^{-1})^{-1} = a$.

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

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

$= aa^{-1}$

$= e$

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

Thus, by uniqueness of the inverse we get $(ab)^{-1} = b^{-1} a^{-1}$.
Note that, for a group G, $(ab)^{-1} = a^{-1} b^{-1}$ $\forall$ $a, b \in G$ only if G 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 E 7).

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

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

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

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

$\Rightarrow b = c$.

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

E 7) Prove (b) of Theorem 5.

Now use Theorem 5 to solve the following exercise.

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

We now prove another property of groups.

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

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

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

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

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

Now we will illustrate the property given in Theorem 6.

Example 7 : Consider $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in $GL_2(R)$ (see Example 5).

Find the solution of $AX = B$.

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

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

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

In the next example we consider an important group.

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

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

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

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

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

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

For A, B in $(\mathcal{P}(S), \Delta)$ 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 $\mathcal{P}(S)$.

Try the following exercise now.

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

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

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

i) $a^0 = e$.

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

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

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

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

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

Theorem 7 : Let G be a group. For $a \in G$ and $m, n \in \mathbb{Z}$,
a) $(a^n)^{-1} = a^{-n} = (a^{-1})^n$, b) $a^m . a^n = a^{m+n}$, c) $(a^m)^n = a^{mn}$.

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

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

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

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

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

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

Case 2 ($m < 0$ and $n < 0$) : Then $(-m) > 0$ and $(-n) > 0$. Thus, by Case 1, $a^{-n} . a^{-m} = a^{-(n+m)} = a^{-(m+n)}$. 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 sides on the left by $a^m = (a^{-m})^{-1}$, we get $a^{m+n} = a^m . a^n$.

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

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

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

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

We will now study three important groups.

2.5 THREE GROUPS

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

2.5.1 Integers Modulo n

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

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

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

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

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

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

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

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

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

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

Thus, + is a binary operation on Z_n.

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

To understand addition in Z_n, try the following exercise.

E 11) Fill up the following operation table for + on Z_4.

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

Now, let us show that $(Z_n, +)$ is a commutative group.

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

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

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

i.e., addition is associative in Z_n.

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

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

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

The properties (i) to (iv) show that $(Z_n, +)$ is an abelian group.

Try the following exercise now.

E 12) Describe the partition of Z determined by the relation 'congruence modulo 5'.

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

Z_n also has a multiplicative identity, namely, $\bar{1}$.

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

But, suppose we consider the non-zero elements of Z_n, that is, $(Z_n^*, .)$. Is this a group? For example $Z_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is not a group because . is not even a binary operation on Z_4^*, since $\bar{2} \cdot \bar{2} = \bar{0} \notin Z_4^*$. But $(Z_p^*, .)$ is an abelian group for any prime p.

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

Let us now discuss the symmetric group.

2.5.2 The Symmetric Group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Try this exercise now.

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

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

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

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

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

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

$f \in S_n$ 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 in S_5.

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

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

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

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

since 1, 3 and 4 are left fixed.

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

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

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

a) $(1\ 2)$

b) $(1\ 3\ 2)$

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

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

2.5.3 Complex Numbers

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

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

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

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

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

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

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

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

Moreover,

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

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

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

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

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

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

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

$$= (1, 0)$$

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

Thus, $(C, +)$ is a group and $(C^*, .)$ 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.

2.6 SUMMARY

In this unit we have

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

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

2.7 SOLUTIONS/ANSWERS

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

Therefore, $\oplus$ is commutative.

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

Therefore, $\oplus$ is associative.

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

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

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

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

Suppose e is the identity element for $*$.

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

Similarly, Δ has no identity element.

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

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

So, the table is

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

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

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

(b) $\mathbf{R}^*$ is an infinite abelian group.

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

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

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

Therefore, G3' holds.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E 11)

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

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

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

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

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

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

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

E 13) The operation table for . on Z_5^* is

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

It shows that . is an associative and commutative binary operation on Z_5^*, $\bar{1}$ is the multiplicative identity and every element has an inverse.

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

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

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

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

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

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

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

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

just interchanging the rows.

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

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

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

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

On the other hand,

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

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

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

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

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

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

$$\begin{aligned} x + iy &= (x, 0) + (0, 1)\,(y, 0) \\ &= (x, 0) + (0, y) \\ &= (x, y), \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

Let us now see another way of representing complex numbers.

Geometric Representation of Complex Numbers

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

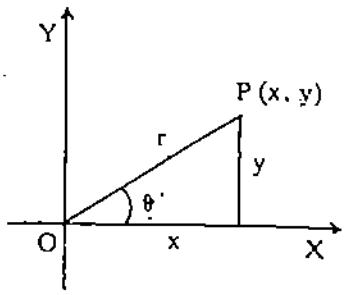


Fig. 3 : Geometric representation of x + iy

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

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

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

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

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

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

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

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

UNIT 3 SUBGROUPS

Structure

3.1 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.

Objectives

After reading 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 a subgroup;
- describe the structure and properties of cyclic groups.

3.2 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 identity element in (G,*) ? Let us see. If h is the identity of (H,*), then, for any $a \in H$, $h * a = a * h = a$. 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.

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

E 1 and the discussion before it allows us to make the following remark.

Remark 1: $(H,*)$ is a subgroup of $(G, *)$ if and only if

i) $e \in H$,

ii) $a, b \in H \Rightarrow a * b \in H$,

iii) $a \in H \Rightarrow a^{-1} \in H$.

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

Remark 2 : If $(H,*)$ is a subgroup of $(G,*)$, **we shall just say that H is a subgroup of G**, provided that there is no confusion about the binary operations. We will also denote this fact by $H \leq G$.

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

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

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

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

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

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 subgroup.

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 $(\mathbb{C}^*, .)$. Show that

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

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

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

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

Example 2: Consider $G = M_{2\times 3}(\mathbb{C})$, the set of all 2×3 matrices over $\mathbb{C}$. Check that $(G,+)$ is an abelian group. Show that

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

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 a binary operation on G. $O = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is the additive identity and

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

Since, $a + b = b + a\ \forall\ a, b \in \mathbb{C}$, + is also abelian.

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

$H \leq (G,+) \Leftrightarrow$
$H \neq \phi$ and
$a - b \in H \; \forall a, b \in H$.

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

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

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

$\therefore \; S \leq G.$

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

Solution : The 3×3 identity matrix is in $SL_3(R)$. Therefore, $SL_3(R) \neq \phi$.
Now, for $A, B \in SL_3(R)$,

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

$\therefore \; AB^{-1} \in SL_3(R)$
$\therefore \; SL_3(R) \leq GL_3(R)$.
Try the following exercise now.

E 2) Show that for any group G, {e} and 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 mZ, where $m \in N$ and $mZ = \{ mt \mid t \in Z\} = \{ 0, \pm m, \pm 2m, \pm 3m, \ldots\ldots\}$.

Solution : We will first show that mZ 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, $0 \in mZ$. Therefore, $mZ \neq \phi$. Also, for $mr, ms \in mZ$, $mr - ms = m(r-s) \in mZ$. Therefore, mZ 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 $S = \{ i \mid i > 0, i \in H\}$.

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. 1.6.1) S has a least elemer', say s. That is, s is the least positive integer that belongs to H.

Now $sZ \subseteq H$. Why ? Well, consider any element $st \in sZ$.
If $t = 0$, then $st = 0 \in H$.
If $t > 0$, then $st = s + s + \ldots\ldots + s$ (t times) $\in H$.
If $t < 0$, then $st = (-s) + (-s) + \ldots + (-s)$ ($-t$ times) $\in H$.

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

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

So we have proved that $H = sZ$.

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

If $z = r(\cos\theta + i \sin\theta)$ is an nth root of 1, then $z^n = 1$.

Thus, by De Moivre's theorem,

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

$\cos(0) + i \sin(0) = r^n (\cos n\theta + i \sin n\theta)$. ..... (1)

Equating the modulus of both the sides of (1), we get $r^n = 1$, i.e., $r = 1$.

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

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

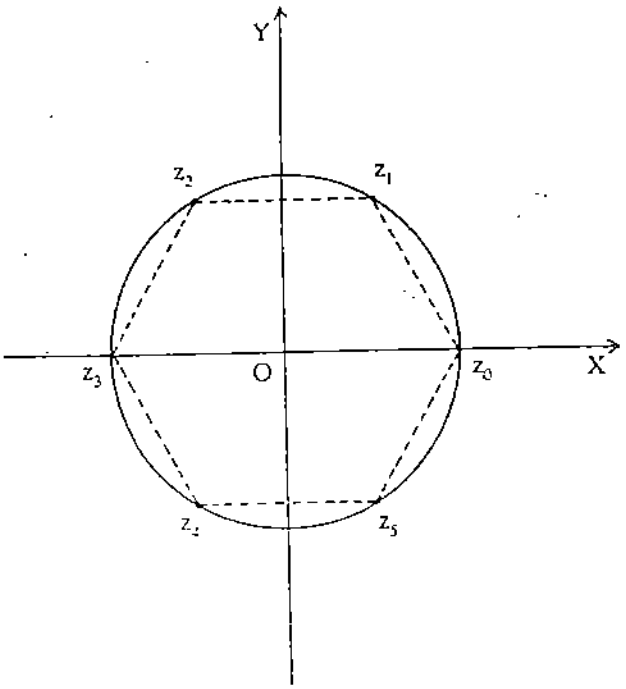


Fig. 1: 6th roots of unity

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

ω is the Greek letter omega.

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

E 3) If $n > 1$ and $\omega = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, then show that

$1 + \omega + \omega^2 + \omega^3 + \ldots\ldots + \omega^{n-1} = 0$.

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

Example 5 : Show that $U_n \leq (C^*, .)$.

Solution : Clearly, $U_n \neq \phi$. Now, let $\omega^i, \omega^j \in U_n$.

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

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

Note that **U_n is a finite 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 introduce you to a subgroup that you will use off and on.

Definition : The **centre of a group** 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 those 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,

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

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

E 4) Show that $Z(S_3) = \{I\}$.
(**Hint :** Write the operation table for S_3.)

Let us now discuss some properties of subgroups.

3.3 PROPERTIES OF SUBGROUPS

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

Theorem 3 : Let G be a group, H be a subgroup of G and K be a subgroup of H. Then K is a subgroup of G.

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

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

Example 6: In Example 4 we have seen that any subgroup of Z is of the form mZ for some $m \in N$. Let mZ and kZ be two subgroups of Z. Show that mZ is a subgroup of kZ iff $k \mid m$.

Solution : We need to show that $mZ \subseteq kZ \Leftrightarrow k \mid m$. Now $mZ \subseteq kZ \Rightarrow m \in mZ \subseteq kZ$
$\Rightarrow m \in kZ \Rightarrow m = kr$ for some $r \in Z \Rightarrow k \mid m$.

Conversely, suppose $k \mid m$.

Then, m = kr for some r ∈ Z. Now consider any n ∈ mZ, and let t ∈ Z such that n = mt.
Then n = mt = (kr) t = k(rt) ∈ kZ .
Hence, mZ ⊆ kZ.
Thus, mZ ≤ kZ iff k | m.

Now, you may like to try the next exercise.

E 5) Which subgroups of Z is 9Z 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 ∩ K is also a subgroup of G.

Proof : Since e ∈ H and e ∈ K, where e is the identity of G, e ∈ H ∩ K.
Thus, H ∩ K ≠ ϕ.
Now, let a, b ∈ H ∩ K. By Theorem 1 , it is enough to show that $ab^{-1} \in H \cap K$. Now, since a, b ∈ H, $ab^{-1} \in H$. Similarly, since a, b ∈ K, $ab^{-1} \in K$. Thus, $ab^{-1} \in H \cap K$.
Hence, H ∩ 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 $(H_i)_{i \in I}$ is a family of subgroups of a group G, then $\bigcap_{i \in I} H_i$ 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 2Z and 3Z of Z. Let S = 2Z ∪ 3Z. Now, 3 ∈ 3Z ⊆ S, 2 ∈ 2Z ⊆ S, but 3 – 2 = 3–2 is neither in 2Z nor in 3Z. Hence, S is not a subgroup of (Z, +). Thus, if A and B are subgroups of G, A∪B need not be a subgroup of G. But, if A ⊆ B, then A∪B = B is a subgroup of G. The next exercise says that this is the only situation in which A∪B is a subgroup of G.

---

6) Let A and B be two subgroups of a group G. Prove that A∪B is a subgroup of G iff A ⊆ B or B ⊆ A.

(**Hint :** Suppose A ⊈ B and B ⊈ A. Take a ∈ A \ B and b ∈ B \ A. Then show that ab ∉ A∪B. Hence, A∪B ≰ G. Note that proving this amounts to proving that A∪B ≤ G ⇒ A ⊆ B or B ⊆ A.)

'≰' denotes 'is not a subgroup of'.

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 | a ∈ A, b ∈ B}.

For example, (2Z) (3Z) = { (2m) (3n) | m, n ∈ Z }
= { 6mn | m, n ∈ Z }
= 6Z.

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

S = {I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}, and its subgroups H = {I, (1 2) } and K = {I, (1 3)}.

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

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

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

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

Theorem 5 : Let H and K be subgroups of a group G. Then HK is a subgroup of G if and only if HK = KH.

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

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

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

Hence, we have shown that HK = KH.

Conversely, assume that HK = KH. We have to prove that HK ≤ G. Since $e = e^2 \in HK$, HK ≠ ϕ. Now, let a, b ∈ HK. Then a = hk and $b = h_1 k_1$ for some h, $h_1 \in H$ and k, $k_1 \in K$. 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, $\exists\ h_2 k_2 \in HK$ such that $(kk_1^{-1})h_1^{-1} = h_2 k_2$.

Then, $ab^{-1} = h(h_2 k_2) = (hh_2)k_2 \in HK$.

Thus, by Theorem 1, HK ≤ G.

The following result is a nice corollary to Theorem 5.

Corollary : If H and K are subgroups of an abelian group G, then HK is a subgroup of G.

Try the following exercise now.

E 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.

3.4 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 $\mathcal{F}$ of all subgroups of G that contain S, that is,

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

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

Note that

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

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

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 $\langle S \rangle$.

Thus, $\langle S \rangle = \cap \{ H \mid H \leq G, S \subseteq H\}$.

If $S = \phi$, then $\langle S \rangle = \{e\}$.

If $\langle S \rangle = G$, then we say that G is **generated by the set S**, and that S is a **set of generators of G.**

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

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

Theorem 6 : If S is a non-empty subset of a group G, then

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

Proof : Let $A = \{ a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \mid a_i \in S \text{ for } 1 \le i \le k, n_1, \ldots, n_k \in Z \}$.

Since $a_1, \ldots, a_k \in S \subseteq \langle S \rangle$ and $\langle S \rangle$ is a subgroup of G, $a_i^{n_i} \in \langle S \rangle$

$\forall$ i = 1, ... k. Therefore, $a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \in \langle S \rangle$, i.e., $A \subseteq \langle S \rangle$.

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

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 $x = a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}$,

$y = b_1^{m_1} b_2^{m_2} \ldots b_r^{m_r}$, $a_i, b_j \in S$ for $1 \le i \le k$, $1 \le j \le r$.

Then $xy^{-1} = (a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}) (b_1^{m_1} b_2^{m_2} \ldots b_r^{m_r})^{-1}$

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

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

This shows that $\langle S \rangle = A$.

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

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 $r \ge 0$ and $s \in S$. Thus, $m \in \langle S \rangle$. And hence, $\langle S \rangle = Z$.

Try the following exercises now.

E 8) Show that $S = \{1\}$ generates Z.

E 9) Show that a subset S of N generates the group Z of all integers iff there exist $s_1, \ldots, s_k$ in S and $n_1, \ldots, n_k$ in Z such that $n_1 s_1 + \ldots + n_k s_k = 1$.
(**Hint** : Apply Theorem 6.)

E 10) Show that if S generates a group G and $S \subseteq T \subseteq G$, then $\langle T \rangle = G$.

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

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

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

A subgroup H of a group G is called a **cyclic subgroup** if it is a cyclic group. Thus, $\langle (1\ 2) \rangle$ is a cyclic subgroup of S_3 and $2Z = \langle 2 \rangle$ is a cyclic subgroup of Z.

We would like to make the following remarks here.

Remark 3 : i) If $K \le G$ and $a \in K$, then $\langle a \rangle \subseteq K$. This is because $\langle a \rangle$ is the smallest subgroup of G containing a

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

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

Now you can try the following simple exercises.

E 11) Show that if $G \neq \{e\}$, then $G \neq < e >$.

E 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 $G = < a > = \{ a^n \mid n \in Z\}$. Then, for any x, y in G, there exist $m, n \in Z$ such that $x = a^m$, $y = a^n$. But, then, $xy = a^m . a^n = a^{m+n} = a^{n+m} = a^n . a^m = yx$. 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 is cyclic. Consider the following example.

Fig. 2: Felix Klein (1849–1925)

Example 7 : Consider the set $K_4 = \{e, a, b, ab\}$ and the binary operation on 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

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 by e, a, b or ab.

Thus, K_4 is not cyclic.

Use Theorem 7 to solve the following exercise.

E 13) Show that S_3 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 $\exists\, n \in Z$ 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 $S = \{ t \in N \mid x^t \in H\}$ 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 $m, r \in Z$, $0 \leq r \leq k-1$. But then $x^r = x^{n-mk} = x^n . (x^k)^{-m} \in H$, 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 $x^n = (x^k)^m \in < x^k >$. 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

$A = <I>$

$B = <(1\ 2)>$

$C = <(1\ 3)>$

$D = <(2\ 3)>$

$E = <(1\ 2\ 3)>$.

H is a proper subgroup of G if $H \subsetneq G$.

As you can see, all these are cyclic. But, by E 13 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.

E 14) Show that any non-abelian group must have a proper subgroup other than {e}.

E 15) Obtain all the subgroups of $\mathbb{Z}_4$, which you know is $<\bar{1}>$.

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

3.5 SUMMARY

In this unit we have covered the following points.

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

3.6 SOLUTIONS/ANSWERS

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

E 2) $\{e\} \neq \emptyset$. Also $ee^{-1} = e \in \{e\}$ $\therefore$, by Theorem 1, $\{e\} \leq G$.

$G \neq \emptyset$. Also for any $a \in G$, $a^{-1} \in G$, $\ldots$ for $a, b \in G$,

$a, b^{-1} \in G$. $\therefore ab^{-1} \in G$ $\therefore G \leq G$

E 3) Since $\omega^n = 1$, $(1-\omega^n) = 0$, $\ldots$

$(1-\omega)(1 + \omega + \omega^2 + \ldots + \omega^{n-1}) = 0$.

Since $\omega \neq 1$, $1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0$.

E 4) From E 14 of Unit 2 recall the elements of S_3. On writing the operation table for S_3 you will find that only I commutes with every permutation in S_3.

E 5) The divisors of 9 are 1, 3 and 9.
Thus, 9Z is a subgroup of Z, 3Z and itself only.

E 6) We know that if $A \subseteq B$ or $B \subseteq A$, then AUB is A or B, and hence, is a subgroup of G.
Conversely, we will assume that $A \not\subseteq B$ and $B \not\subseteq A$, and conclude that $AUB \not\leq G$.
Since $A \not\subseteq B$, $\exists\ a \in A$ such that $a \notin B$.
Since $B \not\subseteq A$, $\exists\ b \in B$ 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, $ab \notin B$. $\therefore ab \notin AUB$.
But $a \in AUB$ and $b \in AUB$. So, $AUB \not\leq G$.

E 7) $AB = \{ I, (1\ 4), (1\ 2), (1\ 2\ 4) \}$.
But, $(1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin AB$. $\therefore AB \not\leq S_4$.

E 8) For any $n \in Z$, $n = n.1 \in <\{1\}>$. $\therefore Z = <\{1\}>$.

E 9) Firstly, suppose $Z = <S>$. Then $1 \in <S>$. $\therefore \exists\ s_1, \ldots, s_k \in S$ and $n_1, \ldots, n_k \in Z$ such that $n_1s_1 + \ldots + n_ks_k = 1$.
Conversely, suppose $\exists\ s_1, \ldots, s_k \in S$ and $n_1, \ldots, n_k \in Z$ such that $n_1s_1 + n_2s_2 + \ldots + n_ks_k = 1$.
Then, for any $n \in Z$, $n = n.1 = nn_1s_1 + \ldots + nn_ks_k \in <S>$.
$\therefore Z = <S>$.

E 10) We know that $G = <S>$. Therefore, for any $g \in G$,
$\exists\ s_1, \ldots, s_k \in S$ and $n_1, \ldots, n_k \in Z$ such that
$g = s_1^{n_1} \ldots s_k^{n_k}$. Since $S \subseteq T$, $s_i \in T\ \forall\ i = 1, \ldots, k$.
$\therefore$ by Theorem 6, we see that $G = <T>$.

E 11) Since $G \neq \{e\}$, $\exists\ a \neq e$ in G. Since $a \neq e$, $a \neq e^r$ for any $r \in Z$. $\therefore a \notin <e>$.
$\therefore G \neq <e>$.

E 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 $n \in Z$.
$\therefore a^n \in <a^{-1}>$. $\therefore <a> \subseteq <a^{-1}>$.
Similarly, $<a^{-1}> \subseteq <a>$.
$\therefore <a> = <a^{-1}>$.

E 13) Since S_3 is not abelian (e.g., $(1\ 3) \circ (1\ 2) \neq (1\ 2) \circ (1\ 3)$), by Theorem 7, S_3 can't be cyclic.

E 14) Let G be a non-abelian group. Then $G \neq \{e\}$. Therefore, $\exists\ a \in G$, $a \neq e$. Then $<a> \leq G$. $G \neq <a>$, since G is non-abelian. $\therefore <a> \not\leq G$.

E 15) Since Z_4 is cyclic, all its subgroups are cyclic.
Thus, its subgroups are Z_4, $<\bar{2}>$, $<\bar{3}>$ and $\{\bar{0}\}$.

UNIT 4 LAGRANGE'S THEOREM

Structure

4.1 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 Block 2 of this course you will be using Lagrange's theorem again and again. So, make sure that you read this unit carefully.

Objectives

After reading this unit, you should be able to

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

4.2 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

$Hx = \{ hx \mid h \in H \}$

a **right coset** of H in G. The element x is a **representative** of Hx.

We can similarly define the left coset

$xH = \{ xh \mid h \in H \}$.

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

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

Let us look at some examples.

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

Solution : Consider the right coset of H in G represented by e, the identity of G. Then

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

Similarly, $eH = H$.

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

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

Solution : Now $H = 4\mathbb{Z} = \{ \ldots, -8, -4, 0, 4, 8, 12, \ldots \}$

The right cosets of H are

$H + 0 = H$, using Example 1.

$H + 1 = \{ \ldots, -11, -7, -3, 1, 5, 9, 13, \ldots \}$

$H + 2 = \{ \ldots, -10, -6, -2, 2, 6, 10, 14, \ldots \}$

$H + 3 = \{ \ldots, -9, -5, -1, 3, 7, 11, 15, \ldots \}$

$H + 4 = \{ \ldots, -8, -4, 0, 4, 8, 12, \ldots \} = H$

Similarly, you can see that $H+5 = H+1$, $H+6 = H+2$, and so on.

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

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

In general, **the distinct right cosets of H (= nZ) in Z are H, H+1, ..., H+(n–1).** 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) $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

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 $x \in Hx$, $x \in H$.

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 $h = (hx^{-1})\, x \in Hx$, since $hx^{-1} \in H$.

$\therefore\ H \subseteq Hx$.

$\therefore\ H = Hx$.

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

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

Thus, we have proved (c).

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

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

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

H is A_3, the alternating group on 3 symbols.

Solution : Two cosets are

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

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

$= \{ (1\ 2), (2\ 3), (1\ 3) \}$

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

$(1\ 2)H = (2\ 3)H = (1\ 3)H$ and

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

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

Try the following exercise now.

E 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 2×2 matrices over **C**,

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

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ 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 a 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 1 (b), we see that

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

Using Theorem 1(c), we see that

$HB = HC = H(-B) = H(-C)$.

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

The following exercise will help you to understand Q_8.

E 2) Show that $K = \{I, -I\}$ is a subgroup of Q_8. Obtain all its right cosets in Q_8.

We will now show that each group can be written as the union of disjoint cosets of any of its subgroups. For this we define a relation on the elements of G.

Definition : Let H be a subgroup of a group G. We define a relation '~' on G by $x \sim y$ iff $xy^{-1} \in H$, where $x, y \in G$. Thus, from Theorem 1 we see that $x \sim y$ iff $Hx = Hy$.

We will prove that this relation is an equivalence relation (see Unit 1).

Theorem 2 : Let H be a subgroup of a group G. Then the relation ~ defined by '$x \sim y$ iff $xy^{-1} \in H$' 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 $xy^{-1} \in H$.

$\therefore (xy^{-1})^{-1} = yx^{-1} \in H$. Thus, $y \sim x$. That is, ~ is symmetric.

Finally, if $x, y, z \in G$ such that $x \sim y$ and $y \sim z$, then $xy^{-1} \in H$ and $yz^{-1} \in H$.

$\therefore (xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H$ $\therefore x \sim z$.

That is, ~ is transitive.

Thus, ~ is an equivalence relation.

The equivalence class determined by $x \in G$ is

$[x] = \{y \in G \mid y \sim x\} = \{y \in G \mid xy^{-1} \in H\}$.

Now, we will show that [x] = Hx. So, let $y \in [x]$. Then Hy = Hx, by Theorem 1. And since $y \in Hy$, $y \in Hx$.

Therefore, $[x] \subseteq Hx$.

Now, consider any element hx of Hx. Then $x(hx)^{-1} = xx^{-1}h^{-1} = h^{-1} \in H$.

Therefore, $hx \sim x$. That is, $hx \in [x]$. This is true for any $hx \in Hx$. Therefore, $Hx \subseteq [x]$.

Thus, we have shown that [x] = Hx.

Using Theorem 2 and Theorem 1(d) of Unit 1, we can make the following remark.

Remark : If Hx and Hy are two right cosets of a subgroup H in G, then **Hx = Hy or $Hx \cap Hy = \phi$.**

Note that what Theorem 2 and the remark above say is that **any subgroup H of a group G partitions G into disjoint right cosets.**

On exactly the same lines as above we can state that

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

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

So, for example, $S_3 = <(1\ 2\ 3)> \cup (1\ 2)<(1\ 2\ 3)>$ (using Example 3).

You may like to do the following exercises now.

E 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 $f : H \to Hx : f(h) = hx$ is a bijection.)

E 4) Write $\mathbb{Z}$ as a union of disjoint cosets of $5\mathbb{Z}$.

Using E 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 in the next section.

4.3 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, $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$!

You can also see that $o(\mathbb{Z}_n) = n$. 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

$$f : \{ Hx \mid x \in G\} \to \{y H \mid y \in G \} : f(Hx) = x^{-1}H.$$

Now try E 5.

E 5) Check that f is a bijection.

E 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 cosets 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 $\{e\}g = \{g\}\ \forall\ g \in G$ and $\{e\}g \neq \{e\}g'$ if $g \neq g'$.

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 1830.

Fig 1: Joseph Louis Lagrange (1736 –1813)

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 $Hx_1, Hx_2, \ldots, Hx_r$ are all the distinct right cosets of H in G, we have

$G = Hx_1 \cup Hx_2 \cup \ldots \cup Hx_r$ .....(1)

and $|G : H| = r$.

From E 3, we know that $|Hx_1| = |Hx_2| = \ldots = |Hx_r| = o(H)$.

For any finite set A, $|A|$ denotes the number of elements in A.

Thus, the total number of elements in the union on the right hand side of (1) is

$o(H) + o(H) + \ldots + o(H)$ (r times) $= r\ o(H)$.

Therefore, (1) says that $o(G) = r\ o(H)$

$= o(H)\ |G : H|$.

You will see the power of Lagrange's theorem when we get down to obtaining all the subgroups 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 $\{e, g, g^2, \ldots\}$ 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 $g^{r-s} = e$ and $r-s \in N$. Thus, the set $\{ t \in N \mid g^t = e \}$ 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

o(g) = 1 iff g = e.

$< g > = \{e, g, g^2, \ldots, g^{n-1}\}$.

Therefore, $o(g) = o(< g >) = n$.

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 $ng = e$.)

Now suppose $g \in G$ is of infinite order. Then, for $m \neq n$, $g^m \neq g^n$. (Because, if $g^m = g^n$, then $g^{m-n} = e$, which shows that $< g >$ is a finite group.) We will use this fact while proving Theorem 5.

Try the following exercise now.

E 6) What are the orders of

a) $(1\ 2) \in S_3$, b) $I \in S_4$, c) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in Q_8$, d) $\bar{3} \in Z_4$, e) $1 \in R$?

Now let us prove an important result about the order of an element.

Theorem 4 : Let G be a group and $g \in G$ be of order n. Then $g^m = e$ for some $m \in N$ iff $n \mid m$.

Proof : We will first show that $g^m = e \Rightarrow n \mid m$. For this consider the set $S = \{ r \in Z \mid g^r = e \}$.

Now, $n \in S$. Also, if $a, b \in S$, then $g^a = e = g^b$. Hence, $g^{a-b} = g^a (g^b)^{-1} = e$. Therefore, $a-b \in S$. Thus, $S \leq Z$.
So, from Example 4 of Unit 3, we see that $S = nZ$. Remember, n is the least positive integer in S!

Now if $g^m = e$ for some $m \in N$, then $m \in S = nZ$. Therefore, $n \mid m$.

Now let us show that $n \mid m \Rightarrow g^m = e$. Since $n \mid m$, $m = nt$ 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 a 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

$$o(g^m) = \frac{n}{(n,m)} \quad \forall\ m = 1, \ldots, n-1.$$ ((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 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 $o(g) = n$, $G = \{e, g, \ldots, g^{n-1}\}$. $< g^m >$, being a subgroup of G, must be of finite order. Thus, g^m is of finite order. Let $o(g^m) = t$. We will show that $t = \frac{n}{(n, m)}$.

Now, $g^{mt} = (g^m)^t = e \Rightarrow n \mid tm$, by Theorem 4.
Let $d = (n, m)$. We can then write $n = n_1 d$, $m = m_1 d$, where $(m_1, n_1) = 1$.

Then $n_1 = \frac{n}{d} = \frac{n}{(n,m)}$.

Now, $n \mid tm \Rightarrow n \mid tm_1 d \Rightarrow n_1 d \mid tm_1 d \Rightarrow n \mid tm_1$.
But $(n, m_1) = 1$. Therefore, $n_1 \mid t$. ..... (1)
Also, $(g^m)^{n_1} = g^{m_1 d n_1} = g^{m_1 n} = (g^n)^{m_1} = e^{m_1} = e$.
Thus, by definition of $o(g^m)$ and Theorem 4, we have

$t \mid n_1$. ..... (2)

(1) and (2) show that

$$t = n_1 = \frac{n}{(n,m)},$$

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.

E 7) Find the orders of $\overline{2}$, $\overline{4}$, and $\overline{5} \in Z_{18}$.

The next exercise is a consequence of Lagrange's theorem.

E 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 E 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 E 8 and Theorem 4, $o(a) \mid p$. 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 Theorems 3 and 6, we can immediately say that all the proper subgroups of a group of order 35 are cyclic.

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 cyclic, say $G = < x >$, where $o(x) = mn$ $(m, n \neq 1)$.

Then, $(x^m)^n = x^{mn} = e$. Thus, by Theorem 4, $o(x^m) \leq n < o(G)$.

Thus, $<x^m>$ is a proper non-trivial subgroup of G.

Now, you can use Theorem 7 to solve the following exercise.

E 9) Obtain two non-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** $\phi : N \to N$ as follows :

$\phi(1) = 1$, and

$\phi(n)$ = 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 $n \geq 2$.

Lemma 1 : Let $G = \left\{ \bar{r} \in Z_n \mid (r,n) = 1 \right\}$, where $n \geq 2$. Then $(G, .)$ is a group, where $\bar{r}.\bar{s} = \overline{rs}\ \forall\ \bar{r}, \bar{s} \in Z_n$. Further, $o(G) = \phi(n)$.

Proof : We first check that G is closed under multiplication.

Now, $\bar{r}, \bar{s} \in G \Rightarrow (r,n) = 1$ and $(s, n) = 1 \Rightarrow (rs, n) = 1$.

$\Rightarrow \overline{rs} \in G$. Therefore, . is a binary operation on G.

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

Now, for any $\bar{r} \in G$, $(r,n) = 1$.

$\Rightarrow ar+bn = 1$ for some $a, b \in Z$ (by Theorem 8 of Unit 1)

$\Rightarrow n \mid ar-1$

$\Rightarrow ar \equiv 1 \pmod{n}$.

$\Rightarrow \bar{a}\ \bar{r} = \bar{1}$.

$\Rightarrow \bar{a} = \bar{r}^{-1}$

Further, $\bar{a} \in G$, because if a and n have a common factor other than 1, then this factor will divide $ar + bn = 1$. But that is not possible.

Thus, every element in G has an inverse.

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

In fact, it is the group of the elements of Z_n that have multiplicative inverses.

Since G consists of all those $\bar{r} \in Z_n$ 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 mathematicians Euler and Pierre Fermat.

Theorem 8 (Euler-Fermat) : Let $a \in N$ and $n \geq 2$ such that $(a,n) = 1$.
Then, $a^{\phi(n)} \equiv 1 \pmod{n}$.

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 E 8 and find that $\bar{a}^{\phi(n)} = \bar{1}$.
Thus, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Now you can use Theorem 8 to solve the following exercises.

E 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.)

E 11) Let $a \in N$ and p be a prime. Show that $a^{p-1} \equiv 1 \pmod{p}$. (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 $m \mid o(G)$, 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

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

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

Now let us summarise what we have done in this unit.

4.4 SUMMARY

In this unit we have covered the following points.

1) The definition and examples of right and left cosets of a subgroup.
2) Two left (right) cosets of a subgroup are disjoint or identical.
3) Any subgroup partitions a group into disjoint left (or right) cosets of the subgroup.
4) The definition of the order of a group and the order of an element of a group.
5) The proof of Lagrange's theorem, which states that if H is a subgroup of a finite group G, then $o(G) = o(H) \mid G : H \mid$. But, if $m \mid o(G)$, then G need not have a subgroup of order m.
6) The following consequences of Lagrange's theorem:
   i) Every group of prime order is cyclic.
   ii) $a^{\phi(n)} \equiv 1 \pmod{n}$, where $a, n \in N$, $(a,n) = 1$ and $n \geq 2$.

4.5 SOLUTIONS/ANSWERS

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

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

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

E 2) Since $ab^{-1} \in K\ \forall\ a, b \in K$, we can apply Theorem 1 of Unit 3 to say that $K \leq Q_8$.
Now, $K = KI = K(-I)$, $KA = K(-A) = \{A, -A\}$,
$KB = K(-B) = \{B, -B\}$, $KC = K(-C) = \{C, -C\}$.

E 3) Let Hx be a coset of H in G. Consider the function $f : H \to Hx : f(h) = hx$.

Now, for $h, h' \in H$, $hx = h'x \Rightarrow h = h'$, 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 $f : H \to xH : f(h) = xh$ is a bijection.
Thus, the elements of H and xH are in one-to-one correspondence.

E 4) The distinct cosets of 5Z in Z are 5Z, 5Z+1, 5Z+2, 5Z+3, 5Z+4.
$\therefore Z = 5Z \cup 5Z+1 \cup 5Z+2 \cup 5Z+3 \cup 5Z+4$.

E 5) f is well defined because $Hx = Hy \Rightarrow xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H$
$\Rightarrow (y^{-1})^{-1}\ x^{-1} \in H \Rightarrow x^{-1}H = y^{-1}H$.
$\Rightarrow f(Hx) = f(Hy)$.
f is 1-1 because $f(Hx) = f(Hy) \Rightarrow x^{-1}H = y^{-1}H$
$\Rightarrow yx^{-1} \in H \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy$.
f is surjective because any left coset of H in G is $yH = f(Hy^{-1})$.

Therefore, f is a bijection.

E 6) a) $(1\ 2) \neq I$, $(1\ 2)^2 = (1\ 2) \circ (1\ 2) = I$. $\therefore o((1\ 2)) = 2$.

b) $I^1 = I$. $\therefore o(I) = 1$.

c) 2

d) $\bar{3} \neq \bar{0}$, $2.\bar{3} = \bar{6} = \bar{2}$, $3.\bar{3} = \bar{9} = \bar{1}$, $4.\bar{3} = \overline{12} = \bar{0}$. $\therefore o(\bar{3}) = 4$.

e) Since $< 1 > = R$ is infinite, 1 is of infinite order.

E 7) $Z_{18} = < \bar{1} >$. Thus, using Theorem 5, we see that

$o(\bar{r}) = o(r.\ \bar{1}) = \dfrac{18}{(18, r)}$, for any $\bar{r} \in Z_{18}$.

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

E 8) Since $o(x) = o(< x >)$ and $o(< x >) \mid o(G)$, $o(x) \mid o(G)$.

Thus, using Theorem 4, $x^{o(G)} = e$.

E 9) $o(Z_8) = 8 = 2 \times 4$.

$\bar{2} \in Z_8$ such that $o(\bar{2}) = 4$. Then $< \bar{2} > \subsetneq Z_8$.

Similarly, $\bar{4} \in Z_8$ such that $o(\bar{4}) = 2$. $\therefore < \bar{4} > \subsetneq Z_8$

E 10) We know that in Z_{23}, $(\bar{3})^{o(23)} = \bar{1}$,

that is, $\bar{3}^{22} = \bar{1}$. $\therefore \bar{3}^{44} = \bar{1}$

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

Thus, $3^{47} \equiv 27 \pmod{23}$.

Therefore, on dividing 3^{47} by 23, the remainder we get is 27.

E 11) We get the result immediately by using Theorem 8 and the fact that $\phi(p) = p-1$.

NOTES

UTTAR PRADESH
RAJARSHI TANDON OPEN UNIVERSITY

UGMM – 06
Abstract Algebra

Block

2

SOME MORE GROUP THEORY

SOME MORE GROUP THEORY

This block is a continuation of Block 1, where we discussed various groups and their subgroups. In this block we start by looking at a particular kind of subgroup, called normal subgroup. In Unit 5 you will see why these subgroups are important.

In the second unit of this block we will introduce you to the concept of algebraically indistinguishable systems. We say that such systems are isomorphic. This word was first used in 1870 by the mathematician Camille Jordan, to describe two groups that are not equal but have the same algebraic behaviour. Isomorphisms are special cases of homomorphisms, which are functions between groups that preserve the algebraic structure of their domains. In Unit 6 we will discuss homomorphisms, isomorphisms and the important Fundamental Theorem of Homomorphism.

In Unit 7 we will study groups of permutations, a detailed study of material covered in Sec. 2.5.2. Permutation groups give you a concrete basis for the abstract group theory that you are studying. These groups are also important because of the fact that every group is isomorphic to a permutation group, as you will see.

In the last unit of this block we will study the algebraic structure of certain finite groups, in particular, groups of order 1 to 10. To do so we will use certain results which were proved by the mathematician Sylow. We will also need the concept of direct products of groups, which we discuss in the unit.

At the end of the block you will find the programme notes of our video programme, "Groups of Symmetries". It deals with some concepts of group theory that we have discussed in Block 1 and this block. You can view this programme at your study centre.

With this block we end the study of group theory. In the next two blocks you will study other algebraic systems, namely, rings and fields. You will see that these systems are also groups. And hence, you will continue to use the concepts that you have studied in this block and the previous one.

After studying this block, you must attempt Assignment 1, which covers Blocks 1 and 2 of this course.

Notations and Symbols

xHy	$\{ xhy \mid h \in H \}$
$H \trianglelefteq G$	H is a normal subgroup of G
A_n	alternating group on n symbols
S_n	symmetric group on n symbols
D_{2n}	dihedral group of order 2n
G/H	quotient group of G by H
Ker f	kernel of the homomorphism f
$[x, y]$	$x^{-1} y^{-1} xy$, the commutator of x and y
$[G, G]$	commutator subgroup of G
$\simeq$	is isomorphic to
Aut G	group of automorphisms of G
Inn G	group of inner automorphisms of G
Z(G)	centre of G
$(i_1 i_2 \ldots i_r)$	an r-cycle
$G \times G'$	external direct product of the groups G and G′
$H \times K$	internal direct product of the subgroups H and K

Also look at the notations given in Block 1.

UNIT 5 NORMAL SUBGROUPS

Structure

5.1 INTRODUCTION

In Block 1 you studied subgroups and cosets. We start this unit by discussing a special class of subgroups, called normal subgroups. You will see that the cosets of such a subgroup form a group with respect to a suitably defined operation. These groups are called quotient groups. We will discuss them in some detail in Sec. 5.3.

Once you are comfortable with normal subgroups and quotient groups, you will find it easier to understand the concepts and results that are presented in the next unit. So, make sure that you have met the following objectives before going to the next unit.

Objectives

After reading this unit, you should be able to

- verify whether a subgroup is normal or not,
- obtain a quotient group corresponding to a given normal subgroup.

5.2 NORMAL SUBGROUPS

In E 1 of Unit 4 you saw that a left coset of a subgroup H, aH, need not be the same as the right coset Ha. But, there are certain subgroups for which the right and left cosets represented by the same element coincide. This type of subgroup is very important in group theory, and we give it a special name.

Definition : A subgroup N of a group G is called a **normal** subgroup of G if $Nx = xN \ \forall \ x \in G$, and we write this as $N \trianglelefteq G$.

For example, any group G has two normal subgroups, namely, {e} and G itself. Can you see why? Well, $\{e\}x = \{x\} = x\{e\}$, for any $x \in G$, and $Gx = G = xG$, for any $x \in G$.

Let us consider another example.

Example 1 : Show that every subgroup of **Z** is normal in **Z**.

Solution : From Example 4 of Unit 3, you know that if H is a subgroup of Z, then $H = m\mathbf{Z}$, for some $m \in \mathbf{Z}$. Now, for any $z \in \mathbf{Z}$,

$$H + z = \{\ldots, -3m + z, -2m + z, -m + z, z, m + z, 2m + z, \ldots\}$$
$$= \{\ldots, z - 3m, z - 2m, z - m, z, z + m, z + 2m, \ldots\} \text{ (since } + \text{ is commutative)}$$
$$= z + H$$

$\therefore H \trianglelefteq Z$.

Example 1 is a special case of the fact that every subgroup of a commutative group is a normal subgroup. We will prove this fact later (in Theorem 2).

Try the following exercise now.

E 1) Show that $A_3 \trianglelefteq S_3$ (see Example 3 of Unit 4).

Let us now prove a result that gives equivalent conditions for a subgroup to be normal.

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

a) H is normal in G.

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

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

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

Proof : We will show that (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a). This will show that the three statements are equivalent.

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

Since $hg \in Hg = gH$, $\exists \; h_1 \in H$ such that $hg = gh_1$.

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

$\therefore$ (b) holds.

(b) $\Longrightarrow$ (c) : Now, we know that (b) holds, i.e., for $g \in G$, $g^{-1}Hg \subseteq H$. We want to show that $H \subseteq g^{-1}Hg$. Let $h \in H$. Then

$h = ehe = (g^{-1}g)\, h\, (g^{-1}g)$

$= g^{-1}\,(ghg^{-1})\, g$

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

$\therefore \; H \subseteq g^{-1}Hg$.

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

$Ha = Hb \Longleftrightarrow Hac = Hbc$ for any $a, b, c \in G$.

(c) $\Longrightarrow$ (a) : For any $g \in G$, we know that $g^{-1}Hg = H$.

$\therefore \; g(g^{-1}Hg) = gH$, that is, $Hg = gH$.

$\therefore \; H \trianglelefteq G$, that is, (a) holds.

We would like to make the following remark about Theorem 1.

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

For example, in E 1 you have shown that $A_3 \trianglelefteq S_3$. Therefore, by Theorem 1, $(1\;2)^{-1}\, A_3 (1\;2) = A_3$. But, $(1\;2)^{-1}(1\;3\;2)\,(1\;2) \neq (1\;3\;2)$. In fact, it is $(1\;2\;3)$.

Try the following exercise now.

E 2) Consider the subgroup $SL_2(R) = \{\, A \in GL_2(R) \mid \det(A) = 1 \,\}$ of $GL_2(R)$ (see Example 5 of Unit 2). Using the facts that

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

prove that $SL_2(R) \trianglelefteq GL_2(R)$.

We now prove a simple result that we stated after Example 1. It is actually a corollary to Theorem 1.

Theorem 2 : Every subgroup of a commutative group is normal.

Proof : Let G be an abelian group, and $H \leq G$. For any $g \in G$ and $h \in H$, $g^{-1}hg = (g^{-1}g)h = h \in H$. $\therefore \; g^{-1}Hg \subseteq H$. Thus, $H \trianglelefteq G$.

Theorem 2 says that if G is abelian, then all its subgroups are normal. Unfortunately, the converse of this is not true. That is, there are non-commutative groups whose subgroups are all normal. We will give you an example after doing Theorem 3. Let us first look at another example of a normal subgroup.

Example 2 : Consider the Klein 4-group, K_4, given in Example 7 of Unit 3. Show that both its subgroups $< a >$ and $< b >$ are normal.

Solution : Consider the table of the operation given in Example 7 of Unit 3. Note that a and b are of order 2. Therefore, $a = a^{-1}$ and $b = b^{-1}$. Also note that $ba = ab$.

Now, let $H = \langle a \rangle = \{e, a\}$. We will check that $H \trianglelefteq K_4$, that is, $g^{-1}hg \in H \; \forall \; g \in K_4$ and $h \in H$.

Now, $g^{-1}eg = e \in H \; \forall \; g \in K_4$.

Further, $e^{-1}ae = a \in H$, $a^{-1}aa = a \in H$, $b^{-1}ab = bab = a \in H$ and $(ab)^{-1}\, a(ab)$
$= b^{-1}\,(a^{-1}aa)b = bab = a \in H$.

$\therefore \; H \trianglelefteq K_4$.

By a similar proof we can show that $\langle b \rangle \trianglelefteq K_4$.

In Example 2, both $\langle a \rangle$ and $\langle b \rangle$ are of index 2 in K_4. We have the following result about such subgroups.

Theorem 3 : Every subgroup of a group G of index 2 is normal in G.

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

Now, $G = N \cup yN$, and $x \in G$. $\therefore \; x \in N$ or $x \in yN$.
Since $N \cap Nx = \phi$, $x \notin N$. $\therefore \; x \in yN$. $\therefore \; xN = yN$.
To show that $N \trianglelefteq G$, we need to show that $Nx = xN$.
Now, for any $n \in N$, $nx \in G = N \cup xN$. Therefore, $nx \in N$ or $nx \in xN$.
But $nx \notin N$, since $x \notin N$. $\therefore \; nx \in xN$.

Thus, $Nx \subseteq xN$.

By a similar argument we can show that $xN \subseteq Nx$.

$\therefore \; Nx = xN$, and $N \trianglelefteq G$.

We will use this theorem in Unit 7 to show that, for any $n \geq 2$, the alternating group A_n is a normal subgroup of S_n.

In fact, if you go back to the end of Sec. 4.3, you can see that $A_4 \trianglelefteq S_4$, since Lagrange's theorem implies that

$$|S_4 : A_4| = \frac{o(S_4)}{o(A_4)} = \frac{4!}{12} = 2.$$

Now let us look at an example to show that the converse of Theorem 2 is not true.

Consider the quaternion group Q_8, which we discussed in Example 4 of Unit 4. It has the following 6 subgroups:

$H_0 = \{I\}$, $H_1 = \{I, -I\}$, $H_2 = \{I, -I, A, -A\}$, $H_3 = \{I, -I, B, -B\}$,
$H_4 = \{I, -I, C, -C\}$, $H_5 = Q_8$.

You know that H_0 and H_5 are normal in Q_8. Using Theorem 3, you can see that H_2, H_3 and H_4 are normal in Q_8.

By actual multiplication you can see that

$g^{-1}H_1g \subseteq H_1 \; \forall \; g \in Q_8$. $\therefore \; H_1 \trianglelefteq Q_8$.

Therefore, all the subgroups of Q_8 are normal.

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

So far we have given examples of normal subgroups. Let us look at an example of a subgroup that isn't normal.

Example 3 : Show that the subgroup $\langle (1\ 2) \rangle$ of S_3 is not normal.

Solution : We have to find $g \in S_3$ such that $g^{-1}(1\ 2)g \notin \langle (1\ 2) \rangle$.

Let us try $g = (1\ 2\ 3)$.
Then, $g^{-1}(1\ 2)g = (3\ 2\ 1)(1\ 2)(1\ 2\ 3)$
$= (3\ 2\ 1)(2\ 3) = (1\ 3) \notin < (1\ 2) >$
Therefore, $< (1\ 2) >$ is not normal in S_3.

Try the following exercises now.

E 3) Consider the group of all 2×2 diagonal matrices over $\mathbb{R}^*$, with respect to multiplication. How many of its subgroups are normal?

E 4) Show that Z(G), the centre of G, is normal in G. (Remember that $Z(G) = \{x \in G \mid xg = gx \ \forall\ g \in G\}$.)

E 5) Show that $< (2\ 3) >$ is not normal in S_3.

In unit 3 we proved that if $H \leq G$ and $K \leq H$, then $K \leq G$. That is, '$\leq$' is a transitive relation. But '$\trianglelefteq$' is not a transitive relation. That is, if $H \trianglelefteq N$ and $N \trianglelefteq G$, it is not necessary that $H \trianglelefteq G$. We'll give you an example in Unit 7. But, corresponding to the property of subgroups given in Theorem 4 of Unit 3, we have the following result.

Theorem 4 : Let H and K be normal subgroups of a group G. Then $H \cap K \trianglelefteq G$.

Proof : From Theorem 4 of Unit 3, you know that $H \cap K \leq G$. We have to show that $g^{-1}xg \in H \cap K\ \forall\ x \in H \cap K$ and $g \in G$.

Now, let $x \in H \cap K$ and $g \in G$. Then $x \in H$ and $H \trianglelefteq G$. $\therefore g^{-1}xg \in H$.
Similarly, $g^{-1}xg \in K$. $\therefore g^{-1}xg \in H \cap K$.
Thus, $H \cap K \trianglelefteq G$.

In the following exercise we ask you to prove an important property of normal subgroups.

E 6) a) Prove that if $H \trianglelefteq G$ and $K \leq G$, then $HK \leq G$.
(**Hint** : Use Theorem 5 of Unit 3.)

b) Prove that if $H \trianglelefteq G$, $K \trianglelefteq G$, then $HK \trianglelefteq G$.

Now consider an important group which is the product of two subgroups, of which only one is normal.

Example 4 : Let G be the group generated by
$\{x, y \mid x^2 = e, y^4 = e, xy = y^{-1}x\}$.

Let $H = < x >$ and $K = < y >$.

'$\not\trianglelefteq$' denotes 'is not a normal subgroup of'.

Then show that $K \trianglelefteq G$, $H \not\trianglelefteq G$ and $G = HK$.

Solution : Note that the elements of G are of the form x^iy^j, where $i = 0, 1$ and $j = 0, 1, 2, 3$.
$\therefore G = \{e, x, xy, xy^2, xy^3, y, y^2, y^3\}$.
$\therefore |G : K| = 2$. Thus, by Theorem 3, $K \trianglelefteq G$.

Note that we can't apply Theorem 2, since G is non-abelian (as $xy = y^{-1}x$ and $y \neq y^{-1}$).

Now let us see if $H \trianglelefteq G$.

Consider $y^{-1}xy$. Now $y^{-1}xy = xy^2$, because $y^{-1}x = xy$.

If $xy^2 \in H$, then $xy^2 = e$ or $xy^2 = x$. (Remember $o(x) = 2$, so that $x^{-1} = x$.)
Now, $xy^2 = e \implies y^2 = x^{-1} = x$
$\implies y^3 = xy = y^{-1}x$
$\implies y^4 = x$
$\implies e = x$, a contradiction.
Again $xy^2 = x \implies y^2 = e$, a contradiction.
$\therefore y^{-1}xy = xy^2 \notin H$, and hence, $H \not\trianglelefteq G$.

Finally, from the definition of G you see that $G = HK$.

The group G is of order 8 and is called the **dihedral group, D_4**. It is the group of symmetries of a square, that is, its elements represent the different ways in which two copies of a square can be placed so that one covers the other. A geometric interpretation of its generators is the following (see Fig. 1) :

Take y to be a rotation of the Euclidean plane about the origin through $\frac{\pi}{2}$, and x the reflection about the vertical axis.

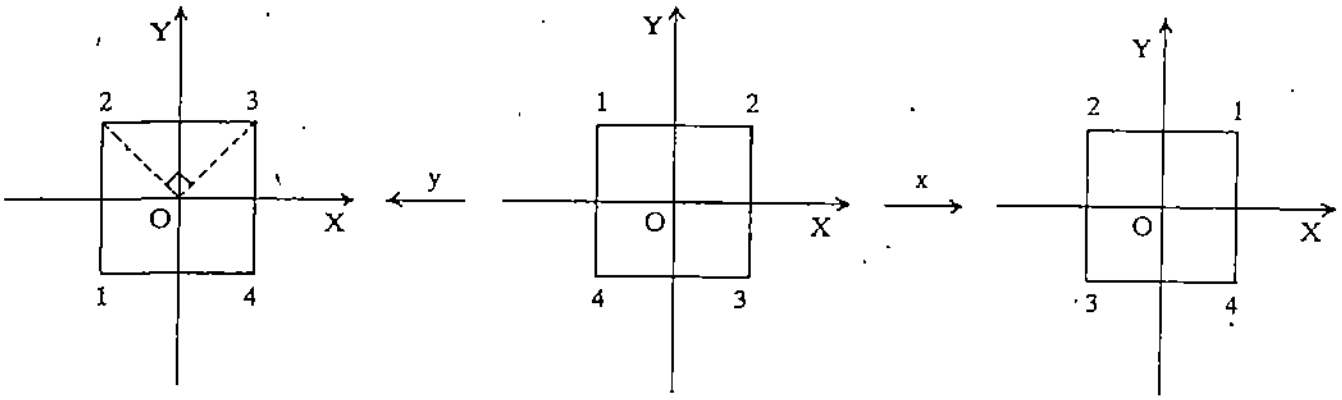


Fig. 1 : Geometric representation of the generators of D_4

We can generalise D_8 to the dihedral group
$D_{2n} = \langle \{x, y \mid x^2 = e, y^n = e, xy = y^{-1}x\} \rangle$, for $n > 2$.

Try the following exercise now.

E 7) Describe D_6 and give its geometric interpretation.

Let us now utilise normal subgroups to form new algebraic structures.

5.3 QUOTIENT GROUPS

In this section we will use a property of normal subgroups to create a new group. This group is analogous to the concept of quotient spaces given in the Linear Algebra course.

Let H be a normal subgroup of a group G. Then $gH = Hg$ for every $g \in G$. Consider the collection of all cosets of H in G. (Note that since $H \trianglelefteq G$, we need not write 'left coset' or 'right coset'; simply 'coset' is enough.) We denote this set by G/H. Now, for $x, y \in H$, we have

$(Hx)(Hy) = H(xH)y$, using associativity,
$= HHxy$, using normality of H,
$= Hxy$, since $HH = H$ because H is a subgroup.

Now, we define the product of two cosets Hx and Hy and G/H by
$(Hx)(Hy) = Hxy$ for all x, y in G.

Our definition seems to depend on the way in which we represent a coset. Let us explain this. Suppose C_1 and C_2 are two cosets, say $C_1 = Hx$ and $C_2 = Hy$. Then $C_1C_2 = Hxy$. But C_1 and C_2 can be written in the form Hx and Hy in several ways. So, you may ask : Does C_1C_2 depend on the particular way of writing C_1 and C_2?

In other words, if $C_1 = Hx = Hx_1$ and $C_2 = Hy = Hy_1$, then is $C_1C_2 = Hxy$ or is $C_1C_2 = Hx_1y_1$? Actually, we will show you that $Hxy = Hx_1y_1$, that is, the product of cosets is well-defined.

Since $Hx = Hx_1$ and $Hy = Hy_1$, $xx_1^{-1} \in H$, $yy_1^{-1} \in H$.

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

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

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

$\therefore Hxy = Hx_1y_1$.

So, we have shown you that multiplication is a well-defined binary operation on G/H.

We will now show that (G/H,.) is a group.

Theorem 5 : Let H be a normal subgroup of a group G and G/H denote the set of all cosets of H in G. Then G/H becomes a group under multiplication defined by Hx.Hy = Hxy, x, y ∈ G. The coset H = He is the identity of G/H and the inverse of Hx is the coset Hx^{-1}.

Proof : We have already observed that the product of two cosets is a coset.

This multiplication is also associative, since

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

Now, if e is the identity of G, then Hx. He = Hxe = Hx and He.Hx = Hex = Hx for every x ∈ G. Thus, He = H is the identity element of G/H.

Also, for any x ∈ G, $Hx\,Hx^{-1} = Hxx^{-1} = He = Hx^{-1}x = Hx^{-1}.Hx$.

Thus, the inverse of Hx is Hx^{-1}.

So, we have proved that G/H, the set of all cosets of a normal subgroup H in G, forms a group with respect to the multiplication defined by Hx.Hy = Hxy. This group is called the **quotient group** (or **factor group**) of G by H.

Note that the order of the quotient group G/H is the index of H in G. Thus, by Lagrange's theorem you know that if G is a finite group, then

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

Also note that if (G, +) is an abelian group and H ≤ G, then H ◁ G. Further, the operation on G/H is defined by (H + x) + (H + y) = H + (x + y).

Let us look at a few examples of quotient groups.

Example 5 : Obtain the group G/H, where $G = S_3$ and $H = A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

Solution : Firstly, note that $A_3 \trianglelefteq S_3$, since $|S_3 : A_3| = 2$.

From Example 3 of Unit 4 you know that G/H is a group of order 2 whose elements are H and (1 2) H.

Example 6 : Show that the group Z/nZ is of order n.

Solution : The elements of Z/nZ are of the form $a + nZ = \{a + kn \mid k \in Z\}$.
Thus, the elements of Z/nZ are precisely the congruence classes modulo n, that is, the elements of Z_n (see Sec. 2.5.1).

Thus, $Z/nZ = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

∴ o(Z/nZ) = n.

Note that addition in Z/nZ is given by $\bar{a} + \bar{b} = \overline{a + b}$.

Try these simple exercises now.

E 8) For any group G, determine the quotient groups corresponding to {e} and G.

E 9) Show that the quotient group of a cyclic group is cyclic.
(Hint : If $G = \langle x \rangle$, then show that $G/H = \langle Hx \rangle$.)

Now, do G and G/H always have the same algebraic properties?

On solving the following exercises you will see that if G is abelian, then so is G/H; but the converse need not be true. That is, if G/H is abelian, G may not be so. Thus, G and G/H need not have the same algebraic properties.

E 10) Show that if a group G is commutative, then so is G/H, for any H $\triangleq$ G.

E 11) Take the group D_8 of Example 4. Show that D_8/K is abelian, even though D_8 is non-abelian.

You may be surprised to know that given a group G, we can always define a normal subgroup H, such that G/H is abelian. This subgroup is the commutator subgroup.

Definition : Let G be a group and x, y $\in$ G. Then $x^{-1}y^{-1}xy$ is called the **commutator** of x and y. It is denoted by **[x, y]**.

The subgroup of G generated by the set of all commutators is called the **commutator subgroup** of G. It is denoted by **[G, G]**.

For example, if G is a commutative group, then
$x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e \forall x, y \in G$. $\therefore [G, G] = \{e\}$.

Try this exercise now.

E 12) Obtain [G, G], where G is cyclic.

Now, let us prove the commutativity of the factor group corresponding to the commutator subgroup.

Theorem 6 : Let G be a group. Then [G, G] is a normal subgroup of G. Further, G/[G, G] is commutative.

Proof : We must show that, for any commutator $x^{-1}y^{-1}xy$ and for any $g \in G$,
$g^{-1}(x^{-1}y^{-1}xy)g \in [G, G]$.

Now $g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in [G, G]$.
$\therefore$ [G, G] $\triangleq$ G.

For the rest of the proof let us denote [G, G] by H, for convenience.

Now, for x, y $\in$ G,

$HxHy = HyHx \Longleftrightarrow Hxy = Hyx \Leftrightarrow (xy)(yx)^{-1} \in H$

$\Longleftrightarrow xy\,x^{-1}\,y^{-1} \in H.$

Thus, since $xy\,x^{-1}\,y^{-1} \in H \forall x, y \in G$, $HxHy = HyHx \forall x, y \in G$. That is, G/H is abelian.

$xy\,x^{-1}\,y^{-1}$
$= (x^{-1})^{-1}(y^{-1})^{-1}x^{-1}y^{-1}$

Note that we have defined the quotient group G/H only if H $\triangleq$ G. But if H $\not\triangleq$ G we can still define G/H to be the set of all left (or right) cosets of H in G. But, in this case G/H will not be a group. The following exercise will give you an example.

E 13) For G = S_3 and H = $\langle (1\ 2) \rangle$, show that the product of right cosets in G/H is not well defined.
(Hint : Show that $H(1\ 2\ 3) = H(2\ 3)$ and $H(1\ 3\ 2) = H(1\ 3)$, but $H(1\ 2\ 3)(1\ 3\ 2) \neq H(2\ 3)(1\ 3)$)

E 13 leads us to the following remark.

Remark : If H is a subgroup of G, then the product of cosets of H is defined only when H $\triangleq$ G. This is because, if HxHy = Hxy $\forall$ x, y $\in$ G, then, in particular,

$x^{-1}Hx = Hx^{-1}x = He = H \forall x \in G$.

Therefore, for any $h \in H$, $x^{-1}hx = ex^{-1}hx \in Hx^{-1}Hx = H$.
That is, $x^{-1}Hx \subseteq H$ for any $x \in G$.
$\therefore H \trianglelefteq G$.

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

5.4 SUMMARY

In this unit we have brought out the following points.

1. The definition and examples of a normal subgroup.
2. Every subgroup of an abelian group is normal.
3. Every subgroup of index 2 is normal.
4. If H and K are normal subgroups of a group G, then so is $H \cap K$.
5. The product of two normal subgroups is a normal subgroup.
6. If $H \trianglelefteq N$ and $N \trianglelefteq G$, then H need not be normal in G.
7. The definition and examples of a quotient group.
8. If G is abelian, then every quotient group of G is abelian. The converse is not true.
9. The quotient group corresponding to the commutator subgroup is commutative.
10. The set of left (or right) cosets of H in G is a group if and only if $H \trianglelefteq G$.

5.5 SOLUTIONS/ANSWERS

E 1) $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$
You can check that
$A_3 I = A_3 = IA_3$, $A_3(1\ 2) = (1\ 2)\ A_3$, and so on.
$\therefore A_3 \trianglelefteq S_3$.

E 2) For any $A \in GL_2(R)$ and $B \in SL_2(R)$,

$$\det(A^{-1}BA) = \det(A^{-1}) \det(B) \det(A)$$
$$= \frac{1}{\det(A)} \det(A), \text{ since } \det(B) = 1$$
$$= 1$$

$\therefore A^{-1}BA \in SL_2(R)$.
$\therefore SL_2(R) \trianglelefteq GL_2(R)$.

E 3) All, since this group is abelian.

E 4) Let $g \in G$ and $x \in Z(G)$. Then
$g^{-1}xg = g^{-1}gx$, since $x \in Z(G)$
$= x \in Z(G)$
$\therefore g^{-1}Z(G)g \subseteq Z(G)\ \forall\ g \in G$.
$\therefore Z(G) \trianglelefteq G$

E 5) Since $(1\ 2\ 3)^{-1}\ (2\ 3)\ (1\ 2\ 3) = (1\ 2) \notin <(2\ 3)>$, $<(2\ 3)> \not\trianglelefteq S_3$.

E 6) a) Take any element $hk \in HK$. Since $H \trianglelefteq G$, $k^{-1}hk \in H$. Let $k^{-1}hk = h_1$. Then $hk = kh_1 \in KH$.
$\therefore hk \in KH\ \forall\ hk \in HK$. $\therefore HK \subseteq KH$.
Again, for any $kh \in KH$, $khk^{-1} \in H$. Let $khk^{-1} = h_2$. Then $kh = h_2k \in HK$.
$\therefore kh \in HK\ \forall\ kh \in KH$.
$\therefore KH \subseteq HK$.

Thus, we have shown that $HK = KH$.
$\therefore$ $HK \leq G$.

b) From (a) we know that $HK \leq G$. To show that $HK \trianglelefteq G$, consider $g \in G$ and $hk \in HK$. Then
$g^{-1}hkg = g^{-1}h(gg^{-1})kg = (g^{-1}hg)(g^{-1}kg) \in HK$, since $H \trianglelefteq G$, $K \trianglelefteq G$.
$\therefore$ $g^{-1}HKg \subseteq HK \; \forall \; g \in G$.
$\therefore$ $HK \trianglelefteq G$.

E 7) D_6 is generated by x and y, where $x^2 = e$, $y^3 = e$ and $xy = y^{-1}x$.
$\therefore$ $D_6 = \{e, x, y, y^2, xy, xy^2\}$.

This is the group of symmetries of an equilateral triangle. Its generators are x and y, where x corresponds to the reflection about the altitude through a fixed vertex and y corresponds to a rotation about the centroid through 120° (see Fig. 2).

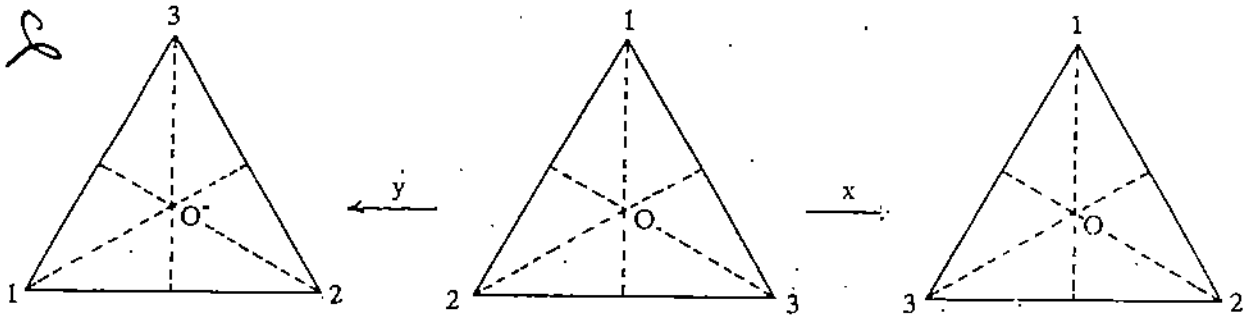


Fig. 2 : Generators of D_6

E 8) $G/\{e\} = \{\{e\}g \mid g \in G\} = \{\{g\} \mid g \in G\}$
$G/G = \{Gg \mid g \in G\} = \{G\}$, since $Gg = G \; \forall \; g \in G$.
So G/G consists of only one element, namely, the identity.

E 9) Let $G = \langle x \rangle$ and G/H be a quotient group of G. Any element of G/H is of the form $Hx^n = (Hx)^n$, since any element of G is of the form x^n. $\therefore$ $G/H = \langle Hx \rangle$.

E 10) For any two elements Hx and Hy in G/H,
$(Hx)(Hy) = Hxy = Hyx$, since G is abelian
$= (Hy)(Hx)$.
$\therefore$ G/H is abelian.

E 11) $D_8/K = \{K, Kx\}$. You can check that this is abelian. You have already seen that $xy \neq yx$. $\therefore$ D_8 is not abelian.

E 12) Since G is cyclic, it is abelian. $\therefore$ $[G, G] = \{e\}$

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

So, $H(1\ 2\ 3) = H(2\ 3)$ and $H(1\ 3\ 2) = H(1\ 3)$, but $H(1\ 2\ 3)(1\ 3\ 2) \neq H(2\ 3)(1\ 3)$.

UNIT 6 GROUP HOMOMORPHISMS

Structure

6.1 INTRODUCTION

So far in this course we have not discussed functions from one group to another. You may have wondered why we reviewed various aspects of functions in Unit 1. In this unit you will see why.

In Sec.6.2 we will discuss various properties of those functions between groups which preserve the algebraic structure of their domain groups. These functions are called group homomorphisms, a term introduced by the mathematician Klein in 1893. This concept is analogous to the concept of a vector space homomorphism, that you studied in the Linear Algebra course.

In Sec.6.3 we will introduce you to a very important mathematical idea, an isomorphism. You will see that an isomorphism is a bijective homomorphism. The importance of isomorphisms lies in the fact that two groups are isomorphic if and only if they have exactly the same algebraic properties.

In Sec.6.4 we will prove a very basic theorem of group theory, namely, the Fundamental Theorem of Homomorphism. We will also give some of its important consequences.

Finally, in Sec.6.5 we will discuss automorphisms, which are isomorphisms of a group onto itself. We shall look at the group of inner automorphisms in particular. This allows us to have an insight into the structure of the quotient group of G by its centre, for any group G.

Before starting this unit, we suggest that you go through Sec.1.5 and Unit 5.

Objectives

After reading this unit, you should be able to

- verify whether a function between groups is a homomorphism or not;
- obtain the kernel and image of any homomorphism;
- check whether a function between groups is an isomorphism or not;
- state, prove and apply the Fundamental Theorem of Homomorphism;
- prove that Inn G $\trianglelefteq$ Aut G and $G/Z(G) \simeq$ Inn G, for any group G.

6.2 HOMOMORPHISMS

Let us start our study of functions from one group to another with an example.

Consider the groups $(\mathbb{Z}, \cdot)$ and $(\{1, -1\}, .)$. If we define

$$f : \mathbb{Z} \to \{1, -1\} \text{ by } f(n) = \begin{cases} 1, \text{ if } n \text{ is even} \\ -1, \text{ if } n \text{ is odd,} \end{cases}$$

then you can see that $f(a + b) = f(a).f(b)\ \forall\ a, b \in \mathbb{Z}$. What we have just seen is an example of a homomorphism, a function that preserves the algebraic structure of its domain.

Definition : Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. A mapping $f : G_1 \longrightarrow G_2$ is said to be a **group homomorphism (or just a homomorphism)**, if

$f(x *_1 y) = f(x) *_2 f(y) \forall\ x, y \in G_1$.

Note that a homomorphism f from G_1 to G_2 carries the product $x *_1 y$ in G_1 to the product $f(x) *_2 f(y)$ in G_2.

The word 'homomorphism' is derived from the two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

Before discussing examples, let us define two sets related to a given homomorphism.

Definition : Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups and $f : G_1 \longrightarrow G_2$ be a homomorphism. Then we define

i) the **image of f** to be the set
$\text{Im } f = \{f(x) \mid x \in G_1\}$.

ii) the **kernel of f** to be the set
$\text{Ker } f = \{x \in G_1 \mid f(x) = e_2\}$, where e_2 is the identity of G_2.

Note that $\text{Im } f \subseteq G_2$, and $\text{Ker } f = f^{-1}(\{e_2\}) \subseteq G_1$.

Now let us consider some examples.

Example 1 : Consider the two groups $(\mathbf{R}, +)$ and $(\mathbf{R}^*, .)$. Show that the map $\exp : (\mathbf{R}, +) \longrightarrow (\mathbf{R}^*, .) : \exp(r) = e^r$ is a group homomorphism. Also find Im exp and Ker exp.

Solution : For any $r_1, r_2 \in \mathbf{R}$, we know that $e^{r_1 + r_2} = e^{r_1} . e^{r_2}$.
$\therefore \exp(r_1 + r_2) = \exp(r_1).\exp(r_2)$.

Hence, exp is a homomorphism from the additive group of real numbers to the multiplicative group of non-zero real numbers.

Now, $\text{Im exp} = \{\exp(r) \mid r \in \mathbf{R}\} = \{e^r \mid r \in \mathbf{R}\}$.
Also, $\text{Ker exp} = \{r \in \mathbf{R} \mid e^r = 1\} = \{0\}$.

Note that exp takes the identity 0 of R to the identity 1 of $\mathbf{R}^*$. exp also carries the additive inverse $-r$ of r to the multiplicative inverse of exp (r).

Example 2 : Consider the groups $(\mathbf{R}, +)$ and $(\mathbf{C}, +)$ and define $f : (\mathbf{C}, +) \longrightarrow (\mathbf{R}, +)$ by $f(x + iy) = x$, the real part of $x + iy$. Show that f is a homomorphism. What are Im f and Ker f ?

Solution : Take any two elements $a + ib$ and $c + id$ in C. Then,
$f((a + ib) + (c + id)) = f((a + c) + i(b + d)) = a + c = f(a + ib) + f(c + id)$
Therefore, f is a group homomorphism.
$\text{Im } f = \{ f(x + iy) \mid x, y \in \mathbf{R} \} = \{x \mid x \in \mathbf{R}\} = \mathbf{R}$.
So, f is a surjective function (see Sec.1.5).
$\text{Ker } f = \{ x + iy \in \mathbf{C} \mid f(x + iy) = 0 \} = \{ x + iy \in \mathbf{C} \mid x = 0 \}$
$= \{ iy \mid y \in \mathbf{R} \}$, the set of purely imaginary numbers.

Note that f carries the additive identity of C to the additive identity of R and $(-z)$ to $-f(z)$, for any $z \in \mathbf{C}$.

The following exercises will help you to see if you have understood what we have covered so far.

E 1) Show that $f : (\mathbf{R}^*, .) \longrightarrow (\mathbf{R}, +) : f(x) = \ln x$, the natural logarithm of x, is a group homomorphism. Find Ker f and Im f also.

E 2) Is $f : (GL_3(\mathbf{R}), .) \longrightarrow (\mathbf{R}^*, .) : f(A) = \det(A)$ a homomorphism? If so, obtain Ker f and Im f.

In Examples 1 and 2 we observed that the homomorphisms carried the identity to the identity and the inverse to the inverse. In fact, these observations can be proved for any group homomorphism.

Theorem 1 : Let $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ be a group homomorphism.

Then

a) $f(e_1) = e_2$, where e_1 is the identity of G_1 and e_2 is the identity of G_2.

b) $f(x^{-1}) = [f(x)]^{-1}$ for all x in G_1.

Proof : (a) Let $x \in G_1$. Then we have $e_1 *_1 x = x$. Hence,
$f(x) = f(e_1 *_1 x) = f(e_1) *_2 f(x)$, since f is a homomorphism. But
$f(x) = e_2 *_2 f(x)$ in G_2.
Thus, $f(e_1) *_2 f(x) = e_2 *_2 f(x)$.

So, by the right cancellation law in G_2, $f(e_1) = e_2$.

(b) Now, for any $x \in G_1$, $f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2$.

Similarly, $f(x^{-1}) *_2 f(x) = e_2$.

Hence, $f(x^{-1}) = [f(x)]^{-1} \forall\ x \in G_1$.

Note that the converse of Theorem 1 is false. That is, if $f : G_1 \longrightarrow G_2$ is a function such that $f(e_1) = e_2$ and $[f(x)]^{-1} = f(x^{-1}) \forall\ x \in G_1$, then f need not be a homomorphism. For example, consider $f : \mathbf{Z} \longrightarrow \mathbf{Z} : f(0) = 0$ and

$$f(n) = \begin{cases} n + 1 \forall\ n > 0 \\ n - 1 \forall\ n < 0. \end{cases}$$

Since $f(1 + 1) \neq f(1) + f(1)$, f is not a homomorphism. But $f(e_1) = e_2$ and
$f(n) = -f(-n) \forall\ n \in \mathbf{Z}$.

Let us look at a few more examples of homomorphisms now. We can get one important class of homomorphisms from quotient groups.

Example 3 : Let $H \triangleq G$. Consider the map $p : G \longrightarrow G/H : p(x) = Hx$. Show that p is a homomorphism. (p is called the **natural** or **canonical** group homomorphism.) Also show that p is onto. What is Ker p?

Solution : For $x, y \in G$, $p(xy) = Hxy = Hx\ Hy = p(x)\ p(y)$. Therefore, p is a homomorphism.

Now, Im $p = \{ p(x) \mid x \in G \} = \{ Hx \mid x \in G \} = G/H$. Therefore, p is onto.
Ker $p = \{ x \in G \mid p(x) = H \}$. (Remember, H is the identity of G/H.)
$= \{ x \in G \mid Hx = H \}$
$= \{ x \in G \mid x \in H \}$, by Theorem 1 of Unit 4.
$= H$.

In this example you can see that Ker $p \triangleq G$. You can also check that Theorem 1 is true here.

Before looking at more examples try the following exercises.

E 3) Define the natural homomorphism p from S_3 to S_3/A_3. Does $(1\ 2) \in$ Ker p? Does $(1\ 2) \in$ Im p?

E 4) Let $S = \{ z \in \mathbf{C} \mid |z| = 1 \}$ (see Example 1 of Unit 3).

Define $f : (\mathbf{R}, +) \longrightarrow (S, .) : f(x) = e^{2\pi i x}$, where n is a fixed positive integer. Is f a homomorphism? If so, find Ker f.

E 5) Let G be a group and $H \triangleq G$. Show that there exists a group G_1 and a homomorphism $f : G \longrightarrow G_1$ such that Ker $f = H$.

(Hint : Does Example 3 help?)

Another class of examples of homomorphisms concerns the inclusion map.

Example 4 : Let H be a subgroup of a group G. Show that the map $i : H \longrightarrow G$, $i(h) = h$ is a homomorphism. This function is called the **inclusion map**.

Solution : Since $i(h_1h_2) = h_1h_2 = i(h_1)i(h_2) \forall\ h_1, h_2 \in H$, i is a group homomorphism.

Let us briefly look at the inclusion map in the context of symmetric groups. Consider two natural numbers m and n, where $m \leq n$.

Then, we can consider $S_m \leq S_n$, where any $\sigma \in S_m$, written as

σ is the Greek letter sigma.

$\begin{pmatrix} 1 & 2 & \ldots & m \\ \sigma(1) & \sigma(2) & \ldots & \sigma(m) \end{pmatrix}$, is considered to be the same as

$\begin{pmatrix} 1 & 2 & \ldots & m & m+1 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(m) & m+1 & \ldots & n \end{pmatrix} \in S_n$, i.e., $\sigma(k) = k$ for $m + 1 \leq k \leq n$.

Then we can define an inclusion map $i : S_m \longrightarrow S_n$.

For example, under $i : S_3 \longrightarrow S_4$, $(1\ 2)$ goes to $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$.

Try this exercise now.

E 6) What are the kernel and image of the inclusion map $i : 3\mathbb{Z} \longrightarrow \mathbb{Z}$?

We will now prove some results about homomorphisms. Henceforth, for convenience, we shall drop the notation for the binary operation, and write $a * b$ as ab.

Now let us look at the composition of two homomorphisms. Is it a homomorphism? Let us see.

Theorem 2 : If $f : G_1 \longrightarrow G_2$ and $g : G_2 \longrightarrow G_3$ are two group homomorphisms, then the composite map $g \circ f : G_1 \longrightarrow G_3$ is also a group homomorphism.

Proof : Let $x, y \in G_1$. Then

$g \circ f(xy) = g(f(xy))$

$= g(f(x)f(y))$, since f is a homomorphism.

$= g(f(x))\, g(f(y))$, since g is a homomorphism.

$= g \circ f(x).g \circ f(y)$.

Thus, $g \circ f$ is a homomorphism.

Now, using Theorem 2, try and solve the following exercise.

E 7) Let $n \in \mathbb{N}$. Show that the composition of $f : \mathbb{Z} \longrightarrow \mathbb{Z} : f(x) = nx$ and $g : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : g(x) = \bar{x}$ is a homomorphism. What are $\text{Ker}(g \circ f)$ and $\text{Im}(g \circ f)$?

So far you have seen that the kernel and image of a homomorphism are sets. In the examples we have discussed so far you may have noticed that they are subgroups. We will now prove that the kernel of a homomorphism is a normal subgroup, and the image is a subgroup.

Theorem 3 : Let $f : G_1 \longrightarrow G_2$ be a group homomorphism. Then

a) Ker f is a normal subgroup of G_1.

b) Im f is a subgroup of G_2.

Proof : a) Since $f(e_1) = e_2$, $e_1 \in \text{Ker } f$. $\therefore \text{Ker } f \neq \phi$.

Now, if $x, y \in \text{Ker } f$, then $f(x) = e_2$ and $f(y) = e_2$.

$\therefore f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\, [f(y)]^{-1} = e_2$.

$\therefore xy^{-1} \in \text{Ker } f$.

Therefore, by Theorem 1 of Unit 3, $\text{Ker } f < G_1$. Now, for any $y \in G_1$ and $x \in \text{Ker } f$,

$f(y^{-1}xy) = f(y^{-1})\, f(x) f(y)$

$= [f(y)]^{-1} e_2 f(y)$, since $f(x) = e_2$ and by Theorem 1.

$= e_2$.

$\therefore \text{Ker } f \trianglelefteq G_1$.

b) $\text{Im } f \neq \phi$, since $f(e_1) \in \text{Im } f$.

Now, let $x_2, y_2 \in \text{Im } f$. Then $\exists\, x_1, y_1 \in G_1$ such that $f(x_1) = x_2$ and $f(y_1) = y_2$.

$\therefore x_2 y_2^{-1} = f(x_1)\, f(y_1^{-1}) = f(x_1 y_1^{-1}) \in \text{Im } f$.

$\therefore \text{Im } f \leq G_2$.

Using this result, from Example 2 we can immediately see that the set of purely imaginary numbers is a normal subgroup of $\mathbb{C}$.

Let us also consider another example, which is a particular case of E 4 (when n = 1).

Consider $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, .) : \phi(x) = \cos x + i \sin x$. We have seen that $\phi(x + y) = \phi(x)\phi(y)$, that is, ϕ is a group homomorphism. Now $\phi(x) = 1$ iff $x = 2\pi n$ for some $n \in \mathbb{Z}$. Thus, by Theorem 3, Ker $\phi = \{2\pi n \mid n \in \mathbb{Z}\}$ is a normal subgroup of $(\mathbb{R}, +)$. Note that this is cyclic, and 2π is a generator.

Similarly, Im ϕ is a subgroup of $\mathbb{C}^*$. This consists of all the complex numbers with absolute value 1, i.e., the complex numbers on the circle with radius 1 unit and centre (0, 0).

You may have noticed that sometimes the kernel of a homomorphism is {e} (as in Example 1), and sometimes it is a large subgroup (as in Example 2). Does the size of the kernel indicate anything? We will prove that a homomorphism is 1-1 iff its kernel is {e}.

Theorem 4 : Let $f : G_1 \longrightarrow G_2$ be a group homomorphism. Then f is injective iff Ker $f = \{e_1\}$, where e_1 is the identity element of the group G_1.

Proof : Firstly, assume that f is injective. Let $x \in$ Ker f. Then $f(x) = e_2$, i.e., $f(x) = f(e_1)$. But f is 1-1. $\therefore x = e_1$.

Thus, Ker $f = \{e_1\}$.

Conversely, suppose Ker $f = \{e_1\}$. Let $x, y \in G_1$ such that $f(x) = f(y)$. Then
$$f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\,[f(y)]^{-1} = e_2.$$
$\therefore xy^{-1} \in$ Ker $f = \{e_1\}$. $\therefore xy^{-1} = e_1$ and $x = y$.
This shows that f is injective.

So, by using Theorem 4 and Example 4, we can immediately say that any inclusion $i : H \longrightarrow G$ is 1-1, since Ker $i = \{e\}$.

Let us consider another example.

Example 5 : Consider the group T of translations of $\mathbb{R}^2$ (Example 6, Unit 2). We define a map $\phi : (\mathbb{R}^2, +) \longrightarrow (T, o)$ by $\phi(a, b) = f_{a,b}$. Show that ϕ is an onto homomorphism, which is also 1-1.

Solution : For (a, b), (c, d) in $\mathbb{R}^2$, we have seen that
$f_{a+c,b+d} = f_{a,b} \circ f_{c,d}$
$\therefore \phi((a, b) + (c, d)) = \phi(a, b) \circ \phi(c, d)$.

Thus, ϕ is a homomorphism of groups.

Now, any element of T is $f_{a,b} = \phi(a, b)$. Therefore, ϕ is surjective. We now show that ϕ is also injective.

Let $(a, b) \in$ Ker ϕ. Then $\phi(a, b) = f_{0,0}$,
i.e., $f_{a,b} = f_{0,0}$
$\therefore f_{a,b}(0, 0) = f_{0,0}(0, 0)$,
i.e., $(a, b) = (0, 0)$
$\therefore$ Ker $\phi = \{(0, 0)\}$
$\therefore \phi$ is 1-1.

So we have proved that ϕ is a homomorphism, which is bijective.

Try the following exercise now.

E 8) For any $n \geq 1$, consider Z_n and U_n (the group of nth roots of unity discussed in Example 5 of Unit 3). Let ω denote an nth root of unity that generates U_n. Then $U_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. Now, consider the map $f : Z_n \longrightarrow U_n : f(\bar{j}) = \omega^j$. Show that f is a group homomorphism. Is f 1-1? Is f surjective?

And now let us look at a very useful property of a homomorphism that is surjective

Theorem 5 : If $f : G_1 \longrightarrow G_2$ is an onto group homomorphism and S is a subset that generates G_1, then $f(S)$ generates G_2.

Proof : We know that

$G_1 = < S > = \{ x_1^{r_1} x_2^{r_2} \ldots x_m^{r_m} \mid m \in N, x_i \in S, r_i \in Z \text{ for all } i\}$. We will show that $G_2 = < f(S) >$.

Let $x \in G_2$. Since f is surjective, there exists $y \in G_1$ such that $f(y) = x$. Since $y \in G_1$, $y = x_1^{r_1} \ldots x_m^{r_m}$, for some $m \in N$, where $x_i \in S$ and $r_i \in Z$, $1 \leq i \leq m$.

Thus, $x = f(y) = f(x_1^{r_1} \ldots x_m^{r_m})$

$= (f(x_1))^{r_1} \ldots (f(x_m))^{r_m}$, since f is a homomorphism.

$\Longrightarrow x \in < f(S) >$, since $f(x_i) \in f(S)$ for every $i = 1, 2, \ldots, r$.

Thus, $G_2 = < f(S) >$.

In the following exercise we present an important property of cyclic groups which you can prove by using Theorem 5.

E 9) Show that the homomorphic image of a cyclic group is cyclic, i.e., if G is a cyclic group and $f : G \longrightarrow G'$ is a homomorphism, then $f(G)$ is cyclic.

Once you have solved E 9, you can immediately say that any quotient group of a cyclic group is cyclic.

So far you have seen examples of various kinds of homomorphisms—injective, surjective and bijective. Let us now look at bijective homomorphisms in particular.

6.3 ISOMORPHISMS

In this section we will discuss homomorphisms that are 1-1 and onto. We start with some definitions.

Definitions : Let G_1 and G_2 be two groups. A homomorphism $f : G_1 \longrightarrow G_2$ is called an **isomorphism** if f is 1-1 and onto.

In this case we say that the group G_1 is isomorphic to the group G_2 or G_1 and G_2 are isomorphic. We denote this fact by $G_1 \simeq G_2$.

The word 'isomorphisms' is derived from the Greek word 'isos' meaning 'equal'.

An isomorphism of a group G onto itself is called an automorphism of G. For example, the identity funtion $I_G : G \longrightarrow G : I_G(x) = x$ is an automorphism.

Let us look at another example of an isomorphism.

Example 6 : Consider the set $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in R \right\}$.

Then G is a group with respect to matrix addition.

Show that $f : G \longrightarrow C : f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$ is an isomorphism.

Solution : Let us first verify that f is a homomorphism. Now, for any two elements $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ in G,

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = f\left(\begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}\right) = (a+c) + i(b+d)$$

$$= (a + ib) + (c + id)$$

$$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$$

Therefore, f is a homomorphism.

Now, $\text{Ker } f = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a + ib = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a = 0, b = 0 \right\} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$.

Therefore, by Theorem 4, f is 1-1.

Finally, since Im f = C, f is surjective.

Therefore, f is an isomorphism.

We would like to make an important remark now.

Remark : If G_1 and G_2 are isomorphic groups, they must have the same algebraic structure and satisfy the same algebraic properties. For example, any group isomorphic to a finite group must be finite and of the same order. Thus, two isomorphic groups are algebraically indistinguishable systems.

The following result is one of the consequences of isomorphic groups being algebraically alike.

Theorem 6 : If $f : G \longrightarrow H$ is a group isomorphism and $x \in G$, then $< x > \simeq < f(x) >$. Therefore,

i) if x is of finite order, then $o(x) = o(f(x))$.

ii) if x is of infinite order, so is f(x).

Proof : If we restrict f to any subgroup K of G, we have the function $f|_K : K \longrightarrow f(K)$. Since f is bijective, so is its restriction $f|_K$. $\therefore K \simeq f(K)$ for any subgroup K of G. In particular, for any $x \in G$, $< x > \simeq f(< x >) = < f(x) >$, by E 9.

Now if x has finite order, then $o(x) = o(< x >) = o(< f(x) >) = o(f(x))$, proving (i).

To prove (ii) assume that x is of infinite order. Then $< x >$ is an infinite group. Therefore, $< f(x) >$ is an infinite group, and hence, f(x) is of infinite order. So, we have proved (ii).

Try the following exercises now.

E 10) Show that $Z \simeq nZ$, for a fixed integer n.
(Hint : Consider $f : (Z, +) \longrightarrow (nZ, +) : f(k) = nk$.)

E 11) Is $f : Z \longrightarrow Z : f(x) = 0$ a homomorphism? an isomorphism?

The next two exercises involve general properties of an isomorphism. E 12 is the isomorphism analogue of Theorem 2. E 13 gives us another example to support the fact that isomorphic groups have the same algebraic properties.

E 12) If $\phi : G \longrightarrow H$ and $\theta : H \longrightarrow K$ are two isomorphisms of groups, then show that $\theta \circ \phi$ is an isomorphism of G onto K.

E 13) If $f : G \longrightarrow H$ is an isomorphism of groups and G is abelian, then show that H is also abelian.

So far we have seen examples of isomorphic groups. Now consider the following example.

Example 7 : Show that $(R^*, .)$ is not isomorphic to $(C^*, .)$.

Solution : Suppose they are isomorphic, and $f : C^* \longrightarrow R^*$ is an isomorphism. Then

$o(i) = o(f(i))$, by Theorem 6. Now $o(i) = 4$. $\therefore o(f(i)) = 4$.

However, the order of any real number different from ± 1 is infinite; and $o(1) = 1$, $o(-1) = 2$.

So we reach a contradiction. Therefore, our supposition must be wrong. That is, R^* and C^* are not isomorphic.

Try these exercises now.

E 14) Show that $(\mathbb{C}^*, .)$ is not isomorphic to $(\mathbb{R}, +)$.

E 15) Is $\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$, for any $n \neq 1$?

You must have noticed that the definition of an isomorphism just says that the map is bijective, i.e., the inverse map exists. It does not tell us any properties of the inverse. The next result does so.

Theorem 7 : If $f : G_1 \longrightarrow G_2$ is an isomorphism of groups, then $f^{-1} : G_2 \longrightarrow G_1$ is also an isomorphism.

Proof : From Unit 1 you know that f^{-1} is bijective. So, we only need to show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ and $a = f^{-1}(a')$, $b = f^{-1}(b')$. Then $f(a) = a'$ and $f(b) = b'$. Therefore, $f(ab) = f(a)\,f(b) = a'b'$. On applying f^{-1}, we get
$f^{-1}(a'b') = ab = f^{-1}(a')\,f^{-1}(b')$. Thus,
$f^{-1}(a'b') = f^{-1}(a')\,f^{-1}(b')$ for all $a', b' \in G_2$.

Hence, f^{-1} is an isomorphism.

From Example 5 and Theorem 7 we can immediately say that
$\phi^{-1} : T \longrightarrow \mathbb{R}^2 : \phi^{-1}(f_{a,b}) = (a, b)$ is an isomorphism.

Theorem 7 says that if $G_1 \simeq G_2$, then $G_2 \simeq G_1$. We will be using this result quite often (e.g., while proving Theorem 9)

Let us now look at a very important theorem in group theory. In Block 3 you will study its analogue in ring theory and in the Linear Algebra course you have already studied its analogue for linear transformations.

6.4 THE ISOMORPHISM THEOREMS

In this section we shall prove some results about the relationship between homomorphisms and quotient groups. The first result is the Fundamental Theorem of Homomorphism for groups. It is called 'fundamental' because a lot of group theory depends upon this result. This result is also called the first isomorphism theorem.

Theorem 8 (Fundamental Theorem of Homomorphism) Let G_1 and G_2 be two groups and $f : G_1 \longrightarrow G_2$ be a group homomorphism. Then
$G_1/\text{Ker } f \simeq \text{Im } f$.

In particular, if f is onto, then $G_1/\text{Ker } f \simeq G_2$.

Proof : Let Ker $f = H$. Note that $H \trianglelefteq G_1$. Let us define the function
$\psi : G_1/H \longrightarrow \text{Im } f : \psi(Hx) = f(x)$.

At first glance it seems that the definition of ψ depends on the coset representative. But we will show that if $x, y \in G_1$ such that $Hx = Hy$, then $\psi(Hx) = \psi(Hy)$. This will prove that ψ is a well-defined function.

Now, $Hx = Hy \Rightarrow xy^{-1} \in H = \text{Ker } f \Rightarrow f(xy^{-1}) = e_2$, the identity of G_2
$\Rightarrow f(x)[f(y)]^{-1} = e_2 \Rightarrow f(x) = f(y)$.
$\Rightarrow \psi(Hx) = \psi(Hy)$

Therefore, ψ is a well-defined function.

Now, let us check that ψ is a homomorphism. For $Hx, Hy \in G_1/H$,
$\psi((Hx)(Hy)) = \psi(Hxy)$
$= f(xy)$
$= f(x)\,f(y)$, since f is a homomorphism.
$= \psi(Hx)\,\psi(Hy)$

Therefore, ψ is a group homomorphism.

Next, let us see whether ψ is bijective or not.

Now, $\psi(Hx) = \psi(Hy)$ for Hx, Hy in G_1/H
$\Rightarrow f(x) = f(y)$
$\Rightarrow f(x)\,[f(y)]^{-1} = e_2$
$\Rightarrow f(xy^{-1}) = e_2$
$\Rightarrow xy^{-1} \in \text{Ker } f = H.$
$\Rightarrow Hx = Hy$

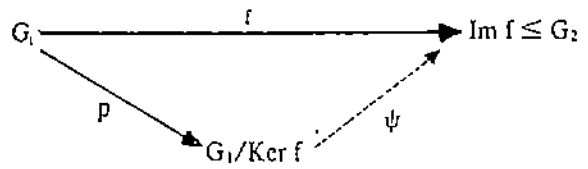
Thus, ψ is 1-1.

Also, any element of Im f is $f(x) = \psi(Hx)$, where $x \in G_1$.
$\therefore$ Im ψ = Im f.

So, we have proved that ψ is bijective, and hence, an isomorphism. Thus, $G_1/\text{Ker } f \simeq \text{Im } f$.

Now, if f is surjective, Im $f = G_2$. Thus, in this case $G_1/\text{Ker } f \simeq G_2$.

The situation in Theorem 8 can be shown in the following diagram.



Here, p is the natural homomorphism (see Example 3).

The diagram says that if you first apply p, and then ψ, to the elements of G_1, it is the same as applying f to them. That is,

$\psi \circ p = f$.

Also, note that Theorem 8 says that two elements of G_1 have the same image under f iff they belong to the same coset of Ker f.

Let us look at a few examples.

One of the simplest situations we can consider is $I_G : G \longrightarrow G$. On applying Theorem 8 here, we see that $G/\{e\} \simeq G$. We will be using this identification of $G/\{e\}$ and G quite often.

Now for some non-trivial examples.

Example 8 : Prove that $C/R \simeq R$.

Solution : Define $f : C \longrightarrow R : f(a + ib) = b$. Then f is a homomorphism, Ker $f = R$ and Im $f = R$. Therefore, on applying Theorem 8 we see that $C/R \simeq R$.

Example 9 : Consider $f : Z \longrightarrow (\{1, -1\}, .) : f(n) = \begin{cases} 1, \text{ if n is even} \\ -1, \text{ if n is odd.} \end{cases}$

At the beginning of Sec.6.2, you saw that f is a homomorphism. Obtain Ker f and Im f. What does Theorem 8 say in this case?

Solution : Let Z_e and Z_o denote the set of even and odd integers, respectively. Then

Ker $f = \{ n \in Z \mid f(n) = 1 \} = Z_e$.
Im $f = \{ f(n) \mid n \in Z \} = \{ 1, -1 \}$
Thus, by Theorem 8, $Z/Z_e \simeq \{ 1, -1 \}$.

This also tells us that $o(Z/Z_e) = 2$. The two cosets of Z_e in Z are Z_e and Z_o.
$\therefore \{ Z_e, Z_o \} \simeq \{ 1, -1 \}$.

Example 10 : Show that $GL_2(R)/SL_2(R) \simeq R^*$, where
$SL_2(R) = \{A \in GL_2(R) \mid \det(A) = 1 \}$.

Solution : We know that the function
$f : GL_2(R) \longrightarrow R^* : f(A) = \det(A)$ is a homomorphism. Now, Ker $f = SL_2(R)$.

Also, Im $f = R^*$, since any $r \in R^*$ can be written as $\det\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}\right)$.

Thus, using Theorem 8, $GL_2(R)/SL_2(R) \simeq R^*$.

Try the following exercises now.

E 16) Consider the situation in Example 1. Show that $(R, +) \simeq (R^*_+)$, the group of positive real numbers.

E 17) Let U_4 be the multiplicative group of 4th roots of unity.
Define $f : Z \longrightarrow U_4 : f(n) = i^n$. Use Theorem 8 to show that $Z_4 \simeq U_4$. ($i = \sqrt{-1}$.)

Now we will use the Fundamental Theorem of Homomorphism to prove a very important result which classifies all cyclic groups.

Theorem 9 : Any cyclic group is isomorphic to $(Z, +)$ or $(Z_n, +)$.

Proof : Let $G = \langle x \rangle$ be a cyclic group. Define
$f : Z \longrightarrow G : f(n) = x^n$.
f is a homomorphism because
$f(n + m) = x^{n+m} = x^n . x^m = f(n) f(m)$.

Also note that Im $f = G$.

Now, we have two possibilities for Ker f — Ker $f = \{0\}$ or Ker $f \neq \{0\}$.
Case 1 (Ker $f = \{0\}$) : In this case f is 1-1. Therefore, f is an isomorphism. Therefore, by Theorem 7, f^{-1} is an isomorphism. That is, $G \simeq (Z, +)$.

Case 2 (Ker $f \neq \{0\}$) : Since Ker $f \leq Z$, from Example 4 of Unit 3 we know that Ker $f = nZ$, for some $n \in N$. Therefore, by the Fundamental Theorem of Homomorphism, $Z/nZ \simeq G$.

$\therefore G \simeq Z/nZ = (Z_n, +)$.

Over here note that since $\langle x \rangle \simeq Z_n$, $o(x) = n$. So, a finite cyclic group is isomorphic to Z_n, where n is the order of the group.

Using Theorem 9 we know that all cyclic groups of order 4 are isomorphic, since they are all isomorphic to Z_4. Similarly, all infinite cyclic groups are isomorphic.

And now you can prove the following nice result.

E 18) Let S be the circle group $\{ z \in C \mid |z| = 1 \}$. Show that $R/Z \simeq S$.
(Hint : Define $f: R \longrightarrow S : f(x) = e^{2\pi i x}$. Show that f is an onto homomorphism and Ker $f = Z$.)

We will now prove the second isomorphism theorem with the help of the Fundamental Theorem of Homomorphism. It is concerned with intersections and products of subgroups. To prove the theorem you will need the results given in the following exercise. So why not do this exercise first!

E 19) Let G be a group, $H \leq G$ and $K \trianglelefteq G$. Then

a) $H \cap K \trianglelefteq H$; and

b) if $A \leq G$ such that $K \subseteq A$, then $K \trianglelefteq A$.

Now let us discuss the theorem.

Theorem 10 : If H and K are subgroups of a group G, with K normal in G, then $H/(H \cap K) \simeq (HK)/K$.

Proof : We must first verify that the quotient groups $H/(H \cap K)$ and $(HK)/K$ are well-defined. From E 19 you know that $H \cap K \trianglelefteq H$. From E 6 of Unit 5 you know that $HK \leq G$. Again, from E 19 you know that $K \trianglelefteq HK$. Thus the given quotient groups are meaningful.

Now, what we want to do is to find an onto homomorphism $f : H \longrightarrow (HK)/K$ with kernel $H \cap K$. Then we can apply the Fundamental Theorem of Homomorphism and get the result. We define $f : H \longrightarrow (HK)/K : f(h) = hK$.

Now, for $x, y \in H$,
$f(xy) = xyK = (xK)(yK) = f(x)\,f(y)$.

Therefore, f is a homomorphism.

$\text{Im } f = \{ f(h) \mid h \in H \} = \{ hK \mid h \in H \}$.

We will show that $\text{Im } f = (HK)/K$. Now, take any element $hK \in \text{Im } f$. Since $h \in H$, $h \in HK$.
$\therefore hK \in (HK)/K$. $\therefore \text{Im } f \subseteq (HK)/K$. On the other hand, any element of $(HK)/K$ is
$hkK = hK$, since $k \in K$.
$\therefore hkK \in \text{Im } f$. $\therefore (HK)/K \subseteq \text{Im } f$.
$\therefore \text{Im } f = (HK)/K$.

Finally, $\text{Ker } f = \{ h \in H \mid f(h) = K \} = \{ h \in H \mid hK = K \}$
$= \{ h \in H \mid h \in K \}$
$= H \cap K$.

Thus, on applying the Fundamental Theorem, we get $H/(H \cap K) \simeq (HK)/K$

We would like to make a remark here.

Remark : If H and K are subgroups of $(G, +)$, then Theorem 10 says that

$(H + K)/K \simeq H/H \cap K$.

Now you can use Theorem 10 to solve the following exercises.

E 20) Let H and K be subgroups of a finite group G, and $H \trianglelefteq G$. Show that

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}$$

E 21) Show that $3\mathbb{Z}/12\mathbb{Z} \simeq Z_4$.
(**Hint :** Take $H = 3\mathbb{Z}$, $K = 4\mathbb{Z}$).

And now for the third isomorphism theorem. This is also a corollary to Theorem 8.

Theorem 11 : Let H and K be normal subgroups of a group G such that $K \subseteq H$. Then

$(G/K)/(H/K) \simeq G/H$.

Proof : We will define a homomorphism from G/K onto G/H, whose kernel will turn out to be H/K.

Consider $f : G/K \longrightarrow G/H : f(Kx) = Hx$. f is well-defined because $Kx = Ky$ for $x, y \in G$
$\Longrightarrow xy^{-1} \in K \subseteq H \Longrightarrow xy^{-1} \in H \Longrightarrow Hx = Hy \Longrightarrow f(Kx) = f(Ky)$

Now we leave the rest of the proof to you (see the following exercise).

E 22) Show that f is an onto homomorphism and $\text{Ker } f = H/K$.

Let us now look at isomorphisms of a group onto itself.

6.5 AUTOMORPHISMS

In this section we will first show that the set of all automorphisms of a group forms a group. Then we shall define a special subgroup of this group.

Let G be a group. Consider

Aut G = { f : G ⟶ G | f is an isomorphism }.

You have already seen that the identity map $I_G \in$ Aut G. From E 12 you know that Aut G is closed under the binary operation of composition. Also, Theorem 7 says that if $f \in$ Aut G, then $f^{-1} \in$ Aut G. We summarise this discussion in the following theorem.

Theorem 12 : Let G be a group. Then Aut G, the set of automorphisms of G, is a group.

Let us look at an example of Aut G.

Example 11 : Show that Aut $\mathbf{Z} \simeq \mathbf{Z}_2$.

Solution : Let $f : \mathbf{Z} \longrightarrow \mathbf{Z}$ be an automorphism. Let $f(1) = n$. We will show that $n = 1$ or -1. Since f is onto and $1 \in \mathbf{Z}$, $\exists\ m \in \mathbf{Z}$ such that $f(m) = 1$, i.e., $mf(1) = 1$, i.e., $mn = 1$.
$\therefore\ n = 1$ or $n = -1$.
Thus, there are only two elements in Aut Z, I and $-I$.
So Aut $\mathbf{Z} = \langle -I \rangle \simeq \mathbf{Z}_2$.

Now, given an element of a group G, we will define an automorphism of G corresponding to it.

Consider a fixed element $g \in G$. Define
$f_g : G \longrightarrow G : f_g(x) = gxg^{-1}$.

We will show that f_g is an automorphism of G.

i) f_g is a homomorphism : If $x, y \in G$, then
$f_g(xy) = g(xy)\,g^{-1}$
$= gx(e)\,yg^{-1}$, where e is the identity of G.
$= gx(g^{-1}g)\,yg^{-1}$
$= (gxg^{-1})\,(gyg^{-1})$
$= f_g(x)\,f_g(y)$.

ii) f_g is 1-1 : For $x, y \in G$, $f_g(x) = f_g(y) \implies gxg^{-1} = gyg^{-1} \implies x = y$, by the cancellation laws in G.

iii) f_g is onto : If $y \in G$, then
$y = (gg^{-1})\,y\,(gg^{-1})$
$= g(g^{-1}yg)\,g^{-1}$
$= f_g(g^{-1}yg) \in \text{Im } f_g$.

Thus, f_g is an automorphism of G. We give this automorphism a special name.

Definition : f_g is called an **inner automorphism** of G induced by the element g in G. The subset of Aut G consisting of all inner automorphism of G is denoted by Inn G.

For example, consider S_3. Let us compute $f_g(I)$, $f_g(1\ 3)$ and $f_g(1\ 2\ 3)$, where $g = (1\ 2)$. Note that $g^{-1} = (1\ 2) = g$.
Now, $f_g(I) = g \circ I \circ g^{-1} = I$.
$f_g(1\ 3) = (1\ 2)\,(1\ 3)\,(1\ 2) = (2\ 3)$.
$f_g(1\ 2\ 3) = (1\ 2)\,(1\ 2\ 3)\,(1\ 2) = (1\ 3\ 2)$.

The following exercise will give you some practice in obtaining inner automorphisms.

E 23) Obtain the image of $f_g \in$ Inn G, where

a) $G = GL_2(R)$ and $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

b) $G = Z$ and $g = 3$.

c) $G = Z/5Z$ and $g = \bar{4}$.

You will now see that Inn G is a normal subgroup of Aut G.

Theorem 13 : Let G be a group. Then Inn G is a normal subgroup of Aut G.

Proof : Inn G is non-empty, because $I_G = f_e \in$ Inn G, where e is the identity in G

Now, let us see if $f_g \circ f_h \in \text{Inn } G$ for $g, h \in G$.

For any $x \in G$, $f_g \circ f_h(x) = f_g(hxh^{-1})$
$= g(hxh^{-1})\, g^{-1}$
$= (gh)\, x\, (gh)^{-1}$
$= f_{gh}(x)$

Thus, $f_{gh} = f_g \circ f_h$, i.e., Inn G is closed under composition. Also $f_e = I_G$ belongs to Inn G.

Now, for $f_g \in \text{Inn } G$, $\exists\ f_{g^{-1}} \in \text{Inn } G$ such that

$f_g \circ f_{g^{-1}} = f_{gg^{-1}} = f_e = I_G$. Similarly, $f_{g^{-1}} \circ f_g = I_G$.

Thus, $f_{g^{-1}} = (f_g)^{-1}$. That is, every element of Inn G has an inverse in Inn G.

This proves that Inn G is a subgroup of Aut G.

Now, to prove that Inn G $\trianglelefteq$ Aut G, let $\phi \in \text{Aut } G$ and $f_g \in \text{Inn } G$. Then, for any $x \in G$

$\phi^{-1} \circ f_g \circ \phi(x) = \phi^{-1} \circ f_g(\phi(x))$
$= \phi^{-1}(g\phi(x)g^{-1})$
$= \phi^{-1}(g)\, \phi^{-1}(\phi(x))\, \phi^{-1}(g^{-1})$
$= \phi^{-1}(g)\, x[\phi^{-1}(g)]^{-1}$
$= f_{\phi^{-1}(g)}(x)$. (Note that $\phi^{-1}(g) \in G$.)

$\therefore\ \phi^{-1} \circ f_g \circ \phi = f_{\phi^{-1}(g)} \in \text{Inn } G\ \forall\ \phi \in \text{Aut } G$ and $f_g \in \text{Inn } G$.

$\therefore$ Inn G $\trianglelefteq$ Aut G.

Now for some exercises! From E 23 you may have already got a hint of the useful result that we give in E 24.

E 24) Show that a group G is commutative iff Inn G = $\{I_G\}$.

E 25) Show that if $x \in G$ such that $f_g(x) = x\ \forall\ g \in G$, then $\langle x \rangle \trianglelefteq G$.

Now we will prove an interesting result which relates the cosets of the centre of a group G to Inn G. Recall that the centre of G, $Z(G) = \{ x \in G \mid xg = gx\ \forall\ g \in G \}$.

Theorem 14 : Let G be a group. Then $G/Z(G) \simeq \text{Inn } G$.

Proof : As usual, we will use the powerful Fundamental Theorem of Homomorphism to prove this result.

We define $f : G \longrightarrow \text{Aut } G : f(g) = f_g$.

Firstly, f is a homomorphism because for $g, h \in G$,
$f(gh) = f_{gh}$
$= f_g \circ f_h$ (see proof of Theorem 13)
$= f(g) \circ f(h)$.

Next, $\text{Im } f = \{ f_g \mid g \in G \} = \text{Inn } G$.

Finally, $\text{Ker } f = \{ g \in G \mid f_g = I_G \}$
$= \{ g \in G \mid f_g(x) = x\ \forall\ x \in G \}$
$= \{ g \in G \mid gxg^{-1} = x\ \forall\ x \in G \}$
$= \{ g \in G \mid gx = xg\ \forall\ x \in G \}$
$= Z(G)$.

Therefore, by the Fundamental Theorem,
$G/Z(G) \simeq \text{Inn } G$.

Now you can use Theorem 14 to solve the next exercise.

E 26) Show that $S_3 \simeq \text{Inn } S_3$.

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

6.6 SUMMARY

In this unit we have covered the following points.

1. The definition and example of a group homomorphism.
2. Let $f : G_1 \longrightarrow G_2$ be a group homomorphism. Then $f(e_1) = e_2$, $[f(x)]^{-1} = f(x^{-1})$, $\text{Im } f \leq G_2$, $\text{Ker } f \trianglelefteq G_1$.
3. A homomorphism is 1-1 iff its kernel is the trivial subgroup.
4. The definition and examples of a group isomorphism.
5. Two groups are isomorphic iff they have exactly the same algebraic structure.
6. The composition of group homomorphisms (isomorphisms) is a group homomorphism (isomorphism).
7. The proof of the Fundamental Theorem of Homomorphism, which says that if $f : G_1 \longrightarrow G_2$ is a group homomorphism, then $G_1/\text{Ker } f \simeq \text{Im } f$.
8. Any infinite cyclic group is isomorphic to $(\mathbf{Z}, +)$. Any finite cyclic group of order n is isomorphic to $(\mathbf{Z}_n, +)$.
9. Let G be a group, $H \leq G$, $K \trianglelefteq G$. Then $H/(H \cap K) \simeq (HK)/K$.
10. Let G be a group, $H \trianglelefteq G$, $K \trianglelefteq G$, $K \subseteq H$. Then $(G/K)/(H/K) \simeq G/H$.
11. The set of automorphisms of a group G, Aut G, is a group with respect to the composition of functions.
12. Inn $G \trianglelefteq$ Aut G, for any group G.
13. $G/Z(G) \simeq$ Inn G, for any group G.

6.7 SOLUTIONS/ANSWERS

E 1) For any $x, y \in \mathbf{R}^*$, $f(xy) = \ln(xy) = \ln x + \ln y$.
$\therefore$ f is a homomorphism.
$\text{Ker } f = \{ x \in \mathbf{R}^* \mid f(x) = 0 \} = \{1\}$.
$\text{Im } f = \{ f(x) \mid x \in \mathbf{R}^* \} = \{ \ln x \mid x \in \mathbf{R}^* \}$.

E 2) For any $A, B \in GL_3(\mathbf{R})$,
$f(AB) = \det(AB) = \det(A)\det(B) = f(A)\,f(B)$
$\therefore$ f is a homomorphism.
$\text{Ker } f = \{ A \in GL_3(\mathbf{R}) \mid f(A) = 1 \} = \{ A \in GL_3(\mathbf{R}) \mid \det(A) = 1 \}$
$= SL_3(\mathbf{R})$, the special linear group of order 3.
$\text{Im } f = \{ \det(A) \mid A \in GL_3(\mathbf{R}) \}$
$= \mathbf{R}^*$ (because for any $r \in \mathbf{R}^*$, $\exists\, A = \begin{bmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(\mathbf{R})$ such that $\det(A) = r$.)

E 3) $p : S_3 \longrightarrow S_3/A_3 : p(x) = A_3x$
Note that $A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$.
Now $\text{Ker } p = A_3$. $\therefore$ $(1\,2) \notin \text{Ker } p$.
$\text{Im } p = \{ A_3x \mid x \in S_3 \}$. $\therefore$ $(1\,2) \notin \text{Im } p$.

E 4) For any $x, y \in \mathbf{R}$, $f(x + y) = e^{i(x+y)}$
$= e^{ix} \cdot e^{iy} = f(x) \cdot f(y)$.
$\therefore$ f is a homomorphism.
$\text{Ker } f = \{ x \in \mathbf{R} \mid f(x) = 1 \} = \{ x \in \mathbf{R} \mid e^{ix} = 1 \}$
$= \{ x \in \mathbf{R} \mid nx \in 2\pi\mathbf{Z} \} = \dfrac{2\pi}{n}\mathbf{Z}$.

E 5) From Example 3, we know that if we take $G_1 = G/H$ and take f to be the natural homomorphism from G onto G/H, then $\text{Ker } f = H$.

E 6) $i : 3\mathbb{Z} \longrightarrow \mathbb{Z} : i(3n) = 3n$.
$\text{Ker } i = \{ 3n \mid 3n = 0 \} = \{ 0 \}$
$\text{Im } i = 3\mathbb{Z}$.

E 7) $g \circ f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : g \circ f(x) = \overline{nx} = \overline{0}$.
Then, for any $x, y \in \mathbb{Z}$
$g \circ f(x+y) = \overline{0} = \overline{0} + \overline{0} = g \circ f(x) + g \circ f(y)$.
$\therefore$ $g \circ f$ is a homomorphism.
$\text{Ker } (g \circ f) = \mathbb{Z}$, $\text{Im } (g \circ f) = \{ \overline{0} \}$.

E 8) For any $\bar{r}, \bar{s} \in \mathbb{Z}_n$.
$f(\bar{r} + \bar{s}) = f(\overline{r+s}) = \omega^{r+s} = \omega^r . \omega^s = f(\bar{r}) . f(\bar{s})$.
$\therefore$ f is a homomorphism.
f is 1-1 because
$f(\bar{r}) = 1 \implies \omega^r = 1$
$\implies r \mid o(\omega) = n$ (see Unit 4)
$\implies \bar{r} = \bar{0}$
$\therefore$ $\text{Ker } f = \{\bar{0}\}$.
f is surjective because any element of U_n is ω^r for $0 \leq r \leq n-1$, and $\omega^r = f(\bar{r})$.

E 9) Let $G = \langle x \rangle$ and $f : G \longrightarrow G'$ be a homomorphism. Then $f : G \longrightarrow f(G)$ is an onto homomorphism.
Therefore, by Theorem 5, $f(G) = \langle f(x) \rangle$, i.e., $f(G)$ is cyclic.

E 10) a) The function $f : \mathbb{Z} \longrightarrow n\mathbb{Z} : f(k) = nk$ is a well-defined function.
Now, $f(m + k) = n(m + k) = nm + nk = f(m) + f(k)$ $\forall$ $m, k \in \mathbb{Z}$.
$\therefore$ f is a homomorphism.
$\text{Ker } f = \{ 0 \}$. $\therefore$ f is 1-1.
$\text{Im } f = n\mathbb{Z}$. $\therefore$ f is surjective.
$\therefore$ f is an isomorphism and $\mathbb{Z} \simeq n\mathbb{Z}$.

E 11) f is a homomorphism, but not 1-1. $\therefore$ f is not an isomorphism.

E 12) By Theorem 2, $\theta \circ \phi$ is a homomorphism. Now let $x \in \text{Ker } (\theta \circ \phi)$.
Then, $(\theta \circ \phi)(x) = 0 \implies \theta(\phi(x)) = 0$
$\implies \phi(x) = 0$, since θ is 1-1.
$\implies x = 0$, since ϕ is 1-1.

$\therefore$ $\text{Ker } (\theta \circ \phi) = \{ 0 \}$. $\therefore$ $\theta \circ \phi$ is 1-1.

Finally, take any $k \in K$. Then $k = \theta(h)$, for some $h \in H$, since θ is onto.
Now, $h = \phi(g)$, for some $g \in G$, since ϕ is onto.

$\therefore$ $k = \theta \circ \phi(g)$. $\therefore$ $\theta \circ \phi$ is onto.
$\therefore$ $\theta \circ \phi$ is an isomorphism.

E 13) Let $a, b \in H$. Then $\exists$ $x, y \in G$ such that $a = f(x)$, $b = f(y)$.
Now $ab = f(x) f(y) = f(xy)$.
$= f(yx)$, since G is abelian.
$= f(y) f(x)$
$= ba$.
$\therefore$ H is abelian.

E 14) Suppose $\mathbb{C}^* \simeq \mathbb{R}$ and $f : \mathbb{C}^* \longrightarrow \mathbb{R}$ is an isomorphism. Then $o(f(i)) = 4$. But, apart from 0, every element of $(\mathbb{R}, +)$ is of infinite order; and $o(0) = 1$. So, we reach a contradiction.

$\therefore$ $\mathbb{C}^*$ and $\mathbb{R}$ are not isomorphic.

E 15) Since $\mathbb{Z}$ is infinite and $\mathbb{Z}/n\mathbb{Z}$ is finite, the two groups can't be isomorphic.

E 16) $\text{Im exp} = \{ e^r \mid r \in \mathbb{R} \} = \mathbb{R}^+$.
$\text{Ker exp} = \{ 0 \}$.
Thus, by the Fundamental Theorem of Homomorphism, $\mathbb{R} \simeq \mathbb{R}^+$.

E 17) $U_4 = \{ 1, i, i^2, i^3 \} = \{ \pm 1, \pm i \}$.
f is a homomorphism, Ker $f = \{ n \mid i^n = 1 \} = 4\mathbb{Z}$
Im $f = U_4$.
$\therefore \mathbb{Z}/4\mathbb{Z} \simeq U_4$

In Unit 5 we have seen that $\mathbb{Z}/4\mathbb{Z}$ is the same as $\mathbb{Z}_4$.

$\therefore \mathbb{Z}_4 \simeq U_4$.

E 18) $f(x + y) = e^{2\pi i(x+y)} = e^{2\pi ix} \cdot e^{2\pi iy} = f(x)f(y)$.

$\therefore$ f is a homomorphism.

Now any element of S is of the form $\cos \theta + i \sin \theta$

$= \cos 2\pi \frac{\theta}{2\pi} + i \sin 2\pi \frac{\theta}{2\pi} = f\left(\frac{\theta}{2\pi}\right)$.

$\therefore$ f is onto.
Also, Ker $f = \{ x \in \mathbb{R} \mid e^{2\pi ix} = 1 \}$
$= \{ x \in \mathbb{R} \mid \cos 2\pi x + i \sin 2\pi x = 1 \}$
$= \mathbb{Z}$, since $\cos \theta + i \sin \theta = 1$ iff $\theta \in 2\pi\mathbb{Z}$.

Therefore, by the Fundamental Theorem of Homomorphism, $\mathbb{R}/\mathbb{Z} \simeq S$.

E 19) a) You know that $H \cap K \leq H$. Now, let $h \in H$ and $x \in H \cap K$.
Then $h^{-1}xh \in H$, since $h, x \in H$.
Also, $h^{-1}xh \in K$, since $x \in K$ and $K \trianglelefteq G$.
$\therefore h^{-1}xh \in H \cap K$. $\therefore H \cap K \trianglelefteq H$.

b) Since $K \leq G$, $K \leq A$. Also, for any $a \in A$, $a \in G$.
Therefore, since $K \trianglelefteq G$, $a^{-1}Ka = K$. $\therefore K \trianglelefteq A$.

E 20) By Theorem 10, $(HK)/H \simeq K/(H \cap K)$.
$\therefore \frac{o(HK)}{o(H)} = \frac{o(K)}{o(H \cap K)}$, i.e., $o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$

E 21) Let $H = 3\mathbb{Z}$, $K = 4\mathbb{Z}$. By Theorem 10 we know that $(H + K)/K \simeq H/(H \cap K)$.

Now $H + K = 3\mathbb{Z} + 4\mathbb{Z} = \mathbb{Z}$. (Use E 9 of Unit 3 and the fact that $1 = 4 - 3$.)

Also $H \cap K = 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$ (since $x \in 3\mathbb{Z} \cap 4\mathbb{Z}$ iff $3 \mid x$ and $4 \mid x$).

Thus, by Theorem 10, $\mathbb{Z}/4\mathbb{Z} \simeq 3\mathbb{Z}/12\mathbb{Z}$.
You also know that $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$.
$\therefore 3\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_4$.

E 22) For any Kx, Ky in G/K,
$f((Kx)(Ky)) = f(Kxy) = Hxy = (Hx)(Hy) = f(Kx)f(Ky)$.
$\therefore$ f is a homomorphism.

Now, any element of G/H is of the form Hx. And
$Hx = f(Kx) \in \text{Im } f$. $\therefore$ Im $f = G/H$.
Finally, Ker $f = \{ Kx \in G/K \mid f(Kx) = H \}$
$= \{ Kx \in G/K \mid Hx = H \}$
$= \{ Kx \in G/K \mid x \in H \}$
$= H/K$

Therefore, by Theorem 8, $(G/K)/(H/K) \simeq G/H$.

E 23) a) $f_g : GL_2(\mathbb{R}) \to GL_2(\mathbb{R}) : f_g\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = g \begin{bmatrix} a & b \\ c & d \end{bmatrix} g^{-1}$

Now, $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ $\therefore g^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$\therefore g \begin{bmatrix} a & b \\ c & d \end{bmatrix} g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$

$\therefore f_g(GL_2(\mathbb{R})) = \left\{ \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R}) \right\}$

b) $f_g : Z \longrightarrow Z : f_g(x) = g + x + (-g) = x$.

$\therefore f_g = I$. $\therefore f_g(Z) = Z$.

c) Here too, since G is abelian, $f_g = I$.

E 24) Firstly assume that G is abelian. Then, for any $f_g \in \text{Inn } G$,
$f_{g^{-1}}(x) = gxg^{-1} = gg^{-1}x = x \; \forall \; x \in G$.
$\therefore f_g = I_G$.
$\therefore \text{Inn } G = \{ I_G \}$.

Conversely, assume that $\text{Inn } G = \{I_G\}$.
Then, for any $x, y \in G$, $f_x(y) = y$.
$\Longrightarrow xyx^{-1} = y \Longrightarrow xy = yx$.
Therefore, any two elements of G commute with each other. That is, G is abelian.

E 25) To show that $g^{-1} < x > g = < x > \forall \; g \in G$, it is enough to show that $g^{-1}xg \in < x > \forall \; g \in G$. Now, for any $g \in G$, we are given that
$f_{g^{-1}}(x) = x$.
$\Longrightarrow g^{-1}x(g^{-1})^{-1} = x$
$\Longrightarrow g^{-1}xg = x$.
$\therefore g^{-1} < x > g = < x >$. $\therefore \; < x > \trianglelefteq G$.

E 26) We know that $S_3/Z(S_3) \simeq \text{Inn } S_3$.
But, $Z(S_3) = \{ I \}$. $\therefore S_3 \simeq \text{Inn } S_3$.

UNIT 7 PERMUTATION GROUPS

Structure

7.1 INTRODUCTION

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

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

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

Objectives

After reading this unit, you should be able to

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

7.2 SYMMETRIC GROUP

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

Let us recall some facts from Sec. 2.5.2.

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

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

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

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

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

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

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

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

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

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

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

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

We show this process diagrammatically in Fig. 1.

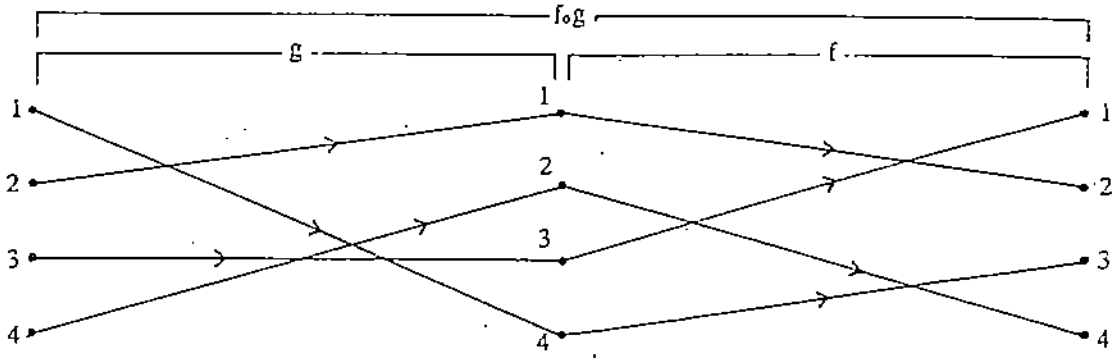


Fig. 1 : $(1\ 2\ 4\ 3) \circ (1\ 4\ 2)$ in S_4

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

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

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

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

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

E 1) Show that $(S_n, \circ)$ is a non-commutative group for $n \geq 3$.

(Hint : Check that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ don't commute.)

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

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

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

7.3 CYCLIC DECOMPOSITION

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

Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. Choose any one of the symbols, say 1.

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

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

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

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

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

(1 3 4 2)

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

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

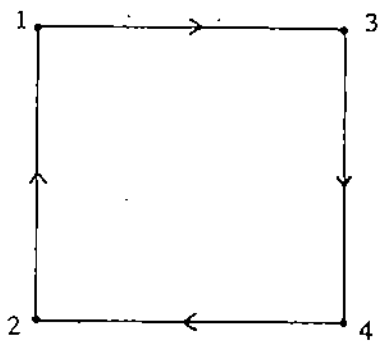


Fig. 2 : (1 3 4 2)

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

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

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

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

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

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

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

Now, can we express any permutation as a cycle? No. Consider the following example from S_5. Let g be the permutation defined by
$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$.
If we start with the symbol 1 and apply the procedure for obtaining a cycle to g, we obtain (1 3 4) after three steps. Because g maps 4 to 1, we close the brackets, even though we have not yet written down all the symbols. Now we simply choose another symbol that has not appeared so far, say 2, and start the process of writing a cycle again. Thus, we obtain another cycle (2 5). Now, all the symbols are exhausted.
∴ g = (1 3 4) (2 5).
We call this expression for g a **product** of a 3-cycle and a transposition. In Fig. 3 we represent g by a diagram which shows the 3-cycle and the 2-cycle clearly.

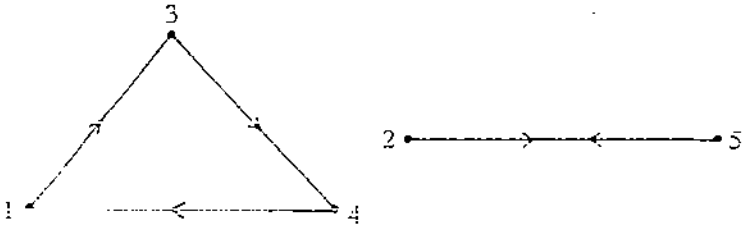


Fig. 3 : (1 3 4) (2 5)

Because of the arbitrary choice of symbol at the beginning of each cycle, there are many ways of expressing g. For example,
g = (4 1 3) (2 5) = (2 5) (1 3 4) = (5 2) (3 4 1).
That is, we can write the product of the separate cycles in any order, and the choice of the starting element within each cycle is arbitrary.

So, you see that g can't be written as a cycle; it is a product of disjoint cycles.

Definition : We call two cycles **disjoint** if they have no symbol in common. Thus, disjoint cycles move disjoint sets of elements. (Note that $f \in S_n$ moves a symbol i if $f(i) \neq i$. We say that f fixes i if $f(i) = i$.)

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

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

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

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

Following our previous rules, we obtain

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

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

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

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

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

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

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

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

What you have seen in E 3 is true in general. We state the following result.

Theorem 2 : Every permutation $f \in S_n$, $f \neq I$, can be expressed as a product of disjoint cycles.

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

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

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

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

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

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

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

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

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

Try the following exercise now.

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

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

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

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

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

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

Similarly, the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$
= (1 3 4) (2 6 5) = (1 4) (1 3) (2 5) (2 6).

Now you can try your hand at this process.

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

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

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

7.4 ALTERNATING GROUP

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

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

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

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

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

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

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

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

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

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

$\prod_{i<j}^{n} a_i - a_j \; a_1 \ldots \ldots a_n$

Try this simple exercise now.

E [1] What is the signature of $I \in S_n$?

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

Theorem 4 : Let $f, g \in S_n$. Then sign $(f \circ g) = (\text{sign } f)(\text{sign } g)$.

Proof : By definition,

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

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

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

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

$\therefore$ sign $(f\circ g) = (\text{sign } f)(\text{sign } g)$.

Now we will show that Im (sign) $= \{1, -1\}$.

Theorem 5 : a) If $t \in S_n$ is a transposition, then sign $t = -1$.
b) sign $f = 1$ or -1 $\forall f \in S_n$.
c) Im (sign) $= \{1, -1\}$.

Proof : a) Let $t = (p\ q)$, where $p < q$.

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

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

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

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

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

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

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

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

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

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

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

$\therefore$ sign $f = 1$ or -1.

c) We know that Im (sign) $\subseteq \{1, -1\}$.
We also know that sign $t = -1$, for any transposition t; and sign $I = 1$.
$\therefore \{1, -1\} \subseteq$ Im (sign).
$\therefore$ Im (sign) $= \{1, -1\}$.

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

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

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

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

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

sign f = 1 iff f is even.

For example, $(1\ 2) \in S_3$ is an odd permutation. In fact, any transposition is an odd permutation. On the other hand, any 3-cycle is an even permutation, since
$(i\ j\ k) = (i\ k)\ (i\ j)$.

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

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

E 13) If $f, g \in S_n$ are odd, then is $f \circ g$ odd too?

E 14) Is the identity permutation odd or even?

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

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

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

Proof : Consider the signature function,
sign : $S_n \to \{1, -1\}$.
Note that $\{1, -1\}$ is a group with respect to multiplication. Now Theorem 4 says that sign is a group homomorphism and Theorem 5 says that Im (sign) $= \{1, -1\}$. Let us obtain Ker (sign).

$$\begin{aligned} \text{Ker (sign)} &= \{f \in S_n \mid \text{sign } f = 1\} \\ &= \{f \in S_n \mid f \text{ is even}\} \\ &= A_n. \end{aligned}$$

$\therefore A_n \trianglelefteq S_n$.
Further, by the Fundamental Theorem of Homomorphism
$S_n / A_n \cong \{1, -1\}$.

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

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

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

Theorem 7 leads us to the following definition.

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

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

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

E 15) Write down all the elements of A_4.

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

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

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

E 16) Check that $(V_4, \circ)$ is a normal subgroup of A_4.

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

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

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

7.5 CAYLEY'S THEOREM

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

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

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

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

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

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

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

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

Try the following exercise now.

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

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

7.6 SUMMARY

In this unit we have discussed the following points.

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

7.7 SOLUTIONS/ANSWERS

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

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

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

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

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

E 4) No. Because

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

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

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

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

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

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

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

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

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

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

E 13) sign (f) = sign (g) = − 1.
∴ sign ($f_o g$) = (−1) (−1) = 1.
∴ $f_o g$ is even.

E 14) sign I = 1. ∴ I is even.

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

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

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

E 17) $f_e(x) = ex = x \; \forall x \in K_4$. ∴ $f_e = I$.
Now, $f_a(e) = a$, $f_a(a) = e$, $f_a(b) = c$, $f_a(c) = b$.
∴ $f_a = (e\ a)\ (b\ c)$.
Similarly, $f_b = (e\ b)\ (a\ c)$ and $f_c = (e\ c)\ (a\ b)$.

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

UNIT 8 FINITE GROUPS

Structure

8.1 INTRODUCTION

By now you are familiar with various finite and infinite groups and their subgroups. In this unit we will pay special attention to certain finite groups and discuss their structures. For example, you will see that any group of order 6 is cyclic or is isomorphic to S_3.

To be able to describe the structure of a finite group we need some knowledge of a direct product of groups. In Sec. 8.2 we will discuss external and internal direct products.

In Sec. 8.3 we discuss the uses of certain results obtained by the famous mathematician Sylow (1832-1918). These theorems, as well as a theorem by Cauchy, allow us to determine various subgroups of some finite groups.

Finally, in Sec. 8.4, we use the knowledge gained in Sec. 8.2 and Sec. 8.3 to describe the structures of several finite groups. In particular, we discuss groups of order less than or equal to 10.

With this unit we wind up our discussion of group theory. In the next block you will start studying ring theory. Of course, you will keep using what you have learnt in the first two blocks, because every ring is a group also, as you will see.

Objectives

After reading this unit, you should be able to

- construct the direct product of a finite number of groups;
- check if a group is a direct product of its subgroups;
- use Sylow's theorems to obtain the possible subgroups and structures of finite groups;
- classify groups of order p, p^2 or pq, where p and q are primes such that $p > q$ and $q \not| p - 1$.

8.2 DIRECT PRODUCT OF GROUPS

In this section we will discuss a very important method of constructing new groups by using given groups as building blocks. We will first see how two groups can be combined to form a third group. Then we will see how two subgroups of a group can be combined to form another subgroup.

8.2.1 External Direct Product

In this sub-section we will construct a new group from two or more groups that we already have.

Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. Consider their Cartesian product (see Sec. 1.3)
$G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$.
Can we define a binary operation on G by using the operations on G_1 and G_2? Let us try the obvious method, namely, componentwise multiplication. That is, we define the operation $*$ on G by $(a, b) * (c, d) = (a *_1 c, b *_2 d) \forall a, c \in G_1, b, d \in G_2$.

The way we have defined $*$ ensures that it is a binary operation.

To check that $(G, *)$ is a group, you need to solve the following exercise.

E 1) Show that the binary operation $*$ on G is associative. Find its identity element and the inverse of any element (x, y) in G.

So, you have proved that $G = G_1 \times G_2$ is a group with respect to $*$. We call G the **external direct product** of $(G_1, *_1)$ and $(G_2, *_2)$.

For example R^2 is the external direct product of R with itself.

Another example is the direct product $(\mathbf{Z}, +) \times (\mathbf{R}^*, .)$ in which the operation is given by $(m, x) * (n, y) = (m + n, xy)$.
We can also define the external direct product of 3, 4 or more groups on the same lines.

Definition : Let $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ be n groups. Their **external direct product** is the group $(G, *)$, where
$G = G_1 \times G_2 \ldots \times G_n$ and

$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \ldots, x_n *_n y_n) \forall\ x_i, y_i \in G_i$.

Thus, $\mathbf{R}^n$ is the external direct product of n copies of R.

We would like to make a remark about notation now.
Remark 1 : Henceforth, we will assume that all the operations $*, *_1, \ldots, *_n$ are multiplication, unless mentioned otherwise. Thus, the operation on
$G = G_1 \times G_2 \times \ldots \times G_n$ will be given by

$(a_1, \ldots, a_n) . (b_1, \ldots, b_n)$
$= (a_1b_1, a_2b_2, \ldots, a_nb_n) \forall\ a_i, b_i \in G_i$.

Now try the following exercise.

E 2) Show that $G_1 \times G_2 \simeq G_2 \times G_1$, for any two groups G_1 and G_2.

Because of E 2 we can speak of the direct product of 2 (or n) groups without bothering about their order.

Now, let G be the external direct product $G_1 \times G_2$. Consider the projection map
$\pi_1 : G_1 \times G_2 \longrightarrow G_1 : \pi_1 (x, y) = x$.
Then π_1 is a group homomorphism, since

$$\begin{aligned}\pi_1 ((a, b) (c, d)) &= \pi_1 (ac, bd) \\ &= ac \\ &= \pi_1(a, b)\ \pi_1 (c, d)\end{aligned}$$

π_1 is also onto, because any $x \in G_1$ is $\pi_1 (x, e_2)$
Now, let us look at Ker π_1.
$\text{Ker } \pi_1 = \{(x, y) \in G_1 \times G_2 \mid \pi_1 (x, y) = e_1\}$
$= \{(e_1, y) \mid y \in G_2\} = \{e_1\} \times G_2$.
$\therefore \{e_1\} \times G_2 \trianglelefteq G_1 \times G_2$.
Also, by the Fundamental Theorem of Homomorphism $(G_1 \times G_2)/(\{e_1\} \times G_2) \simeq G_1$.
We can similarly prove that $G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2$ and $(G_1 \times G_2)/(G_1 \times \{e_2\}) \simeq G_2$.

In the following exercises we give you general facts about external direct products of groups.

E 3) Show that $G_1 \times G_2$ is the product of its normal subgroups $H = G_1 \times \{e_2\}$ and $K = \{e_1\} \times G_2$.
Also show that $(G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2) = \{(e_1, e_2)\}$.

The direct product of finite cyclic groups is cyclic iff their orders are relatively prime.

E 4) Prove that $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$, where $Z(G)$ denotes the centre of G (see Theorem 2 of Unit 3).

E 5) Let A and B be cyclic groups of order m and n, respectively, where $(m, n) = 1$. Prove that $A \times B$ is cyclic of order mn.
(Hint : Define $f : \mathbf{Z} \longrightarrow \mathbf{Z}_m \times \mathbf{Z}_n : f(r) = (r + m\mathbf{Z}, r + n\mathbf{Z})$. Then apply the Fundamental Theorem of Homomorphism to show that $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$.

So, far we have seen the construction of $G_1 \times G_2$ from two groups G_1 and G_2. Now we will see under what conditions we can express a group as a direct product of its subgroups.

8.2.2 Internal Direct Product

Let us begin by recalling from Unit 5 that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. We are interested in the case when HK is the whole of G. We have the following definition.

Definition : Let H and K be normal subgroups of a group G. We call G the **internal direct product** of H and K if

$G = HK$ and $H \cap K = \{e\}$.

We write this fact as $\mathbf{G = H \times K}$.

For example, let us consider the familiar Klein 4-group

$K_4 = \{e, a, b, ab\}$, where $a^2 = e$, $b^2 = e$ and $ab = ba$.

Let $H = < a >$ and $K = < b >$. Then $H \cap K = \{e\}$. Also, $K_4 = HK$.
$\therefore K_4 = H \times K$.

Note that $H \simeq \mathbf{Z}_2$ and $K \simeq \mathbf{Z}_2 \therefore K_4 \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$.

For another example, consider $\mathbf{Z}_{10}$. It is the internal direct product of its subgroups $H = \{\bar{0}, \bar{5}\}$ and $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$. This is because

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

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

Now, can an external direct product also be an internal direct product? Well, go back to E 3. What does it say? It says that the external product of $G_1 \times G_2$ is the internal product $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

We would like to make a remark here.
Remark 2 : Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is isomorphic to the external direct product of H and K. Therefore, when we talk of an internal direct product of subgroups we can drop the word internal, and just say 'direct product of subgroups'.

Let us now extend the definition of the internal direct product of two subgroups to that of several subgroups.
Definition : A group G is the **internal direct product** of its normal subgroups $H_1, H_2, \ldots, H_n$ if

i) $G = H_1 H_2 \ldots H_n$, and
ii) $H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = \{e\} \; \forall \; i = 1, \ldots, n$.

For example, look at the group G generated by $\{a, b, c\}$, where $a^2 = e = b^2 = c^2$ and $ab = ba$, $ac = ca$, $bc = cb$. This is the internal direct product of $< a >$, $< b >$ and $< c >$. That is $G = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

Now, can every group be written as an internal direct product of two or more of its proper normal subgroups? Consider Z. Suppose $\mathbf{Z} = H \times K$, where H, K are subgroups of Z. From Example 4 of Unit 3 you know that $H = < m >$ and $K = < n >$ for some m, $n \in \mathbf{Z}$. Then $mn \in H \cap K$. But if $H \times K$ is a direct product, $H \cap K = \{0\}$. So, we reach a contradiction. Therefore, Z can't be written as an internal direct product of two subgroups.

By the same reasoning we can say that Z can't be expressed as $H_1 \times H_2 \times \ldots \times H_n$, where $H_i \leq \mathbf{Z} \; \forall \; i = 1, 2, \ldots, n$.

When a group is an internal direct product of its subgroups, it satisfies the following theorem.

Theorem 1 : Let a group G be the internal direct product of its subgroups H and K. Then

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

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

Proof : a) We know that $G = HK$. Therefore, if $x \in G$, then $x = hk$, for some $h \in H$, $k \in K$. Now suppose $x = h_1k_1$ also, where $h_1 \in H$ and $k_1 \in K$. Then $hk = h_1k_1$.
$\therefore h_1^{-1}h = k_1k^{-1}$. Now $h_1^{-1}h \in H$.
Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1}h \in K$. $\therefore h_1^{-1}h \in H \cap K = \{e\}$.
$\therefore h_1^{-1}h = e$, which implies that $h = h_1$.
Similarly, $k_1k^{-1} = e$, so that $k_1 = k$.
Thus, the representation of x as the product of an element of H and an element of K is unique.
b) The best way to show that two elements x and y commute is to show that their commutator $x^{-1}y^{-1}xy$ is identity. So, let $h \in H$ and $k \in K$ and consider $h^{-1}k^{-1}hk$. Since $K \trianglelefteq G$, $h^{-1}k^{-1}h \in K$.
$\therefore h^{-1}k^{-1}hk \in K$.
By similar reasoning, $h^{-1}k^{-1}hk \in H$. $\therefore h^{-1}k^{-1}hk \in H \cap K = \{e\}$.
$\therefore h^{-1}k^{-1}hk = e$, that is, $hk = kh$.

Try the following exercise now.

E 6) Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that $G \cong H \times K$.

Now let us look at the relationship between internal direct products and quotient groups.

Theorem 2 : Let H and K be normal subgroups of a group G such that $G = H \times K$. Then $G/H \cong K$ and $G/K \cong H$.

Proof : We will use Theorem 8 of Unit 6 to prove this result.
Now $G = HK$ and $H \cap K = \{e\}$. Therefore,

$G/H = HK/H \cong K/H \cap K = K/\{e\} \cong K$.

We can similarly prove that $G/K \cong H$.

We now give a result which immediately follows from Theorem 2 and which will be used in Sec. 8.4.

Theorem 3 : Let G be a finite group and H and K be its subgroups such that $G = H \times K$. Then $o(G) = o(H)\, o(K)$.

We leave the proof to you (see the following exercise).

E 7) Use Theorem 2 to prove Theorem 3.

And now let us discuss some basic results about the structure of any finite group.

8.3 SYLOW THEOREMS

In Unit 4 we proved Lagrange's theorem, which says that the order of a subgroup of a finite group divides the order of the group. We also said that if G is a finite cyclic group and $m \mid o(G)$, then G has a subgroup of order m. But if G is not cyclic, this statement need not be true, as you have seen in the previous unit. In this context, in 1845 the mathematician Cauchy proved the following useful result.

Theorem 4 : If a prime p divides the order of a finite group G, then G contains an element of order p.

The proof of this result involves a knowledge of group theory that is beyond the scope of this course. Therefore, we omit it. An immediate consequence of this result is the following.

Theorem 5 : If a prime p divides the order of a finite group G, then G contains a subgroup of order p.

Proof : Just take the cyclic subgroup generated by an element of order p. This element exists because of Theorem 4.

So, by Theorem 5 we know that any group of order 30 will have a subgroup of order 2, a subgroup of order 3 and a subgroup of order 5. In 1872 Ludwig Sylow, a Norwegian mathematician, proved a remarkable extension of Cauchy's result. This result, called the first Sylow theorem, has turned out to be the basis of finite group theory. Using this result we can say, for example, that any group of order 100 has subgroups of order 2, 4, 5 and 25. Let us see what this powerful theorem is.

Theorem 6 (First Sylow Theorem) : Let G be a finite group such that $o(G) = p^n m$, where p is a prime, $n \geq 1$ and $(p, m) = 1$. Then G contains a subgroup of order $p^k \; \forall \; k = 1, \ldots, n$.

We shall not prove this result or the next two Sylow theorems either. But, after stating all these results we shall show how useful they are.

The next theorem involves the concepts of conjugacy and Sylow p-subgroups which we now define.

Definition : Two subgroups H and K of a group G are **conjugate** in G if $\exists\; g \in G$ such that $K = g^{-1}Hg$, and then K is called a conjugate of H in G.

Can you do the following exercise now?

E 8) Show that $H \trianglelefteq G$ iff the only conjugate of H in G is H itself.

Now we define Sylow p-subgroups.

Definition : Let G be a finite group and p be a prime such that $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$, for some $n \geq 1$. Then a subgroup of G of order p^n is called a **Sylow p-subgroup** of G.

So, if $o(G) = p^n m$, $(p, m) = 1$, then a subgroup of G of order p^n is a Sylow p-subgroup. Theorem 6 says that this subgroup always exists. But, a group may have more than one Sylow p-subgroup. The next result tells us how two Sylow p-subgroups of a group are related.

Theorem 7 (Second Sylow Theorem) : Let G be a group such that $o(G) = p^n m$, $(p, m) = 1$, p a prime. Then any two Sylow p-subgroups of G are conjugate in G.

And now let us see how many Sylow p-subgroups a group can have.

Theorem 8 (Third Sylow Theorem) : Let G be a group of order $p^n m$, where $(p, m) = 1$ and p is a prime. Then n_p, the number of distinct Sylow p-subgroups of G, is given by $n_p = 1 + kp$ for some $k \geq 0$. And further, $n_p \mid o(G)$.

We would like to make a remark about the actual use of Theorem 8.

Remark 3 : Theorem 8 says that $n_p \equiv 1 \pmod{p}$ (see Sec. 2.5.1). $\therefore (n_p, p) = 1$. Also, since $n_p \mid o(G)$, using Theorem 9 of Unit 1 we find that $n_p \mid m$. This fact helps us to cut down the possibilities for n_p, as you will see in the following examples.

Example 1 : Show that any group of order 15 is cyclic.

Solution : Let G be a group of order $15 = 3 \times 5$. Theorem 6 says that G has a Sylow 3-subgroup. Theorem 8 says that the number of such subgroups must divide 15 and must be congruent to 1(mod 3). In fact, by Remark 3 the number of such subgroups must divide 5 and must be congruent to 1(mod 3). Thus, the only possibility is 1. Therefore, G has a unique Sylow 3-subgroup, say H. Hence, by Theorem 7 and E 8 we know that $H \trianglelefteq G$. Since H is of prime order, it is cyclic.

Similarly, we know that G has a subgroup of order 5. The total number of such subgroups is 1, 6 or 11 and must divide 3. Thus, the only possibility is 1. So G has a unique subgroup of order 5, say K. Then $K \trianglelefteq G$ and K is cyclic.

Now, let us look at $H \cap K$. Let $x \in H \cap K$. Then $x \in H$ and $x \in K$.
$\therefore o(x) \mid o(H)$ and $o(x) \mid o(K)$ (by E 8 of Unit 4), i.e., $o(x) \mid 3$ and $o(x) \mid 5$.
$\therefore o(x) = 1$. $\therefore x = e$. That is, $H \cap K = \{e\}$. Also,

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = 15 = o(G).$$

$\therefore G = HK$.
So, $G = H \times K \simeq Z_3 \times Z_5 \simeq Z_{15}$, by E 5.

Example 2 : Show that a group G of order 30 either has a normal subgroup of order 5 or a normal subgroup of order 3.

Solution : Since $30 = 2 \times 3 \times 5$, G has a Sylow 2-subgroup, a Sylow 3-subgroup and a Sylow 5-subgroup. The number of Sylow 5-subgroups is of the form $1 + 5k$ and divides 6 (by Remark 3). Therefore, it can be 1 or 6. If it is 1, then the Sylow 5-subgroup is normal in G.

On the other hand, suppose the number of Sylow 5-subgroups is 6. Each of these subgroups are distinct cyclic groups of order 5, the only common element being e. Thus, together they contain $24 + 1 = 25$ elements of the group. So, we are left with 5 elements of the group which are of order 2 or 3. Now, the number of Sylow 3-subgroups can be 1 or 10. We can't have 10 Sylow 3-subgroups, because we only have at most 5 elements of the group which are of order 3. So, if the group has 6 Sylow 5-subgroups, then it has only 1 Sylow 3-subgroup. This will be normal in G.

Try the following exercises now.

E 9) Show that every group of order 20 has a proper normal non-trivial subgroup.

E 10) Determine all the Sylow p-subgroups of Z_{24}, where p varies over all the primes dividing 24.

E 11) Show that a group G of order 255 ($= 3 \times 5 \times 17$) has either 1 or 51 Sylow 5-subgroups. How many Sylow 3-subgroups can it have?

Now let us use the powerful Sylow theorems to classify groups of order 1 to 10. In the process we will show you the algebraic structure of several types of finite groups.

8.4 GROUPS OF ORDER 1 TO 10

In this section we will apply the results of the previous section to study some finite groups. In particular, we will list all the groups of order 1 to 10, upto isomorphism.

We start with proving a very useful result.
Theorem 9 : Let G be a group such that $o(G) = pq$, where p, q are primes such that $p > q$ and $q \nmid p - 1$. Then G is cyclic.

Proof : Let P be a Sylow p-subgroup and Q be a Sylow q-subgroup of G. Then $o(P) = p$ and $o(Q) = q$. Now, any group of prime order is cyclic, so $P = \langle x \rangle$ and $Q = \langle y \rangle$ for some $x, y \in G$. By the third Sylow theorem, the number n_p of subgroups of order p can be $1, 1 + p, 1 + 2p, \ldots$, and it must divide q. But $p > q$. Therefore, the only possibility for n_p is 1. Thus, there exists only one Sylow p-subgroup, i.e., P. Further, by Sylow's second theorem $P \trianglelefteq G$.
Again, the number of distinct Sylow q-subgroups of G is $n_q = 1 + kq$ for some k, and $n_q \mid p$. Since p is a prime, its only factors are 1 and p. $\therefore n_q = 1$ or $n_q = p$. Now if $1 + kq = p$, then $q \mid p - 1$. But we started by assuming that $q \nmid p - 1$. So we reach a contradiction. Thus, $n_q = 1$ is the only possibility. Thus, the Sylow q-subgroup Q is normal in G.

Now we want to show that $G = P \times Q$. For this, let us consider $P \cap Q$. The order of any element of $P \cap Q$ must divide p as well as q, and hence it must divide $(p, q) = 1$.
$\therefore P \cap Q = \{e\}$. $\therefore o(PQ) = o(P)\, o(Q) = pq = o(G)$. $\therefore G = PQ$.
So we find that $G = P \times Q \simeq Z_p \times Z_q \simeq Z_{pq}$, by E 5.
Therefore, G is cyclic of order pq.

Using Theorem 9, we can immediately say that any group of order 15 is cyclic (Example 1). Similarly, if $o(G) = 35$, then G is cyclic.

Now if $q \mid p - 1$, then does $o(G) = pq$ imply that G is cyclic? Well, consider S_3. You know that $o(S_3) = 6 = 2.3$, but S_3 is not cyclic. In fact, we have the following result.

Theorem 10 : Let G be a group such that $o(G) = 2p$, where p is an odd prime. Then either G is cyclic or G is isomorphic to the dihedral group D_{2p} of order 2p.
(Recall that $D_{2p} = \langle \{x, y \mid x^p = e = y^2 \text{ and } yx = x^{-1}y\} \rangle$.)

Proof : As in the proof of Theorem 9, there exists a subgroup $P = \langle x \rangle$ of order p with $P \trianglelefteq G$ and a subgroup $Q = \langle y \rangle$ of order 2, since $p > 2$. Since $(2, p) = 1$,
$P \cap Q = \{e\}$. $\therefore o(PQ) = o(G)$.
$\therefore G = PQ$.
Now, two cases arise, namely, when $Q \trianglelefteq G$ and when $Q \not\trianglelefteq G$.

If $Q \trianglelefteq G$, then $G = P \times Q$. And then $G = \langle xy \rangle$.

If Q is not normal in G, then G must be non-abelian.
(Remember that every subgroup of an abelian group is normal.)
$\therefore xy \neq yx$. $\therefore y^{-1}xy \neq x$.
Now, since $P = \langle x \rangle \trianglelefteq G$, $y^{-1}xy \in P$. $\therefore y^{-1}xy = x^r$, for some $r = 2, \ldots, p - 1$.
Therefore, $y^{-2}xy^2 = y^{-1}(y^{-1}xy)y = y^{-1}x^ry = (y^{-1}xy)^r = (x^r)^r = x^{r^2}$.
$\Longrightarrow x = x^{r^2}$, since $o(y) = 2$.
$\Longrightarrow x^{r^2-1} = e$.
But $o(x) = p$. Therefore, by Theorem 4 of Unit 4, $p \mid r^2 - 1$, i.e., $p \mid (r - 1)(r + 1)$
$\Longrightarrow p \mid (r - 1)$ or $p \mid (r + 1)$. But $2 \leq r \leq p - 1$. $\therefore p = r + 1$,
i.e., $r = p - 1$. So we see that
$y^{-1}xy = x^r = x^{p-1} = x^{-1}$.
So, $G = PQ = \langle \{x, y \mid x^p = e, y^2 = e, y^{-1}xy = x^{-1}\} \rangle$, which is exactly the same algebraic structure as that of D_{2p}.
$\therefore G \simeq D_{2p} = \{e, x, x^2, \ldots, x^{p-1}, y, xy, x^2y, \ldots, x^{p-1}y\}$

You can see the utility of Theorem 10 in the following example.

Example 3 : What are the possible algebraic structures of a group of order 6?

Solution : Let G be a group of order 6. Then, by Theorem 10, $G \simeq Z_6$ or $G \simeq D_6$. Of course, in E 7 of Unit 5, you must have already noted that $S_3 \simeq D_6$. So, if G is not cyclic, then $G \simeq S_3$. You may like to try the following exercise now.

E 12) Show that if G is a group of order 10, then $G \simeq Z_{10}$ or $G \simeq D_{10}$.

Now, from Theorem 6 of Unit 4, we know that if $o(G)$ is a prime, then G is cyclic. Thus, groups of orders 2, 3, 5 and 7 are cyclic. This fact, together with Example 3 and E 12, allows us to classify all groups whose orders are 1, 2, 3, 5, 6, 7 or 10. What about the structure of groups of order $4 = 2^2$ and $9 = 3^2$? Such groups are covered by the following result.

Theorem 11 : If G is a group of order p^2, p a prime, then G is abelian.

We will not prove this result, since its proof is beyond the scope of this course. But, using this theorem, we can easily classify groups of order p^2.

Theorem 12 : Let G be a group such that $o(G) = p^2$, where p is a prime. Then either G is cyclic or $G \simeq Z_p \times Z_p$, a direct product of two cyclic groups of order p.

Proof : Suppose G has an element a of order p^2. Then $G = \langle a \rangle$.

On the other hand, suppose G has no element of order p^2. Then, for any $x \in G$, $o(x) = 1$ or $o(x) = p$ (using Lagrange's Theorem).

Let $x \in G$, $x \neq e$ and $H = \langle x \rangle$. Since $x \neq e$, $o(H) \neq 1$

$\therefore o(H) = p$.

Therefore, $\exists\ y \in G$ such that $y \notin H$. Then, by the same reasoning, $K = \langle y \rangle$ is of order p. Both H and K are normal in G, since G is abelian (by Theorem 11).

We want to show that $G = H \times K$. For this, consider $H \cap K$. Now $H \cap K \leq H$.

$\therefore o(H \cap K) \mid o(H) = p$. $\therefore o(H \cap K) = 1$ or $o(H \cap K) = p$.

If $o(H \cap K) = p$, then $H \cap K = H$, and by similar reasoning, $H \cap K = K$. But then, $H = K$. $\therefore y \in H$, a contradiction.

$\therefore o(H \cap K) = 1$, i.e., $H \cap K = \{e\}$.

So, $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$ and $o(HK) = p^2 = o(G)$.

$\therefore G = H \times K \simeq Z_p \times Z_p$.

Now, try the following exercise.

E 13) What are the possible algebraic structures of groups of order 4 and 9?

So far we have shown the algebraic structure of all groups of order 1 to 10, except groups of order 8. Now we will list (without proof) the classification of groups of order 8.
If G is an abelian group of order 8, then

i) $G \simeq Z_8$, the cyclic group or order 8, or

ii) $G \simeq Z_4 \times Z_2$, or

iii) $G \simeq Z_2 \times Z_2 \times Z_2$.

If G is a non-abelian group of order 8, then

i) $G \simeq Q_8$, the quaternion group discussed in Example 4 of Unit 4, or

ii) $G \simeq D_8$, the dihedral group discussed in Example 4 of Unit 5.

So, we have seen what the algebraic structure of any group of order 1, 2, ... , 10 must be. We have said that this classification is upto isomorphism. So, for example, any group of order 10 is isomorphic to Z_{10} or D_{10}. It need not be equal to either of them.

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

8.5 SUMMARY

In this unit we have discussed the following points.

1. The definition and examples of external direct products of groups.
2. The definition and examples of internal direct products of normal subgroups
3. If $(m, n) = 1$, then $Z_m \times Z_n \simeq Z_{mn}$.
4. $o(H \times K) = o(H)\, o(K)$.
5. The statement and application of Sylow's theorems, which state that:
   Let G be a finite group of order $p^n m$, where p is a prime and $p \nmid m$. Then
   i) G contains a subgroup of order $p^k\ \forall\ k = 1, \ldots, n$;
   ii) any two Sylow p-subgroups are conjugate in G;
   iii) the number of distinct Sylow p-subgroups of G is congruent to 1 (mod p) and divides o(G) (in fact, it divides m).
6. Let $o(G) = pq$, p a prime, $p > q$, $q \nmid p - 1$. Then G is cyclic.

7. Let $o(G) = p^2$, p a prime. Then
   i) G is abelian.
   ii) G is cyclic or $G \simeq Z_p \times Z_p$.

8. The classification of groups of order 1 to 10, which we give in the following table.

o(G)	Algebraic structure
1	{e}
2	Z_2
3	Z_3
4	Z_4 or $Z_2 \times Z_2$
5	Z_5
6	Z_6 or S_3
7	Z_7
8	Z_8 or $Z_4 \times Z_2$ or $Z_2 \times Z_2 \times Z_2$ (if G is abelian)
	Q_8 or D_8 (if G is non-abelian)
9	Z_9 or $Z_3 \times Z_3$
10	Z_{10} or D_{10}

8.6 SOLUTIONS/ANSWERS

E 1) $*$ is associative : Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.
Use the fact that $*_1$ and $*_2$ are associative to prove that
$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3))$.
The identity element of G is (e_1, e_2), where e_1 and e_2 are the identities in G_1 and G_2, respectively.
The inverse of $(x, y) \in G$ is (x^{-1}, y^{-1}).

E 2) Define $f : G_1 \times G_2 \longrightarrow G_2 \times G_1 : f(a, b) = (b, a)$.
Then f is 1-1, surjective and a homomorphism. That is, f is an isomorphism.
$\therefore G_1 \times G_2 \simeq G_2 \times G_1$.

E 3) We need to show that any element of $G_1 \times G_2$ is of the form hk, where $h \in H$ and $k \in K$.
Now, any element of $G_1 \times G_2$ is $(x, y) = (x, e_2)(e_1, y)$ and $(x, e_2) \in H$, $(e_1, y) \in K$.
$\therefore G_1 \times G_2 = HK$.
Now, let us look at $H \cap K$. Let $(x, y) \in H \cap K$.
Since $(x, y) \in H$, $y = e_2$. Since $(x, y) \in K$, $x = e_1$.
$\therefore (x, y) = (e_1, e_2)$. $\therefore H \cap K = \{(e_1, e_2)\}$.

E 4) Now, $(x, y) \in Z(G_1 \times G_2)$.
$\iff (x, y)(a, b) = (a, b)(x, y) \; \forall (a, b) \in G_1 \times G_2$
$\iff (xa, yb) = (ax, by) \; \forall a \in G_1, b \in G_2$
$\iff xa = ax \; \forall a \in G_1$ and $yb = by \; \forall b \in G_2$
$\iff x \in Z(G_1)$ and $y \in Z(G_2)$
$\iff (x, y) \in Z(G_1) \times Z(G_2)$
$\therefore Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

E 5) Let $A = \langle x \rangle$ and $B = \langle y \rangle$, where $o(x) = m$, $o(y) = n$.
Then $A \simeq Z_m$ and $B \simeq Z_n$.
If we prove that $Z_m \times Z_n \simeq Z_{mn}$, then we will have proved that $A \times B \simeq Z_{mn}$, that is, $A \times B$ is cyclic of order mn.
So, let us prove that if $(m, n) = 1$, then $Z_{mn} \simeq Z_m \times Z_n$.
Define $f : Z \longrightarrow Z_m \times Z_n : f(r) = (r + mZ, r + nZ)$.
(Remember that $Z_s = Z/sZ$, for any $s \in N$.)
Now, f is a homomorphism because
$f(r + s) = ((r + s) + mZ, (r + s) + nZ)$
$= (r + mZ, r + nZ) + (s + mZ, s + nZ)$.
$= f(r) + f(s)$.
$\text{Ker } f = \{r \in Z \mid r \in mZ \cap nZ\}$
$= \{r \in Z \mid r \in mnZ\}$
$= mnZ$.

Finally, we will show that f is surjective. Now, take any element $(u + mZ, v + nZ) \in Z_m \times Z_n$. Since $(m, n) = 1$, $\exists$ $s, t \in Z$ such that $ms + nt = 1$ (see Sec. 1.6). Using this equation we see that
$f(u(1 - ms) + v(1 - nt)) = (u + mZ, v + nZ)$.
Thus, f is surjective.
Now, we apply the Fundamental Theorem of Homomorphism and find that
$Z/\text{Ker } f \simeq \text{Im } f$, that is, $Z/mnZ \simeq Z_m \times Z_n$, that is, $Z_{mn} \simeq Z_m \times Z_n$.
$\therefore$ $A \times B$ is cyclic of order mn.

E 6) We know that each $x \in G$ can be expressed as hk, where $h \in H$ and $k \in K$.
$\therefore$ $G = HK$.
We need to show that $H \cap K = \{e\}$. Let $x \in H \cap K$.
Then $x \in H$ and $x \in K$. $\therefore$ $xe \in HK$ and $ex \in HK$.
So, x has two representations, xe and ex, as a product of an element of H and an element of K. But we have assumed that each element must have only one such representation. So the two representations xe and ex must coincide, that is,
$x = e$. $\therefore$ $H \cap K = \{e\}$.
$\therefore$ $G = H \times K$.

E 7) $G = H \times K \implies G/H \simeq K \implies o(G/H) = o(K) \implies o(G)/o(H) = o(K)$.
$\implies o(G) = o(H)\, o(K)$.

E 8) $H \trianglelefteq G \iff g^{-1}Hg = H \; \forall g \in G \iff$ the only conjugate of H in G is H.

E 9) Let G be a group of order 20. Since $20 = 2^2 \times 5$, G has a Sylow 5-subgroup. The number of such subgroups is congruent to 1(mod 5) and divides 4. Thus, the number is 1. Therefore, the Sylow 5-subgroup of G is normal in G, and is the required subgroup.

E 10) $o(Z_{24}) = 24 = 2^3 \times 3$.
$\therefore$ Z_{24} has a Sylow 2-subgroup and a Sylow 3-subgroup. The number of Sylow 2-subgroups is 1 or 3 and the number of Sylow 3-subgroups is 1 or 4. Now, if Z_{24} has only 1 Sylow 2-subgroup, this accounts for 8 elements of the group. So, we are left with 16 elements of order 3. But this is not possible because we can only have at most 4 distinct Sylow 3-subgroups (i.e., 8 elements of order 3). So, we reach a contradiction.
$\therefore$ Z_{24} must have 3 Sylow 2-subgroups. And then it will have only 1 Sylow 3-subgroup. These are all the Sylow p-subgroups of Z_{24}.

E 11) $255 = 3 \times 5 \times 17 = 5 \times 51$.
The number of Sylow 5-subgroups is congruent to 1(mod 5) and must divide 51. Thus, it is 1 or 51.
Since $255 = 3 \times 85$, the number of Sylow 3-subgroups that G can have is congruent to 1(mod 3) and must divide 85. Thus, it is 1 or 85.

E 12) We can apply Theorem 10 here.

E 13) Applying Theorem 12, we see that
i) $o(G) = 4 \implies G \simeq Z_4$ or $G \simeq Z_2 \times Z_2$.
ii) $o(G) = 9 \implies G \simeq Z_9$ or $G \simeq Z_3 \times Z_3$.

VIDEO PROGRAMME NOTES (MTE-06)

Groups of Symmetries

(To be viewed after studying Block 2)

Content Coordinator: Dr. Parvin Sinclair
School of Sciences
IGNOU

Producer: Sunil Das
Communication Division
IGNOU

A symmetry of an object is a movement that brings the object into superposition with itself. In this programme we look at the symmetries of various two- and three-dimensional geometrical objects. We use them as examples to concretise certain concepts of group theory that you have studied in the first two blocks of this course.

During the programme you will see that the set of all symmetries of an object forms a group, which is the **group of symmetries** (or the **symmetry group**) of the object. It turns out that this group is a permutation group.

An object can have rotational as well as reflection symmetries. In the programme you will see that the set of rotational symmetries is a subgroup of the group of symmetries of the object. In particular, you will see that

i) the group of rotational symmetries of a regular n-sided polygon is the dihedral group
$D_{2n} = \langle \{x,y \mid x^2 = e,\ y^n = e,\ xy = y^{-1}x\} \rangle$,
where e is the identity of the group.

ii) the group of rotational symmetries of a regular tetrahedron is A_4, and the group of all its symmetries is S_4.

iii) the group of rotational symmetries of a cube is S_4.

iv) the group of rotational symmetries of a regular octahedron is S_4, since a cube and regular octahedron are the **duals** of each other.

During the programme we have given you the following **activities to do after viewing the programme.**

1) Check that the composition of symmetries of an object is an associative operation.

2) Obtain the group of symmetries of a snow crystal.
(Hint: As we have said in the programme, this is the same as the group of symmetries of a regular hexagon. You need to check that this group is D_{12}. Note that a 5-cycle can't be a symmetry of a hexagon, because any symmetry that moves 5 vertices must move all 6 vertices.)

3) Find the group of rotational symmetries of a methane molecule.
(Hint: The molecule's structure is tetrahedral, with the hydrogen atoms at the vertices and the carbon atom inside the tetrahedron, at an equal distance from each of the vertices.)

4) Find all the 24 rotational symmetries of a cube.
(In the programme we have shown you that these symmetries are elements of S_4, S_6 or S_8, depending on whether we are observing the permutations of its diagonals, its faces or its vertices.)

UTTAR PRADESH
RAJARSHI TANDON OPEN UNIVERSITY

UGMM – 06

Abstract Algebra

Block

3

ELEMENTARY RING THEORY

BLOCK 3 ELEMENTARY RING THEORY

Pussy said to the Owl, 'You elegant fowl!
How charmingly sweet you sing!
O let us be married! Too long we have tarried:
But what shall we do for a ring?'

From 'The Owl and The Pussycat' by Edward Lear.

In the first two blocks of this course we acquainted you with various aspects of group theory. In the three units of this block, we will introduce you to another algebraic structure. It consists of a set along with two binary operations defined on it. We will call such a system a ring if it satisfies certain axioms that we state in Unit 9.

The notion of a ring is due to the mathematicians Richard Dedekind (1831-1916) and Leopold Kronecker (1823-1891). Kronecker called such a system an 'order'. The famous David Hilbert introduced the term 'ring' in 1897. The current definition of an abstract ring appears to be due to Emmy Noether, who used it extensively in her paper published in 1921.

As you go through the block you will see that a ring is an abelian group with some extra properties. You will realise that we can very naturally generalise many of the concepts of group theory to ring theory. Thus, whatever you have studied about groups will help you to study this block, and the next one.

Our exposition of ring theory will follow the path that we used for acquainting you with group theory. We will start by defining different types of rings. Then we shall introduce you to subrings (the analogue of subgroups) and ideals (the analogue of normal subgroups). As in Unit 5, this will lead us to quotient rings, the analogue of quotient groups. In the last unit of this block we shall discuss ring homomorphisms and isomorphisms. You will discover that the extremely useful isomorphism theorems for groups can be carried over to rings. This helps us greatly in analysing the structure of rings.

As in the previous blocks, we shall help you to digest the material by exposing you to plenty of examples and exercises. The exercises are as important as the rest of the material in the unit; so please attempt them as and when you come across them, and move further only after solving them.

Notations and Symbols

$a \equiv b \pmod{n}$	a is congruent to b modulo n.
$\wp(\overset{X}{=})$	set of all subsets of X.
$A \Delta B$	$(A \setminus B) \cup (B \setminus A)$
R/I	quotient ring of R by I.
$< a >$	principal ideal generated by a.
$< a_1, ..., a_n >$	ideal generated by $a_1, ..., a_n$.
Ker f	kernel of the homomorphism f.
$\simeq$	is isomorphic to

UNIT 9 RINGS

Structure

9.1 INTRODUCTION

With this unit we start the study of algebraic systems with two binary operations satisfying certain properties. Z, Q and R are examples of such a system, which we shall call a ring.

Now, you know that both addition and multiplication are binary operations on Z. Further, Z is an abelian group under addition. Though it is not a group under multiplication, multiplication is associative. Also, addition and multiplication are related by the distributive laws

$a(b + c) = ab + ac$, and $(a + b)c = ac + bc$

for all integers a, b and c. We generalise these very properties of the binary operations to define a ring in general. This definition is due to the famous algebraist Emmy Noether.

Fig. 1 : Emmy Noether (1882-1935)

After defining rings we shall give several examples of rings. We shall also give some properties of rings that follow from the definition itself. Finally, we shall discuss certain types of rings that are obtained when we impose more restrictions on the "multiplication" in the ring.

As the contents suggest, this unit lays the foundation for the rest of this course. So make sure that you have attained the following objectives before going to the next unit.

Objectives

After reading this unit, you should be able to

- define and give examples of rings;
- derive some elementary properties of rings from the defining axioms of a ring;
- define and give examples of commutative rings, rings with identity and commutative rings with identity.

9.2 WHAT IS A RING?

You are familiar with Z, the set of integers. You also know that it is a group with respect to addition. Is it a group with respect to multiplication too? No. But multiplication is associative and distributes over addition. These properties of addition and multiplication of integers allow us to say that the system $(Z, +, .)$ is a ring. But, what do we mean by a ring?

Definition : A non-empty set R together with two binary operations, usually called addition (denoted by $+$) and multiplication (denoted by $.$), is called a **ring** if the following axioms are satisfied :

R 1) $a + b = b + a$ for all a, b in R, i.e., addition is commutative.

R 2) $(a + b) + c = a + (b + c)$ for all a, b, c in R, i.e., addition is associative

R 3) There exists an element (denoted by 0) of R such that
$a + 0 = a = 0 + a$ for all a in R, i.e., R has an additive identity.

R 4) For each a in R, there exists x in R such that $a + x = 0 = x + a$, i.e., every element of R has an additive inverse.

R 5) $(a . b).c = a.(b . c)$ for all a, b, c in R, i.e., multiplication is associative.

R 6) $a.(b + c) = a . b + a . c$, and
$(a + b).c = a . c + b . c$
for all a, b, c in R,
i.e., multiplication distributes over addition from the left as well as the right.

The axioms R1–R4 say that $(R, +)$ is an abelian group. The axiom R5 says that multiplication is associative. Hence, we can say that the system $(R, +, .)$ is a ring if

i) $(R, +)$ is an abelian group,

ii) $(R, .)$ is a semigroup, and

iii) for all a, b, c in R, $a.(b + c) = a . b + a . c$, and $(a + b).c = a . c + b . c$.

From Unit 2 you know that the addition identity 0 is unique, and each element a of R has a unique additive inverse (denoted by $-a$). We call the element 0 the **zero element** of the ring.

By convention, we write $a - b$ for $a + (-b)$.

Let us look at some examples of rings now. You have already seen that Z is a ring. What about the sets Q and R? Do $(Q, +, .)$ and $(R, +, .)$ satisfy the axioms R1-R6? They do. Therefore, these systems are rings.

The following example provides us with another set of examples of rings.

Example 1 : Show that $(nZ, +, .)$ is a ring, where $n \in Z$.

Solution : You know that $nZ = \{ nm \mid m \in Z \}$ is an abelian group with respect to addition. You also know that multiplication in nZ is associative and distributes over addition from the right as well as the left. Thus, nZ is a ring under the usual addition and multiplication.

The underlying set of a ring $(R, +, .)$ is the set R.

So far the examples that we have considered have been **infinite rings**, that is, their underlying sets have been infinite sets. Now let us look at a **finite ring**, that is, a ring $(R, +, .)$ where R is a finite set. Our example is the set Z_n that you studied in Unit 2 (Sec. 2.5.1). Let us briefly recall the construction of Z_n, the set of residue classes modulo n.

If a and b are integers, we say that a is congruent to b modulo n if $a - b$ is divisible by n; in symbols, $a \equiv b \pmod n$ if $n \mid (a - b)$. The relation 'congruence modulo n' is an equivalence relation in Z. The equivalence class containing the integer a is

$\bar{a} = \{ b \in Z \mid a - b \text{ is divisible by } n \}$
$= \{a + mn \mid m \in Z \}$.

It is called the congruence class of a modulo n or the residue class of a modulo n. The set of all equivalence classes is denoted by Z_n. So

$Z_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$.

We define addition and multiplication of classes in terms of their representatives by

$\bar{a} + \bar{b} = \overline{a + b}$ and
$\bar{a}.\bar{b} = \overline{ab} \ \forall \ \bar{a}, \bar{b} \in Z_n$.

In Sec. 2.5.1 you have seen that these operations are well defined in Z_n. To help you regain some practice in adding and multiplying in Z_n, consider the following Cayley tables for Z_5.

Addition in Z_5

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Multiplication in Z_5

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Now let us go back to looking for a finite ring.

Example 2 : Show that $(Z_n, +, .)$ is a ring.

Solution : You already know that $(Z_n, +)$ is an abelian group, and that multiplication is associative in Z_n. Now we need to see if the axiom R6 is satisfied.

For any $\bar{a}, \bar{b}, \bar{c} \in Z_n$,

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

Thus, $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.

Similarly, $(\bar{a} + \bar{b}) . \bar{c} = \bar{a}.\bar{c} + \bar{b}.\bar{c}$ $\forall$ $\bar{a}, \bar{b}, \bar{c} \in Z_n$.
So, $(Z_n, +, .)$ satisfies the axioms R1–R6. Therefore, it is a ring.

Try this exercise now.

E 1) Write out the Cayley tables for addition and multiplication in Z_6^*, the set of non-zero elements of Z_6. Is $(Z_6^*, +, .)$ a ring? Why?

Now let us look at a ring whose underlying set is a subset of C.

Example 3 : Consider the set
$Z + iZ = \{ m + in \mid m \text{ and } n \text{ are integers} \}$, where $i^2 = -1$.
We define '+' and '.' in $Z + iZ$ to be the usual addition and multiplication of complex numbers. Thus, for $m + in$ and $s + it$ in $Z + iZ$,
$(m + in) + (s + it) = (m + s) + i(n + t)$, and
$(m + in) . (s + it) = (ms - nt) + i(mt + ns)$.

Verify that $Z + iZ$ is a ring under this addition and multiplication. (This ring is called the ring of **Gaussian integers**, after the mathematician Carl Friedrich Gauss.)

Solution : Check that $(Z + iZ, +)$ is a subgroup of $(C, +)$. Thus, the axioms R1–R4 are satisfied. You can also check that
$((a + ib) . (c + id)) . (m + in) = (a + ib) . ((c + id) . (m + in))$
$\forall$ $a + ib, c + id, m + in \in Z + iZ$.

This shows that R5 is also satisfied.

Finally, you can check that the right distributive law holds, i.e.,
$((a + ib) + (c + id)) . (m + in) = (a + ib) . (m + in) + (c + id) . (m + in)$ for any $a + ib, c + id, m + in \in Z + iZ$.

Similarly, you can check that the left distributive law holds. Thus, $(Z + iZ, +, .)$ is a ring.

The next example is related to Example 8 of Unit 2. The operations that we consider in it are not the usual addition and multiplication.

Example 4 : Let X be a non-empty set, $\mathcal{P}(X)$ be the collection of all subsets of X and Δ denote the symmetric difference operation. Show that $(\mathcal{P}(X), \Delta, \cap)$ is a ring.

Solution : For any two subsets A and B of X,
$A \Delta B = (A \setminus B) \cup (B \setminus A)$

In Example 8 of Unit 2 we showed that $(\mathcal{P}(X), \Delta)$ is an abelian group. You also know that $\cap$ is associative. Now let us see if $\cap$ distributes over Δ.

Let $A, B, C \in \mathcal{P}(X)$. Then
$A \cap (B \Delta C) = A \cap [(B \setminus C) \cup (C \setminus B)]$
$= [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)]$, since $\cap$ distributes over $\cup$.
$= [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)]$, since $\cap$ distributes over complementation.
$= (A \cap B) \Delta (A \cap C)$.

So, the left distributive law holds.

Also, $(B \Delta C) \cap A = A \cap (B \Delta C)$, since $\cap$ is commutative.
$= (A \cap B) \Delta (A \cap C)$
$= (B \cap A) \Delta (C \cap A)$

Therefore, the right distributive law holds also.

Therefore, $(\mathcal{P}(X), \Delta, \cap)$ is a ring.

So far you have seen examples of rings in which both the operations defined on the ring have been commutative. This is not so in the next example

Example 5 : Consider the set

$$M_2(R) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| \; a_{11}, a_{12}, a_{21} \text{ and } a_{22} \text{ are real numbers} \right\}$$

Show that $M_2(R)$ is a ring with respect to addition and multiplication of matrices.

Solution : Just as we have solved Example 2 of Unit 3, you can check that $(M_2(R), +)$ is an abelian group. You can also verify the associative property for multiplication. (Also see Example 5 of Unit 2.) We now show that $A.(B + C) = A.B + A.C$ for A, B, C in $M_2(R)$.

$$\begin{aligned}
A.(B + C) &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right) \\
&= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{bmatrix} \\
&= \begin{bmatrix} a_{11}(b_{11} + c_{11}) + a_{12}(b_{21} + c_{21}) & a_{11}(b_{12} + c_{12}) + a_{12}(b_{22} + c_{22}) \\ a_{21}(b_{11} + c_{11}) + a_{22}(b_{21} + c_{21}) & a_{21}(b_{12} + c_{12}) + a_{22}(b_{22} + c_{22}) \end{bmatrix} \\
&= \begin{bmatrix} (a_{11}b_{11} + a_{12}b_{21}) + (a_{11}c_{11} + a_{12}c_{21}) & (a_{11}b_{12} + a_{12}b_{22}) + (a_{11}c_{12} + a_{12}c_{22}) \\ (a_{21}b_{11} + a_{22}b_{21}) + (a_{21}c_{11} + a_{22}c_{21}) & (a_{21}b_{12} + a_{22}b_{22}) + (a_{21}c_{12} + a_{22}c_{22}) \end{bmatrix} \\
&= \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix} + \begin{bmatrix} a_{11}c_{11} + a_{12}c_{21} & a_{11}c_{12} + a_{12}c_{22} \\ a_{21}c_{11} + a_{22}c_{21} & a_{21}c_{12} + a_{12}c_{22} \end{bmatrix} \\
&= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \\
&= A.B + A.C.
\end{aligned}$$

In the same way we can obtain the other distributive law, i.e., $(A + B).C = A.C + B.C \; \forall \; A, B, C \in M_2(R)$.

Thus, $M_2(R)$ is a ring under matrix addition and multiplication.

Note that multiplication over $M_2(R)$ is not commutative. So, we can't say that the left distributive law implies the right distributive law in this case.

Try the following exercises now.

E 2) Show that the set $Q + \sqrt{2}Q = \{ p + \sqrt{2}q \mid p, q \in Q \}$ is a ring with respect to addition and multiplication of real numbers.

E 3) Let $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \; a, b \text{ are real numbers} \right\}$. Show that R is a ring under matrix addition and multiplication.

E 4) Let $R = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| \; a, b \text{ are real numbers} \right\}$. Prove that R is a ring under matrix addition and multiplication.

E 5) Why is $(\mathcal{P}(X), \cup, \cap)$ not a ring?

Let us now look at rings whose elements are functions.

Example 6 : Consider the class of all continuous real valued functions defined on the closed interval [0, 1]. We denote this by C[0, 1]. If f and g are two continuous functions on [0, 1], we define $f + g$ and fg as

$(f + g)(x) = f(x) + g(x)$ (i.e., pointwise addition)

and $(f.g)(x) = f(x).g(x)$ (i.e., pointwise multiplication)

for every $x \in [0, 1]$. From the Calculus course you know that the function $f + g$ and fg are defined and continuous on [0, 1], i.e., if f and $g \in C[0, 1]$, then both $f + g$ and $f.g$ are in C[0, 1]. Show that C[0, 1] is a ring with respect to + and

Solution : Since addition in R is associative and commutative, so is addition in C[0, 1]. The additive identity of C[0, 1] is the zero function. The additive inverse of $f \in C[0, 1]$ is $(-f)$, where $(-f)(x) = -f(x) \forall x \in [0, 1]$. See Fig. 2 for a visual interpretation of $(-f)$. Thus, $(C[0, 1], +)$ is an abelian group. Again, since multiplication in R is associative, so is multiplication in C[0, 1].

Now let us see if the axiom R6 holds.

To prove $f.(g + h) = f.g + f.h$, we consider $(f.(g + h))(x)$ for any x in [0, 1].

Now $(f.(g + h))(x) = f(x)\,(g + h)(x)$
$= f(x)\,(g(x) + h(x))$
$= f(x)\,g(x) + f(x)\,h(x)$, since . distributes over + in R.
$= (f.g)(x) + (f.h)(x)$
$= (f.g + f.h)(x)$
Hence, $f.(g + h) = f.g + f.h$.

Since multiplication is commutative in C[0, 1], the other distributive law also holds. Thus, R6 is true for C[0, 1]. Therefore, $(C[0, 1], +, .)$ is a ring.

This ring is called the **ring of continuous functions on [0, 1].**

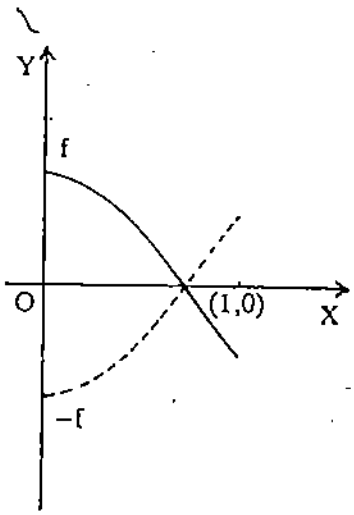


Fig 2 : The graphs of f and (− f) over [0, 1].

An endomorphism of a group G is a homomorphism from G into G.

The next example also deals with functions.

Example 7 : Let (A, +) be an abelian group. The set of all endomorphisms of A is

End A = $\{ f : A \to A \mid f(a + b) = f(a) + f(b) \forall a, b \in A \}$
For $f, g \in$ End A, we define $f + g$ and $f.g$ as
$(f + g)(a) = f(a) + g(a)$, and
$(f.g)(a) = f \circ g(a) = f(g(a)) \forall a \in A$ ..... (1)

Show that (End A, +, .) is a ring. (This ring is called the **endomorphism ring** of A.)

Solution : Let us first check that + and . defined by (1) are binary operations on End A.

For all $a, b \in A$,
$(f + g)(a + b) = f(a + b) + g(a + b)$
$= (f(a) + f(b)) + (g(a) + g(b))$
$= (f(a) + g(a)) + (f(b) + g(b))$
$= (f + g)(a) + (f + g)(b)$, and
$(f.g)(a + b) = f(g(a + b))$
$= f(g(a) + g(b))$
$= f(g(a)) + f(g(b))$
$= (f.g)(a) + (f.g)(b)$
Thus, $f + g$ and $f.g \in$ End A.

Now let us see if (End A, +, .) satisfies R1–R6.

Since + in the abelian group A is associative and commutative, so is + in End A. The zero homomorphism on A is the zero element in End A. $(-f)$ is the additive inverse of $f \in$ End A. Thus, (End A, +) is an abelian group.

You also know that the composition of functions is an associative operation in End A.

Finally, to check R6 we look at $f.(g + h)$ for any $f, g, h \in$ End A. Now for any $a \in A$,
$[f.(g + h)](a) = f((g + h)(a))$
$= f(g(a) + h(a))$
$= f(g(a)) + f(h(a))$
$= (f.g)(a) + (f.h)(a)$
$= (f.g + f.h)(a)$
$\therefore f.(g + h) = f.g + f.h$.

We can similarly prove that $(f + g).h = f.h + g.h$.
Thus, R1-R6 are true for End A.
Hence, (End A, +, .) is a ring.
Note that . is not commutative since $f.g$ need not be equal to $g.f$ for $f, g \in$ End A

You may like to try these exercises now.

E 6) Let X be a non-empty set and $(R, +, .)$ be any ring. Define the set Map(X, R) to be the set of all functions from X to R. That is,
$\text{Map}(X, R) = \{ f \mid f : X \to R \}$.
Define $+$ and $.$ in Map (X, R) by pointwise addition and multiplication. Show that $(\text{Map}(X, R), +, .)$ is a ring.

E 7) Show that the set R of real numbers is a ring under addition and multiplication given by $a \oplus b = a + b + 1$, and $a \odot b = a.b + a + b$
for all $a, b \in R$, where $+$ and $.$ denote the usual addition and multiplication of real numbers.

On solving E 7 you must have realised that a given set can be an underlying set of many different rings.

Now, let us look at the Cartesian product of rings.

Example 8 : Let $(A, +, .)$ and $(B, \boxplus, \boxdot)$ be two rings. Show that their Cartesian product $A \times B$ is a ring with respect to $\oplus$ and $*$ defined by
$(a, b) \oplus (a', b') = (a + a', b \boxplus b')$, and
$(a, b) * (a', b') = (a . a', b \boxdot b')$

for all $(a, b), (a', b')$ in $A \times B$.

Solution : We have defined the addition and multiplication in $A \times B$ componentwise. The zero element of $A \times B$ is $(0, 0)$. The additive inverse of (a, b) is $(-a, \boxminus b)$, where $\boxminus b$ denotes the inverse of b with respect to $\boxplus$.

Since the multiplications in A and B are associative, $*$ is associative in $A \times B$. Again, using the fact that R6 holds for A and B, we can show that R6 holds for $A \times B$. Thus,
$(A \times B, \oplus, *)$ is a ring.

If you have understood this example, you will be able to do the next exercise.

E 8) Write down the addition and multiplication tables for $\mathbf{Z}_2 \times \mathbf{Z}_3$.

Before going further we would like to make a remark about notational conventions. In the case of groups, we decided to use the notation G for $(G, *)$ for convenience. Here too, in future, we shall use the notation R for $(R, +, .)$ for convenience. Thus, we shall assume that $+$ and $.$ are known. We shall also denote the product of two ring elements a and b by ab instead of $a . b$.

So now let us begin studying various properties of rings.

9.3 ELEMENTARY PROPERTIES

In this section we will prove some simple but important properties of rings which are immediate consequences of the definition of a ring. As we go along you must not forget that for any ring R, $(R, +)$ is an abelian group. Hence the results obtained for groups in the earlier units are applicable to the abelian group $(R, +)$. In particular,

i) the zero element, 0, and the additive inverse of any element is unique.

ii) the cancellation law holds for addition.
i.e., $\forall a, b, c \in R$, $a + c = b + c \Rightarrow a = b$

As we have mentioned earlier, we will write $a - b$ for $a + (-b)$ and ab for $a . b$, where $a, b \in R$.

So let us state some properties which follow from the axiom R6, mainly,

Theorem 1 : Let R be a ring. Then, for any $a, b, c \in R$,

i) $a0 = 0 = 0a$.

ii) $a(-b) = (-a)b = -(ab)$.

iii) $(-a)(-b) = ab$,

iv) $a(b - c) = ab - ac$, and

v) $(b - c)a = ba - ca$.

Proof : i) Now, $0 + 0 = 0$
$\Rightarrow a(0 + 0) = a0$
$\Rightarrow a0 + a0 = a0$, applying the distributive law.
$= a0 + 0$, since 0 is the additive identity.
$\Rightarrow a0 = 0$, by the cancellation law for $(R, +)$.

Using the other distributive law, we can similarly show that $0a = 0$.
Thus, $a0 = 0 = 0a$ for all $a \in R$.

ii) From the definition of additive inverse, we know that $b + (-b) = 0$.
Now, $0 = a0$, from (i) above.
$= a(b + (-b))$, as $0 = b + (-b)$.
$= ab + a(-b)$, by distributivity.
Now, $ab + [-(ab)] = 0$ and $ab + a(-b) = 0$. But you know that the additive inverse of an element is unique.

Hence, we get $-(ab) = a(-b)$.

In the same manner, using the fact that $a + (-a) = 0$, we get $-(ab) = (-a)b$.
Thus, $a(-b) = (-a)b = -(ab)$ for all $a, b \in R$.

iii) For $a, b \in R$,
$(-a)(-b) = -(a(-b))$, from (ii) above.
$= a(-(-b))$, from (ii) above.
$= ab$, since b is the additive inverse of $(-b)$.

iv) For $a, b, c \in R$,
$a(b - c) = a(b + (-c))$
$= ab + a(-c)$, by distributivity.
$= ab + (-(ac))$, from (ii) above.
$= ab - ac$.

We can similarly prove (v).

Try this exercise now.

E 9) Show that $\{0\}$ is a ring with respect to the usual addition and multiplication. (This is called the **trivial ring**.)

Also show that if any singleton is a ring, the singleton must be $\{0\}$.

E 10) Prove that the only ring R in which the two operations are equal (i.e., $a + b = ab$ $\forall$ $a, b \in R$) is the trivial ring.

Now let us look at the sum and the product of three or more elements of a ring. We define them recursively, as we did in the case of groups (see Unit 2).

If k is an integer ($k \geq 2$) such that the sum of k elements in a ring R is defined, we define the sum of $(k + 1)$ elements $a_1, a_2, \ldots, a_{k+1}$ in R, taken in that order, as
$a_1 + \ldots + a_{k+1} = (a_1 + \ldots + a_k) + a_{k+1}$.

In the same way if k is a positive integer such that the product of k elements in R is defined, we define the product of $(k + 1)$ elements $a_1, a_2, \ldots, a_{k+1}$ (taken in that order) as
$a_1 \ldots a_{k+1} = (a_1 \ldots a_k) a_{k+1}$.

As we did for groups, we can obtain laws of indices in the case of rings also with respect to both $+$ and $\cdot$. In fact, we have the following results for any ring R.

(i) If m and n are positive integers and $a \in R$, then
$a^m \cdot a^n = a^{m+n}$, and
$(a^m)^n = a^{mn}$.

(ii) If m and n are arbitrary integers and $a, b \in R$, then
$(n + m)a = na + ma$

$(nm)a = n(ma) = m(na)$,
$n(a + b) = na + nb$,
$m(ab) = (ma)b = a(mb)$, and
$(ma)(nb) = mn(ab) = (mna)b$.

(iii) If $a_1, a_2, ..., a_m, b_1, ..., b_n \in R$ then
$(a_1 + ... + a_m)(b_1 + ... + b_n)$
$= a_1b_1 + ... + a_1b_n + a_2b_1 + ... + a_2b_n + ... + a_mb_1 + ... + a_mb_n$.

Try this simple exercise now.

E 11) If R is a ring and $a, b \in R$ such that $ab = ba$, then use induction on $n \in \mathbf{N}$ to derive the binomial expansion
$(a + b)^n = a^n + {}^nC_1a^{n-1}b + ... + {}^nC_ka^{n-k}b^k + ... + {}^nC_{n-1}ab^{n-1} + b^n$,
where ${}^nC_k = \dfrac{n!}{k!(n-k)!}$.

There are several other properties of rings that we will be discussing throughout this block. For now let us look closely at two types of rings, which are classified according to the behaviour of the multiplication defined on them.

9.4 TWO TYPES OF RINGS

The definition of a ring guarantees that the binary operation multiplication is associative and, along with +, satisfies the distributive laws. Nothing more is said about the properties of multiplication. If we place restrictions on this operation we get several types of rings. Let us introduce you to two of them now.

Definition : We say that a ring $(R, +, .)$ is **commutative** if . is commutative, i.e., if $ab = ba$ for all $a, b \in R$.

For example, Z, Q and R are commutative rings.

Definition : We say that a ring $(R, +, .)$ is a **ring with identity (or with unity)** if R has an identity element with respect to multiplication, i.e., if there exists an element e in R such that $ae = ea = a$ for all $a \in R$.

Can you think of such a ring? Aren't Z, Q and R examples of a ring with identity?

Try this quickie before we go to our next definition.

E 12) Prove that if a ring R has an identity element with respect to multiplication, then it is unique. (We denote this unique identity element in a ring with identity by the symbol 1.)

Now let us combine the previous two definitions.

Definition : We say that a ring $(R, +, .)$ is a **commutative ring with unity**, if it is a commutative ring and has the multiplicative identity element 1.

Thus, the rings Z, Q, R and C are all commutative rings with unity. The integer 1 is the multiplicative identity in all these rings.

We can also find commutative rings which are not rings with identity. For example, 2Z, the ring of all even integers is commutative. But it has no multiplicative identity.

Similarly, we can find rings with identity which are not commutative. For example, $M_2(R)$ has the unit element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ but it is not commutative. For instance,
if $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \text{ and}$$

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

Thus, $AB \neq BA$.

E 14) Show that the ring in E 7 is a commutative ring with identity.

E 15) Show that the set of matrices $\left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle| \, x \in R \right\}$ is a commutative ring with unity.

E 16) Let R be a Boolean ring (i.e., $a^2 = a \; \forall \; a \in R$). Show that $a = -a \; \forall \; a \in R$. Hence show that R must be commutative.

Now we will give an important example of a non-commutative ring with identity. This is the ring of real quaternions. It was first described by the Irish mathematician William Rowan Hamilton (1805-1865). It plays an important role in geometry, number theory and the study of mechanics.

Example 9 : Let $H = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbf{R} \}$, where i, j, k are symbols that satisfy $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

We define addition and multiplication in H by

$(a + bi + cj + dk) + (a_1 + b_1 i + c_1 j + d_1 k)$

$= (a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k$, and

$(a + bi + cj + dk)(a_1 + b_1 i + c_1 j + d_1 k) = (aa_1 - bb_1 - cc_1 - dd_1)$

$+ (ab_1 + ba_1 + cd_1 - dc_1)i + (ac_1 - bd_1 + ca_1 + db_1)j + (ad_1 + bc_1 - cb_1 + da_1)k$

(This multiplication may seem complicated. But it is not so. It is simply performed as for polynomials, keeping the relationships between i, j and k in mind.)

Show that H is a ring.

Solution : Note that $\{ \pm 1, \pm i, \pm j, \pm k \}$ is the group Q_8 (Example 4, Unit 4).

Now, you can verify that $(H, +)$ is an abelian group in which the additive identity is $0 = 0 + 0i + 0j + 0k$, multiplication in H is associative, the distributive laws hold and $1 = 1 + 0i + 0j + 0k$ is the unity in H.

Do you agree that H is not a commutative ring? You will if you remember that $ij \neq ji$, for example.

So far, in this unit we have discussed various types of rings. We have seen examples of commutative and non-commutative rings. Though non-commutative rings are very important, for the sake of simplicity we shall only deal with commutative rings henceforth. Thus, from now on, for us **a ring will always mean a commutative ring.** We would like you to remember that both + and . are commutative in a commutative ring.

Now, let us summarise what we have done in this unit.

9.5 SUMMARY

In this unit we discussed the following points.

1) Definition and examples of a ring.

2) Some properties of a ring like
   $a \cdot 0 = 0 = 0 \cdot a$,
   $a(-b) = -(ab) = (-a)b$,
   $(-a)(-b) = ab$,
   $a(b - c) = ab - ac$,
   $(b - c)a = ba - ca$
   $\forall$ a, b, c in a ring R.

3) The laws of indices for addition and multiplication, and the generalised distributive law.

4) Commutative rings, rings with unity and commutative rings with unity.

Henceforth, we will always assume that a ring means a commutative ring, unless otherwise mentioned.

9.6 SOLUTIONS/ANSWERS

E 1) Addition in Z_6^*

+	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Multiplication in Z_6^*

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the tables you can see that neither addition nor multiplication are binary operations in Z_6^*, since $0 \notin Z_6^*$. Thus, $(Z_6^*, +, .)$ can't be a ring.

E 2) We define addition and multiplication in $Q + \sqrt{2}Q$ by
$(a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c) + \sqrt{2}(b + d)$, and
$(a + \sqrt{2}b) \cdot (c + \sqrt{2}d) = (ac + 2bd) + \sqrt{2}(ad + bc)$ $\forall$ a, b, c, d $\in$ Q.

Since + is associative and commutative in R, the same holds for + in $Q + \sqrt{2}Q$. $0 = 0 + \sqrt{2}.0$ is the additive identity and $(-a) + \sqrt{2}(-b)$ is the additive inverse of $a + \sqrt{2}b$.

Since multiplication in R is associative, R5 holds also. Since multiplication distributes over addition in R, it does so in $Q + \sqrt{2}Q$ as well. Thus, $(Q + \sqrt{2}Q, +, .)$ is a ring.

E 3) + and . are well defined binary operations on R. R1, R2, R5 and R6 hold since the same properties are true for $M_2(R)$ (Example 5).

The zero element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. The additive inverse of $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is $\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$.
Thus, R is a ring.

E 4) $+$ and . are binary operations on R. You can check that $(R, +, .)$ satisfies R1-R6.

E 5) $\cup$ and $\cap$ are well defined binary operations on $\wp(X)$. Let us check which of the axioms R1-R6 is not satisfied by $(\wp(X), \cup, \cap)$. Since $\cup$ is abelian, R1 is satisfied.
Since $\cup$ is associative, R2 is satisfied.
Also, for any $A \subseteq X$, $A \cup \phi = A$. Thus, ϕ is the identity with respect to $\cup$.
Thus, R3 is satisfied.
Now, for any $A \subseteq X$, $A \neq \phi$, there is no $B \subseteq X$ such that $A \cup B = \phi$.
Thus, R4 is not satisfied. Hence, $(\wp(X), \cup, \cap)$ is not a ring.

E 6) Since R satisfies R1, R2, R5 and R6, so does Map (X, R). The zero element is $0 : X \to R : 0(x) = 0$. The additive inverse of $f : X \to R$ is $(-f) : X \to R$.
Thus, (Map (X, R), +, .) is a ring.

E 7) Firstly, $\oplus$ and $\odot$ are well defined binary operations on

R. Next, let us check if $(R, \oplus, \odot)$ satisfies R1-R6 $\forall$ a, b, c $\in$ R.

R1 : $a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$.

R2 : $(a \oplus b) \oplus c = (a + b + 1) \oplus c = a + b + 1 + c + 1$

$= a + (b + c + 1) + 1 = a \oplus (b \oplus c)$

R3 : $a \oplus (-1) = a - 1 + 1 = a \; \forall \; a \in R$. Thus, (-1) is the identity with respect to $\oplus$

R4 : $a \oplus (-a - 2) = a + (-a - 2) + 1 = -1$. Thus, $-a - 2$ is the inverse of a with respect to $\oplus$.

R5 : $(a \odot b) \odot c = (ab + a + b) \odot c = (ab + a + b)c + (ab + a + b) + c$

$= a(bc + b + c) + a + (bc + b + c)$

$= a \odot (b \odot c)$.

R6 : $a \odot (b \oplus c) = a \odot (b + c + 1) = a(b + c + 1) + a + (b + c + 1)$
$= (ab + a + b) + (ac + a + c) + 1$
$= (a \odot b) \oplus (a \odot c)$.

Thus, $(R, \oplus, \odot)$ is a ring.

E 8) $Z_2 = \{\bar{0}, \bar{1}\}$, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$
$\therefore Z_2 \times Z_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}) (\bar{1}, \bar{1}) (\bar{1}, \bar{2})\}$.

Thus, the tables are

τ	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$

$*$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$
$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{2})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{2})$
$(\bar{1}, \bar{2})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{2})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{1})$

E 9) Note that + and . are binary operations on {0}. The properties R1-R6 are trivially satisfied.

Now, suppose a singleton {a} is a ring. Then this must contain the additive identity 0. Thus, {a} = {0}.

E 10) We know that $a + 0 = a \; \forall \; a \in R$. Since $a + 0 = a.0$, we find that $a.0 = a \; \forall \; a \in R$. But, by Theorem 1 we know that $a.0 = 0$. Thus, $a = 0 \; \forall \; a \in R$. That is, $R = \{0\}$.

E 11) Since $(a + b)^1 = a^1 + b^1$, the statement is true for $n = 1$. Assume that the equality is true for $n = m$, i.e.,

$(a + b)^m = a^m + {}^mC_1 a^{m-1}b + \ldots + {}^mC_{m-1} ab^{m-1} + b^m$.

Now, $(a + b)^{m+1} = (a + b)(a + b)^m = (a + b)\left(\sum_{0}^{m} {}^mC_k a^{m-k} b^k\right)$

$= \sum_{k=0}^{m} {}^mC_k a^{m-k+1} b^k + \sum_{k=0}^{m} {}^mC_k a^{m-k} b^{k+1}$, by distributivity.

$= (a^{m+1} + {}^mC_1 a^{m+1-1} b + {}^mC_2 a^{m+1-2} b^2 + \ldots + {}^mC_m ab^m)$

$+ ({}^mC_0 a^m b + {}^mC_1 a^{m-1} b^2 + \ldots + {}^mC_{m-1} ab^m + b^{m+1})$

$= a^{m+1} + ({}^mC_1 + {}^mC_0) a^{m+1-1} b + \ldots + ({}^mC_k + {}^mC_{k-1}) a^{m+1-k} b^k + \ldots + b^{m+1}$

$= a^{m+1} + {}^{m+1}C_1 a^{m+1-1} b + \ldots + {}^{m+1}C_k a^{m+1-k} b^k + \ldots + {}^{m+1}C_m ab^m + b^{m+1}$

(since ${}^mC_k + {}^mC_{k-1} = {}^{m+1}C_k$)

Thus, the equality is true for $n = m + 1$ also.

Hence, by the principle of induction, it is true for all n.

E 12) Let e and e′ be two multiplicative identity elements of R. Then

$e = e.e'$, since e is a multiplicative identity.

$= e'$, since e is a multiplicative identity.

Thus, $e = e'$, i.e., the multiplicative identity of R is unique.

E 13) For $n = 1$, $nZ = Z$ is a commutative ring with identity 1.

$\forall \; n > 1$, nZ is commutative, but without identity.

Z_n is commutative with identity $\bar{1}$.

$Z + iZ$ is commutative with identity $1 + 0i$.

$\mathcal{P}(X)$ is commutative with identity X, since $A \cap X = A \; \forall \; A \subseteq X$.

$C[0, 1]$ is commutative with identity $1 : [0, 1] \to R$ $x \mapsto 1$.

End A is not commutative. It has identity $I_A : A \to A$ $I_A(x) = x$.

E 14) Since $a \odot b = b \odot a \; \forall \; a, b \in R$, $\odot$ is commutative. Also, $a \odot 0 = a \; \forall \; a \in R$. Thus, 0 is the multiplicative identity.

E 15) You must first check that the set satisfies R1-R6.

Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity.

Then you should check that $AB = BA$ for any two elements A and B. Thus, the ring is commutative. It has identity $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$.

E 16) For any $a \in R$, $a^2 = a$.

In particular, $(2a)^2 = 2a \implies 4a^2 = 2a \implies 4a = 2a \implies 2a = 0$

$\implies a = -a$.

Now, for any $a, b \in R$, $a + b \in R$.

$\therefore (a + b)^2 = a + b \implies a^2 + ab + ba + b^2 = a + b$

$\implies a + ab + ba + b = a + b$, since $a^2 = a$ and $b^2 = b$

$\implies ab = -ba$

$\implies ab = ba$, since $-ba = ba$.

Thus, R is commutative.

UNIT 10 SUBRINGS AND IDEALS

Structure

10.1 INTRODUCTION

In this unit we will study various concepts in ring theory corresponding to some of those that we discussed in group theory. We start with the notion of a subring, which corresponds to that of a subgroup, as you may have guessed already.

Then we take a close look at a special kind of subring, called an ideal. You will see that the ideals in a ring play the role of normal subgroups in a group. That is, they help us to define a notion in ring theory corresponding to that of a quotient group, namely, a quotient ring.

After defining quotient rings, we will look at several examples of such rings. But you will only be able to realise the importance of quotient rings in the future units.

We hope that you will be able to meet the following objectives of this unit, because only then will you be comfortable in the future units of this course.

Objectives

After reading this unit you should be able to

- give examples of subrings and ideals of some familiar rings;
- check whether a subset of a ring is a subring or not;
- check whether a subset of a ring is an ideal or not;
- define and give examples of quotient rings.

10.2 SUBRINGS

In Unit 3 we introduced you to the concept of subgroups of a group. In this section we will introduce you to an analogous notion for rings. Remember that **for us a ring means a commutative ring.**

In the previous unit you saw that, not only is $\mathbb{Z} \subseteq \mathbb{Q}$, but $\mathbb{Z}$ and $\mathbb{Q}$ are rings with respect to the same operations. This shows that $\mathbb{Z}$ is a subring of $\mathbb{Q}$, as you will now realise.

Definition : Let $(R, +, .)$ be a ring and S be a subset of R. We say that S is a **subring** of R, if $(S, +, .)$ is itself a ring, i.e., S is a ring with respect to the operations on R.

For example, using Example 1 of Unit 9 we can say that $2\mathbb{Z}$, the set of even integers, is a subring of $\mathbb{Z}$.

Before giving more examples, let us analyse the definition of a subring. The definition says that a subring of a ring R is a ring with respect to the operations on R. Now, the distributive, commutative and associative laws hold good in R. Therefore, they hold good in any subset of R also. So, to prove that a subset S of R is a ring we don't need to check all the 6 axioms R1-R6 for S. It is enough to check that

i) S is closed under both $+$ and $.$,

ii) $0 \in S$, and

iii) for each $a \in S$, $-a \in S$

If S satisfies these three conditions, then S is a subring of R. So we have an alternative definition for a subring.

Definition : Let S be a subset of a ring (R, +, .). S is called a subring of R if

i) S is closed under + and . , i.e., $a + b, a . b \in S$ whenever $a, b \in S$,

ii) $0 \in S$, and

iii) for each $a \in S$, $-a \in S$.

Even this definition can be improved upon. For this, recall from Unit 3 that $(S, +) \leq (R, +)$ if $a - b \in S$ whenever $a, b \in S$. This observation allows us to give a set of conditions for a subset to be a subring, which are easy to verify.

Theorem 1 : Let S be a non-empty subset of (R, +, .). Then S is a subring of R if and only if

a) $x - y \in S \; \forall \; x, y \in S$; and

b) $xy \in S \; \forall \; x, y \in S$.

Proof : We need to show that S is a subring of R according to our definition iff S satisfies (a) and (b). Now, S is a subring of R iff $(S, +) \leq (R, +)$ and S is closed under multiplication, i.e., iff (a) and (b) hold.

So, we have proved the theorem.

This theorem allows us a neat way of showing that a subset is a subring.

Let us look at some examples.

We have already noted that **Z** is a subring of **Q**. In fact, you can use Theorem 1 to check that **Z** is subring of **R**, **C** and $\mathbf{Z} + i\mathbf{Z}$ too. You can also verify that **Q** is a subring of **R**, **C** and $\mathbf{Q} + \sqrt{2}\,\mathbf{Q} = \{ \alpha + \sqrt{2}\,\beta \mid \alpha, \beta \in \mathbf{Q} \}$.

The following exercise will give you some more examples of subrings.

E 1) Show that **R** is a subring of **C**, $\mathbf{Z} + i\mathbf{Z}$ is a subring of **C** and $\mathbf{Q} + \sqrt{2}\,\mathbf{Q}$ is a subring of **R**.

Now, let us look at some examples of subrings other than the sets of numbers.

Example 1 : Consider $\mathbf{Z}_6$, the ring of integers modulo 6. Show that $3\mathbf{Z}_6 = \{ 3.\bar{0}, 3.\bar{1}, ..., 3.\bar{5} \}$ is a subring of $\mathbf{Z}_6$.

Solution : Firstly, do you agree that $3\mathbf{Z}_6 = \{ \bar{0}, \bar{3} \}$? Remember that $\bar{6} = \bar{0}, \bar{9} = \bar{3}$, and so on. Also, $\bar{0} - \bar{3} = -\bar{3} = \bar{3}$. Thus, $x - y \in 3\mathbf{Z}_6 \; \forall \; x, y \in 3\mathbf{Z}_6$. You can also verify that $xy \in 3\mathbf{Z}_6 \; \forall \; x, y \in 3\mathbf{Z}_6$. Thus, by Theorem 1, $3\mathbf{Z}_6$ is a subring of $\mathbf{Z}_6$.

Example 2 : Consider the ring $\wp(X)$ given in Example 4 of Unit 9. Show that $S = \{ \phi, X \}$ is a subring of $\wp(X)$.

Solution : Note that $A \Delta A = \phi \; \forall \; A \in \wp(X)$. $\therefore \; A = -A$ in $\wp(X)$.
Now, to apply Theorem 1 we first note that S is non-empty.
Next, $\phi \Delta \phi = \phi \in S$, $X \Delta X = \phi \in S$,
$\phi \Delta X = X \in S$, $\phi \cap \phi = \phi \in S$, $X \cap X = X \in S$, $\phi \cap X = \phi \in S$
Thus, by Theorem 1, S is a subring of $\wp(X)$.

Try a related exercise now.

E 2) Let $A \subsetneq X$, $A \neq \phi$. Show that $S = \{ \phi, A, A^c, X \}$ is a subring of $\wp(X)$.

E 2 shows that for each proper subset of X we get a subring of $\wp(X)$. Thus, a ring can have several subrings. Let us consider two subrings of the ring $\mathbf{Z}$.

Example 3 : Show that $S = \{ (n, 0) \mid n \in \mathbf{Z} \}$ is a subring of $\mathbf{Z} \times \mathbf{Z}$. Also show that $D = \{ (n, n) \mid n \in \mathbf{Z} \}$ is a subring of $\mathbf{Z} \times \mathbf{Z}$.

Solution : You can recall the ring structure of Z^2 from Example 8 of Unit 9. Both S and D are non-empty. Both of them satisfy (a) and (b) of Theorem 1. Thus, S and D are both subrings of Z^2.

We would like to make a remark here which is based on the examples of subrings that you have seen so far.

Remark : i) If R is a ring with identity, a subring of R may or may not be with identity. For example, the ring Z has identity 1, but its subring nZ ($n \geq 2$) is without identity.

ii) The identity of a subring, if it exists, may not coincide with the identity of the ring. For example, the identity of the ring $Z \times Z$ is (1, 1). But the identity of its subring $Z \times \{0\}$ is (1, 0).

Try the following exercise now.

E 3) Show that $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in Z \right\}$ is a subring of $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in R \right\}$. Does S have a unit element?

If yes, then is the unit element the same as that of R?

Now let us look at an example which throws up several subrings of any ring.

Example 4 : Let R be a ring and $a \in R$. Show that the set $aR = \{ ax \mid x \in R \}$ is a subring of R.

Solution : Since $R \neq \phi$, $aR \neq \phi$. Now, for any two elements ax and ay of aR,

$ax - ay = a(x - y) \in aR$ and $(ax)(ay) = a(xay) \in aR$.

Thus, by Theorem 1, aR is a subring of R.

Using Example 4 we can immediately say that $\bar{m}Z_n$ is a subring of $Z_n \forall\ \bar{m} \in Z_n$. This also shows us a fact that we have already seen : nZ is a subring of $Z \forall\ n \in Z$.

Try these exercises now.

E 4) For any ring R, show that {0} and R are its subrings.

E 5) Show that if A is a subring of B and B is a subring of C, then A is a subring of C.

E 6) Give an example of a subset of Z which is not a subring.

E5 is very useful. For instance, E1 and E5 tell us that $Q + \sqrt{2}Q$ is a subring of C.

Now let us look at some properties of subrings. From Unit 3 you know that the intersection of two or more subgroups is a subgroup. The following result says that the same is true for subrings.

Theorem 2 : Let S_1 and S_2 be subrings of a ring R. Then $S_1 \cap S_2$ is also a subring of R.

Proof : Since $0 \in S_1$ and $0 \in S_2$, $0 \in S_1 \cap S_2$ $\therefore$ $S_1 \cap S_2 \neq \phi$.

Now, let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$. Thus, by Theorem 1, $x - y$ and xy are in S_1 as well as in S_2, i.e., they lie in $S_1 \cap S_2$.

Thus, $S_1 \cap S_2$ is a subring of R.

On the same lines as the proof above we can prove that the intersection of any family of subrings of a ring R is a subring of R.

Now consider the union of subrings of a ring. Do you think it will be a subring? Consider the following exercise.

E 7) You know that $\mathbf{Z} + i\mathbf{Z}$ and $\mathbf{Q}$ are subrings of $\mathbf{C}$. Is their union a subring of $\mathbf{C}$? Why?

Now let us look at the Cartesian product of subrings.

Theorem 3 : Let S_1 and S_2 be subrings of the rings R_1 and R_2, respectively. Then $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

Proof : Since S_1 and S_2 are subrings of R_1 and R_2, $S_1 \neq \phi$ and $S_2 \neq \phi$. $\therefore S_1 \times S_2 \neq \phi$.

Now, let (a, b) and $(a', b') \in S_1 \times S_2$. Then $a, a' \in S_1$ and $b, b' \in S_2$. As S_1 and S_2 are subrings, $a - a'$, $a \cdot a' \in S_1$ and $b - b'$, $b \cdot b' \in S_2$.
(We are using $+$ and $\cdot$ for both R_1 and R_2 here, for convenience.) Hence,
$(a, b) - (a', b') = (a - a', b - b') \in S_1 \times S_2$, and

$(a, b) \cdot (a', b') = (aa', bb') \in S_1 \times S_2$.

Thus, by Theorem 1, $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

You can use this result to solve the following exercise.

E 8) Obtain two proper non-trivial subrings of $\mathbf{Z} \times \mathbf{R}$ (i.e., subrings which are neither zero nor the whole ring).

Let us now discuss an important class of subrings.

10.3 IDEALS

In Block 2 you studied normal subgroups and the role that they play in group theory. You saw that the most important reason for the existence of normal subgroups is that they allow us to define quotient groups. In ring theory we would like to define a similar concept, a quotient ring. In this section we will discuss a class of subrings that will help us to do so. These subrings are called ideals. While exploring algebraic number theory, the 19th century mathematicians Dedekind, Kronecker and others developed this concept. Let us see how we can use it to define a quotient ring.

Consider a ring $(R, +, \cdot)$ and a subring I of R. As $(R, +)$ is an abelian group, the subgroup, I is normal in $(R, +)$, and hence the set $R/I = \{ a + I \mid a \in R \}$, of all cosets of I in R, is a group under the binary operation $+$ given by
$(a + I) + (b + I) = (a + b) + I$ ..... (1)
for all $a + I, b + I \in R/I$. We wish to define $\cdot$ on R/I so as to make R/I a ring. You may think that the most natural way to do so is to define
$(a + I) \cdot (b + I) = ab + I \forall a + I, b + I \in R$ .... (2)

But, is this well defined? Not always. For instance, consider the subring Z of R and the set of cosets of Z in R. Now, since $1 = 1 - 0 \in Z$, $1 + Z = 0 + Z$.

Therefore, we must have
$(\sqrt{2} + Z) \cdot (1 + Z) = (\sqrt{2} + Z) \cdot (0 + Z)$, i.e., $\sqrt{2} \quad Z = 0 + Z$, i.e., $\sqrt{2} \in Z$.

But this is a contradiction. Thus, our definition of multi' ... is not valid for the set R/Z.

But, it is valid for R/I if we add some condition ... ? What should these conditions be? To answer this, assume that the multiplication in ... is well defined.
Then, $(r + I) \cdot (0 + I) = r \cdot 0 + I = 0 + I = I$ for all $r \in R$

Now, you know that if $x \in I$, then $x + I = 0 + I = I$.
As we have assumed that $\cdot$ is well defined, we get
$(r + I) \cdot (x + I) = (r + I) \cdot (0 + I) = 0 + I$ whenever $r \in R$, $x \in I$.
i.e. $rx + I = I$ whenever $r \in R$, $x \in I$.

Thus, $rx \in I$, whenever $r \in R$, $x \in I$.

So, if . is well defined we see that the subring I must satisfy the additional condition that $rx \in I$ whenever $r \in R$ and $x \in I$.

In Sec. 10.4 we will prove that this extra condition on I is enough to make the operation . a well defined one and $(R/I, +, .)$ a ring. In this section we will consider the subrings I of R on which we impose the condition
$rx \in I$ whenever $r \in R$ and $x \in I$.

Definition : We call a non-empty subset I of a ring $(R, +, .)$ an ideal of R if

i) $a - b \in I$ for all $a, b \in I$, and

ii) $ra \in I$ for all $r \in R$ and $a \in I$.

Over here we would like to remark that we are always assuming that our rings are commutative. In the case of non-commutative rings the definition of an ideal is partially modified as follows.

A non-empty subset I of a **non-commutative ring R** is an ideal if

i) $a - b \in I \; \forall \; a, b \in I$, and

ii) $ra \in I$ and $ar \in I \; \forall \; a \in I, r \in R$.

Now let us go back to commutative rings. From the definition we see that **a subring I of a ring R is an ideal of R iff $ra \in I \; \forall \; r \in R$ and $a \in I$.**

Let us consider some examples. In E 4 you saw that for any ring R, the set $\{0\}$ is a subring. In fact, it is an ideal of R called the **trivial ideal of R.** Other ideals, if they exist, are known as **non-trivial ideals of R.**

You can also verify that every ring is an ideal of itself. If an ideal I of a ring R is such that $I \neq R$, then I is called a **proper ideal** of R.

For example, if $n \neq 0, 1$, then the subring $nZ = \{ nm \mid m \in Z \}$ is a proper non-trivial ideal of Z. This is because for any $z \in Z$ and $nm \in nZ$, $z(nm) = n(zm) \in nZ$.

Try this exercise now.

E 9) Show that $\{ \bar{0}, \bar{3} \}$ and $\{ \bar{0}, \bar{2}, \bar{4} \}$ are proper ideals of Z_6.

Now let us consider some more examples of ideals.

Example 5 : Let X be an infinite set. Consider I, the class of all finite subsets of X. Show that I is an ideal of $\wp(X)$.

Solution : $I = \{A \mid A$ is a finite subset of X $\}$. Note that

i) $\phi \in I$, i.e., the zero element of $\wp(X)$ is in I.

ii) $A - B = A + (-B) = A + B$, as $B = -B$ in $\wp(X)$
$= A \Delta B$.

Thus, if $A, B \in I$, then $A + B$ is again a finite subset of X, and hence $A - B \in I$.

iii) $AB = A \cap B$. Now, whenever A is a finite subset of X and B is any element of $\wp(X)$, $A \cap B$ is a finite subset of X. Thus, $A \in I$ and $B \in \wp(X) \Rightarrow AB \in I$.

Hence, I is an ideal of $\wp(X)$.

Example 6 : Let X be a set and Y be a non-empty subset of X. Show that
$I = \{ A \in \wp(X) \mid A \cap Y = \phi \}$ is an ideal of $\wp(X)$.

In particular, if we take $Y = \{x_0\}$, where x_0 is a fixed element of X, then
$I = \{ A \in \wp(X) \mid x_0 \notin A \}$ is an ideal of $\wp(X)$.

Solution : Firstly, $\phi \in I$.
Secondly, $\forall \; A, B \in I$,
$(A - B) \cap Y = (A \Delta B) \cap Y = (A \cap Y) \Delta (B \cap Y) = \phi \Delta \phi = \phi$, so that $A - B \in I$.

Finally, for $A \in I$ and $B \in \mathcal{P}(X)$,
$(AB) \cap Y = (A \cap B) \cap Y = (A \cap Y) \cap B = \phi \cap B = \phi$, so that $AB \in I$.
Thus, I is an ideal of $\mathcal{P}(X)$.

Example 7 : Consider the ring C[0, 1] given in Example 6 of Unit 9.
Let $M = \{ f \in C[0, 1] \mid f(1/2) = 0 \}$. Show that M is an ideal of C[0, 1].

Solution : The zero element 0 is defined by $0(x) = 0$ for all $x \in [0, 1]$. Since $0(1/2) = 0$, $0 \in M$.
Also, if $f, g \in M$, then $(f - g)(1/2) = f(1/2) - g(1/2) = 0 - 0 = 0$.
So, $f - g \in M$.

Next, if $f \in M$ and $g \in C[0, 1]$ then $(fg)(1/2) = f(1/2)\, g(1/2) = 0\, g(1/2) = 0$, so $fg \in M$.

Thus, M is an ideal of C[0, 1].

When you study Unit 11, you will see that M is the kernel of the homomorphism
$\phi : C[0, 1] \to \mathbf{R} : \phi(f) = f(1/2)$.

Now you can try an exercise that is a generalisation of Example 7.

E 10) Let $a \in [0, 1]$. Show that the set
$I_a = \{ f \in C[0, 1] \mid f(a) = 0 \}$ is an ideal of C[0, 1].

In the next exercise we ask you to look at the subring in Example 4.

E 11) Let R be a ring and $a \in R$. Show that Ra is an ideal of R.

Now that you've solved E 11, solving E 9 is a matter of seconds! Let us see if E 11 can be generalised.

Example 8 : For any ring R and $a_1, a_2 \in R$, show that
$Ra_1 + Ra_2 = \{ x_1a_1 + x_2a_2 \mid x_1, x_2 \in R \}$ is an ideal of R.

Solution : Firstly, $0 = 0a_1 + 0a_2$. $\therefore 0 \in Ra_1 + Ra_2$.
Next, $(x_1a_1 + x_2a_2) - (y_1a_1 + y_2a_2)$
$= (x_1 - y_1)a_1 + (x_2 - y_2)a_2 \in Ra_1 + Ra_2 \; \forall\, x_1, x_2, y_1, y_2 \in R$.

Finally, for $r \in R$ and $x_1a_1 + x_2a_2 \in Ra_1 + Ra_2$,
$r(x_1a_1 + x_2a_2) = rx_1a_1 + rx_2a_2 \in Ra_1 + Ra_2$.
Thus, $Ra_1 + Ra_2$ is an ideal of R.

This method of obtaining ideals can be extended to give ideals of the form
$\{ x_1a_1 + x_2a_2 + \ldots + x_na_n \mid x_i \in R \}$ for fixed elements $a_1, \ldots, a_n$ of R. Such ideals crop up again and again in ring theory. We give them a special name.

Definition : Let $a_1, \ldots, a_n$ be given elements of a ring R. Then the ideal generated by $a_1, \ldots, a_n$ is
$Ra_1 + Ra_2 + \ldots + Ra_n = \{ x_1a_1 + x_2a_2 + \ldots + x_na_n \mid x_i \in R \}$. $a_1, \ldots, a_n$ are called the generators of this ideal.

We also denote this ideal by $< a_1, a_2, \ldots, a_n >$.
When $n = 1$, the ideal we get is called a **principal ideal**. Thus, if $a \in R$, then $Ra = < a >$ is a principal ideal of R. In the next block you will be using principal ideals quite a lot.

Now an exercise on principal ideals.

E 12) Let R be a ring with identity. Show that $< 1 > = R$.

E 13) Find the principal ideals of Z_{10} generated by $\bar{3}$ and $\bar{5}$.

Now we look at a special ideal of a ring. But, to do so we need to give a definition.

Definition : An element a of a ring R is called **nilpotent** if there exists a positive integer n such that $a^n = 0$.

For example, $\overline{3}$ and $\overline{6}$ are nilpotent elements of Z_9, since $\overline{3}^2 = \overline{9} = \overline{0}$ and $\overline{6}^2 = \overline{36} = \overline{0}$. Also, in any ring R, 0 is a nilpotent element.

Now consider the following example.

Example 9 : Let R be a ring. Show that the set of nilpotent elements of R is an ideal of R. This ideal is called the **nil radical** of R.

Solution : Let $N = \{ a \in R \mid a^n = 0 \text{ for some positive integer } n \}$. Then $0 \in N$.

Also, if $a, b \in N$, then $a^n = 0$ and $b^m = 0$ for some positive integers m and n.

Now, $(a - b)^{m+n} = \sum_{r=0}^{m+n} {}^{m+n}C_r \, a^r(-b)^{m+n-r}$ (see E 11 of Unit 9).

For each $r = 0, 1, \ldots, m + n$, either $r \geq n$ or $m + n - r \geq m$, and hence, either $a^r = 0$ or $b^{m+n-r} = 0$. Thus, the term $a^r b^{m+n-r} = 0$. So $(a - b)^{m+n} = 0$.
Thus, $a - b \in N$ whenever $a, b \in N$.

Finally, if $a \in N$, $a^n = 0$ for some positive integer n, and hence, for any $r \in R$, $(ar)^n = a^n r^n = 0$, i.e., $ar \in N$.

So, N is an ideal of R.

Let us see what the nil radicals of some familiar rings are. For the rings **Z**, **Q**, **R** or **C**, $N = \{0\}$, since the power of any non-zero element of these rings is non-zero.

For Z_4, $N = \{ \overline{0}, \overline{2} \}$.

Try the following exercises now.

E 14) Find the nil radicals of Z_8 and $\mathcal{P}(X)$.

E 15) Let R be a ring and $a \in R$. Show that $I = \{ r \in R \mid ra = 0 \}$ is an ideal of R. (This ideal is called the annihilator of a.)

By now you must be familiar with the concept of ideals. Let us now obtain some results about ideals.

Theorem 4 : Let R be a ring with identity 1. If I is an ideal of R and $1 \in I$, then $I = R$.

Proof : We know that $I \subseteq R$. We want to prove that $R \subseteq I$. Let $r \in R$. Since $1 \in I$ and I is an ideal of R, $r = r.1 \in I$. So, $R \subseteq I$. Hence $I = R$.

Using this result we can immediately say that **Z** is not an ideal of **Q**. Does this also tell us whether **Q** is an ideal of **R** or not? Certainly. Since $1 \in Q$ and $Q \neq R$, Q can't be an ideal of R.

Now let us shift our attention to the algebra of ideals. In the previous section we proved that the intersection of subrings is a subring. We will now show that the intersection of ideals is an ideal. We will also show that the sum of ideals is an ideal and a suitably defined product of ideals is an ideal.

Theorem 5 : If I and J are ideals of a ring R, then

a) $I \cap J$,

b) $I + J = \{ a + b \mid a \in I \text{ and } b \in J \}$, and

c) $IJ = \{ x \in R \mid x \text{ is a finite sum } a_1b_1 + \ldots + a_mb_m, \text{ where } a_i \in I \text{ and } b_i \in J \}$ are ideals of R.

Proof : a) From Theorem 2 you know that $I \cap J$ is a subring of R. Now, if $a \in I \cap J$, then $a \in I$ and $a \in J$. Therefore, $ax \in I$ and $ax \in J$ for all x in R. So $ax \in I \cap J$ for all $a \in I \cap J$ and $x \in R$. Thus, $I \cap J$ is an ideal of R.

b) Firstly, $0 = 0 + 0 \in I + J \therefore I + J \neq \phi$.
Secondly, if $x, y \in I + J$, then $x = a_1 + b_1$ and $y = a_2 + b_2$ for some $a_1, a_2 \in I$ and $b_1, b_2 \in J$.
So $x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$.
Finally, let $x \in I + J$ and $r \in R$. Then $x = a + b$ for some $a \in I$ and $b \in J$. Now
$xr = (a + b)r = ar + br \in I + J$, as $a \in I$ implies $ar \in I$ and $b \in J$ implies $br \in J$ for all $r \in R$.
Thus, $I + J$ is an ideal of R.

c) Firstly, $IJ \neq \phi$, since $I \neq \phi$ and $J \neq \phi$.
Next, let $x, y \in IJ$. Then $x = a_1b_1 + \ldots + a_mb_m$ and
$y = a'_1b'_1 + \ldots + a'_nb'_n$ for some $a_1, \ldots, a_m, a'_1, \ldots, a'_n \in I$ and $b_1, \ldots, b_m, b'_1, \ldots, b'_n \in J$.
$\therefore x - y = (a_1b_1 + \ldots + a_mb_m) - (a'_1b'_1 + \ldots + a'_nb'_n)$
$= a_1b_1 + \ldots + a_mb_m + (-a'_1)b'_1 + \ldots + (-a'_n)b'_n$
which is a finite sum of elements of the form ab with $a \in I$ and $b \in J$.
So, $x - y \in IJ$.
Finally, let $x \in IJ$ say $x = a_1b_1 + \ldots + a_nb_n$ with $a_i \in I$ and $b_i \in J$. Then, for any $r \in R$
$xr = (a_1b_1 + \ldots + a_nb_n)r = a_1(b_1r) + \ldots + a_n(b_nr)$,
which is a finite sum of elements of the form ab with $a \in I$ and $b \in J$.
(Note that $b_i \in J \implies b_ir \in J$ for all r in R.)
Thus, IJ is an ideal of R.

Over here, we would like to remark that if we define $IJ = \{ ab \mid a \in I, b \in J \}$, then IJ need not even be a subring, leave alone being an ideal. This is because if $x, y \in IJ$, then with this definition of IJ it is not necessary that $x - y \in IJ$.

Let us now look at the relationship between the ideals obtained in Theorem 5. Let us first look at the following particular situation :
$R = \mathbb{Z}$, $I = 2\mathbb{Z}$ and $J = 10\mathbb{Z}$. Then $I \cap J = J$, since $J \subseteq I$. Also, any element of $I + J$ is of the form $x = 2n + 10m$, where $n, m \in \mathbb{Z}$. Thus, $x = 2(n + 5m) \in 2\mathbb{Z}$. On the other hand $2\mathbb{Z} = I \subseteq I + J$. Thus, $I + J = \langle 2, 10 \rangle = \langle 2 \rangle$.
Similarly, you can see that $IJ = \langle 20 \rangle$.
Note that $IJ \subseteq I \cap J \subseteq I \subseteq I + J$.
In fact, these inclusions are true for any I and J (see E 16). We show the relationship in Fig. 1.

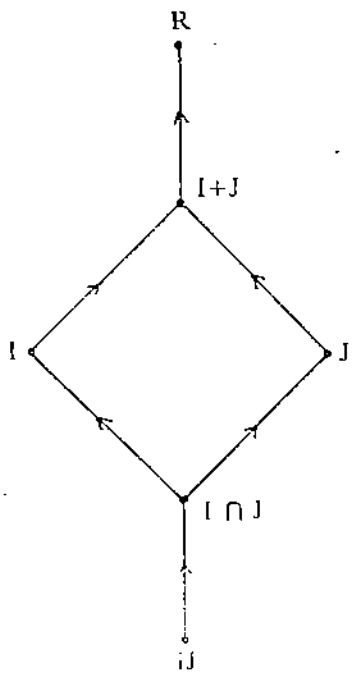


Fig. 1 : The ideal hierarchy!

E 16) If I and J are ideals of a ring R, then show that

a) $IJ \subseteq I \cap J \subseteq I \subseteq I + J$
and $IJ \subseteq I \cap J \subseteq J \subseteq I + J$;

b) $I + J$ is the smallest ideal containing both the ideals I and J, i.e., if A is an ideal of R containing both I and J, then A must contain $I + J$.

c) $I \cap J$ is the largest ideal that is contained in both I and J;

d) if $1 \in R$ and $I + J = R$, then $IJ = I \cap J$, i.e., if the top two of Fig. 1 are equal, then so are the lowest two.

Let us now go back to what we said at the beginning of this section—the importance of ideals.

10.4 QUOTIENT RINGS

In Unit 5 you have studied quotient groups. You know that given a normal subgroup N of a group G, the set of all cosets of N is a group and is called the quotient group associated with the normal subgroup N. Using ideals, we will now define a similar concept for rings. At the beginning of Sec. 10.3 we said that if $(R, +, .)$ is a ring and I is a subring of R such that $(R/I, +, .)$ is a ring, where $+$ and $.$ are defined by
$(x + I) + (y + I) = (x + y) + I$ and
$(x + I) . (y + I) = xy + I \; \forall \; x + I, y + I \in R/I$,
then the subring I should satisfy the extra condition that $rx \in I$ whenever $r \in R$ and $x \in I$, i.e., I should be an ideal. We now show that if I satisfies this extra condition then the operations that we have defined on R/I are well defined.

From group theory we know that $(R/I, +)$ is an abelian group. So we only need to check that . is well defined, i.e., if
$a + I = a' + I$, $b + I = b' + I$, then $ab + I = a'b' + I$.
Now, since $a + I = a' + I$, $a - a' \in I$.
Let $a - a' = x$. Similarly, $b - b' \in I$, say $b - b' = y$.
Then $ab = (a' + x)(b' + y) = a'b' + (xb' + a'y + xy)$.
$\therefore$ $ab - a'b' \in I$, since $x \in I$, $y \in I$ and I is an ideal of R.
$\therefore$ $ab + I = a'b' + I$.
Thus, . is well defined on R/I.

Now our aim is to prove the following result.

Theorem 6 : Let R be a ring and I be an ideal in R. Then R/I is a ring with respect to addition and multiplication defined by
$(x + I) + (y + I) = (x + y) + I$, and
$(x + I)(y + I) = xy + I \; \forall \; x, y \in R$.

Proof : As we have noted earlier, $(R/I, +)$ is an abelian group. So, to prove that R/I is a ring we only need to check that . is commutative, associative and distributive over $+$.

Now,

i) . is commutative : $(a + I).(b + I) = ab + I = ba + I = (b + I).(a + I)$ for all $a + I, b + I \in R/I$.

ii) . is associative : $\forall$ $a, b, c \in R$
$((a + I).(b + I)).(c + I) = (ab + I).(c + I)$
$= (ab)c + I$
$= a(bc) + I$
$= (a + I).((b + I).(c + I))$

iii) Distributive law : Let $a + I, b + I, c + I \in R/I$. Then
$(a + I).((b + I) + (c + I)) = (a + I)[(b + c) + I]$
$= a(b + c) + I$
$= (ab + ac) + I$
$= (ab + I) + (ac + I)$.
$= (a + I).(b + I) + (a + I).(c + I)$

Thus, R/I is a ring.

This ring is called the **quotient ring** of R by the ideal I.

R/I is read as 'R modulo I' or 'R mod I'

Let us look at some examples. We start with the example that gave rise to the terminology 'R mod I'.

Example 10 : Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. What is R/I?

Solution : In Sec. 10.3 you have seen that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. From Unit 2 you know that
$\mathbb{Z}/n\mathbb{Z} = \{ n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z} \}$.
$= \{ \bar{0}, \bar{1}, ..., \overline{n-1} \}$, the same as the set of equivalence classes modulo n.

So, R/I is the ring $\mathbb{Z}_n$.

Now let us look at an ideal of $\mathbb{Z}_n$, where $n = 8$.

Example 11 : Let $R = \mathbb{Z}_8$. Show that $I = \{ \bar{0}, \bar{4} \}$ is an ideal of R. Construct the Cayley tables for $+$ and . in R/I.

Solution : $I = \bar{4}R$, and hence is an ideal of R. From group theory you know that the number of elements in $R/I = o(R/I) = \frac{o(R)}{o(I)} = \frac{8}{2} = 4$.

You can see that these elements are
$0 + I = \{ \bar{0}, \bar{4} \}, 1 + I = \{ \bar{1}, \bar{5} \}, 2 + I = \{ \bar{2}, \bar{6} \}, 3 + I = \{ \bar{3}, \bar{7} \}$.

The Cayley tables for $+$ and . in R/I are

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

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

Try this exercise now.

E 17) Show that if R is a ring with identity, then R/I is a ring with identity for any ideal I of R.

E 18) If R is a ring with identity 1 and I is an ideal of R containing 1, then what does R/I look like?

E 19) Let N be the nil radical of R. Show that R/N has no non-zero nilpotent elements.

You will realise the utility and importance of quotient rings after we discuss homomorphisms in the next unit, and when we discuss polynomial rings (Block 4).

Now let us briefly summarise what we have done in this unit.

10.5 SUMMARY

In this unit we have discussed the following points, with the assumption that all rings are commutative.

1. The definition and examples of a subring.
2. The proof and use of the fact that a non-empty subset S of a ring R is a subring of R iff $x - y \in S$ and $xy \in S \; \forall \; x, y \in S$.
3. The intersection of subrings of a ring is a subring of the ring.
4. The Cartesian product of subrings is a subring of the Cartesian product of the corresponding rings.
5. The definition and examples of an ideal.
6. The definition of an ideal generated by n elements.
7. The set of nilpotent elements in a ring is an ideal of the ring.

8. If I is an ideal of a ring R with identity and $1 \in I$, then $I = R$.
9. If I and J are ideals of a ring R, then $I \cap J$, $I + J$ and IJ are also ideals of R.
10. The definition and examples of a quotient ring.

10.6 SOLUTIONS/ANSWERS

E 1) $\forall\ x, y \in R$, $x - y \in R$ and $xy \in R$. Thus, R is a subring of C. Similarly, you can check the other two cases.

E 2) Clearly, S is non-empty.
Also, for any $x, y \in S$, $x - y = x \Delta (-y) = x \Delta y$
(as pointed out in Example 2).
You can check that $x \Delta y \in S\ \forall\ x, y \in S$.
Also, for any $x, y \in S$, $x.y = x \cap y \in S$, as you can check.
Thus, S is a subring of $\wp(X)$.

E 3) Firstly, $S \neq \phi$. Secondly, for any $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $C = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ in S,

$$A - C = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S \text{ and } AC = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S.$$

Thus, S is a subring of R.

The unit element of $S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = the unit element of R.

E 4) Both {0} and R are non-empty and satisfy (a) and (b) of Theorem 1.

E 5) Since A is a subring of B, $A \neq \phi$ and $\forall\ x, y \in A$, $x - y \in A$ and $xy \in A$. Here the addition and multiplication are those defined on B. But these are the same as those defined on C since B is a subring of C. Thus, A satisfies Theorem 1, and hence is a subring of C.

E 6) There are several examples. We take {1}. In fact, any finite subset of Z, apart from {0}, will do.

E 7) $1 + i$ and $\frac{1}{2}$ are elements of the union.

But $1 + i - \frac{1}{2} = \frac{1}{2} + i \notin Z + iZ \cup Q$. Thus, $Z + iZ \cup Q$ is not a subring of C.

E 8) $2Z \times R$, $3Z \times \{0\}$ are two among infinitely many examples.

E 9) Note that the two sets are $\overline{3}Z_6$ and $\overline{2}Z_6$. From Example 4 you know that they are subrings of Z_6. Now, by element wise multiplication you can check that
$rx \in \overline{3}Z_6\ \forall\ r \in Z_6$ and $x \in \overline{3}Z_6$. (For instance, $\overline{5}.\overline{3} = \overline{15} = \overline{3} \in \overline{3}Z_6$.)
You can similarly see that $rx \in \overline{2}Z_6\ \forall\ r \in Z_6$, $x \in \overline{2}Z_6$.
Thus, $\overline{3}Z_6$ and $\overline{2}Z_6$ are ideals of Z_6.

E 10) $I_a \neq \phi$, since $0 \in I_a$.
$f, g \in I_a \Rightarrow (f - g)(a) = f(a) - g(a) = 0 \Rightarrow f - g \in I_a$.
$f \in I_a, g \in C[0, 1] \Rightarrow (fg)(a) = f(a)\, g(a) = 0.g(a) = 0 \Rightarrow fg \in I_a$.
$\therefore$ I_a is an ideal of C[0, 1].

E 11) Ra is a subring of R (see Example 4).
Also, for $r \in R$ and $xa \in Ra$,
$r(xa) = (rx)a \in Ra$.
$\therefore$ Ra is an ideal of R.

E 12) We know that $< 1 > \subseteq R$. We need to show that $R \subseteq < 1 >$.
Now, for any $r \in R$, $r = r.1 \in < 1 >$. Thus, $R \subseteq < 1 >$.
$\therefore$ $R = < 1 >$

E 13) $\bar{3}Z_{10} = \{ \bar{3}x \mid x \in Z_{10} \} = \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27} \}$
$= \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{2}, \bar{5}, \bar{8}, \bar{1}, \bar{4}, \bar{7} \}$
$= Z_{10}$.
$\bar{5}Z_{10} = \{ \bar{0}, \bar{5} \}$.

E 14) Let the nil radical of Z_8 be N. Then $\bar{0} \in N$.
$\bar{1} \notin N$ since $\bar{1}^n = \bar{1} \neq \bar{0}$ for all n.
$\bar{2}^3 = \bar{0} \implies \bar{2} \in N$.
$\bar{3}^n \neq \bar{0} \forall$ n. $\therefore \bar{3} \notin N$.
Similarly, you can check that $\bar{4}, \bar{6} \in N$ and $\bar{5}, \bar{7} \notin N$.
$\therefore N = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6} \}$.
For any $A \in \wp(X)$, $A^n = A \cap A \cap \ldots\ldots \cap A = A \forall$ n.
Thus, $A^n = \phi$ iff $A = \phi$. Thus, the nil radical of $\wp(X)$ is $\{ \phi \}$.

E 15) Firstly, $I \neq \phi$ since $0 \in I$.
Secondly, $r, s \in I \implies ra = 0 = sa \implies (r - s)a = 0 \implies r - s \in I$.
Finally, $r \in I$ and $x \in R \implies (rx)a = x(ra) = x0 = 0 \implies rx \in I$.
Thus, I is an ideal of R.

E 16) a) For any $a \in I$ and $b \in J$, $ab \in I$ and $ab \in J$.
Thus, $ab \in I \cap J$. Since $I \cap J$ is an ideal, any finite sum of such elements will also be in $I \cap J$. Thus, $IJ \subseteq I \cap J$.
Clearly, $I \cap J \subseteq I$ and $I \cap J \subseteq J$.
Also, $I \subseteq I + J$, $J \subseteq I + J$ is obvious.

b) Let A be an ideal of R containing I as well as J. Then certainly $I + J \subseteq A$. Thus, (b) is proved.

c) Let B be an ideal of R such that $B \subseteq I$ and $B \subseteq J$. Then certainly, $B \subseteq I \cap J$. Thus, (c) is proved.

d) We want to show that $I \cap J \subseteq IJ$.
Let $x \in I \cap J$. Then $x \in I$ and $x \in J$.
Since $1 \in R = I + J$, $1 = i + j$, for some $i \in I$ and $j \in J$.
$\therefore x = x.1 = xi + xj = ix + xj \in IJ$.
Thus, $I \cap J \subseteq IJ$.

E 17) $I + I$ is the identity of R/I.

E 18) From Theorem 4, you know that $I = R$.
$\therefore R/I = \{ \bar{0} \}$.

E 19) Let $x + N \in R/N$ be a nilpotent element.
Then $(x + N)^n = N$ for some positive integer n.
$\implies x^n \in N$ for some positive integer n.
$\implies (x^n)^m = 0$ for some positive integer m.
$\implies x^{nm} = 0$ for some positive integer nm.
$\implies x \in N$
$\implies x + N = 0 + N$, the zero element of R/N.
Thus, R/N has no non-zero nilpotent elements.

UNIT 11 RING HOMOMORPHISMS

Structure

11.1 INTRODUCTION

In Unit 6 you studied about functions between groups that preserve the binary operation. You also saw how useful they were for studying the structure of a group. In this unit we will discuss functions between rings which preserve the two binary operations. Such functions are called ring homomorphisms. You will see how homomorphisms allow us to investigate the algebraic nature of a ring.

If a homomorphism is a bijection, it is called an isomorphism. The role of isomorphisms in ring theory, as in group theory, is to identify algebraically identical systems. That is why they are important. We will discuss them also.

Finally, we will show you the interrelationship between ring homomorphisms, ideals and quotient rings.

Objectives

After reading this unit, you should be able to

- check whether a function is a ring homomorphism or not;
- obtain the kernel and image of any homomorphism;
- give examples of ring homomorphisms and isomorphisms;
- prove and use some properties of a ring homomorphism;
- state, prove and apply the Fundamental Theorem of Homomorphism for rings.

11.2 HOMOMORPHISMS

Analogous to the notion of a group homomorphism, we have the concept of a ring homomorphism. Recall that a group homomorphism preserves the group operation of its domain. So it is natural to expect a ring homomorphism to preserve the ring structure of its domain. Consider the following definition.

Definition : Let $(R_1, +, .)$ and $(R_2, \dot{+}, \dot{.})$ be two rings and $f : R_1 \to R_2$ be a map. We say that f is a **ring homomorphism** if
$f(a + b) = f(a) \dot{+} f(b)$, and
$f(a . b) = f(a) \dot{.} f(b)$ for all a, b in R_1.
Note that the $\dot{+}$ and $\dot{.}$ occurring on the left hand sides of the equations in the definition above are defined on R_2, while the $+$ and $.$ occurring on the right hand sides are defined on R_1.

So we can say that $f : R_1 \to R_2$ is a homomorphism if

(i) the image of a sum is the sum of the images, and

(ii) the image of a product is the product of the images

Thus, the ring homomorphism f is also a group homomorphism from $(R_1, +)$ into $(R_2, \dot{+})$.

Just as we did in Unit 6, before giving some examples of homomorphisms let us define the kernel and image of a homomorphism. As is to be expected, these definitions are analogous to the corresponding ones in Unit 6.

Definition : Let R_1 and R_2 be two rings and $f : R_1 \to R_2$ be a ring homomorphism. Then we define

i) the **image of f** to be the set $\text{Im } f = \{f(x) \mid x \in R_1\}$.

ii) the **kernel of f** to be the set $\text{Ker } f = \{x \in R_1 \mid f(x) = 0\}$.

Note that $\text{Im } f \subseteq R_2$ and $\text{Ker } f \subseteq R_1$.
If $\text{Im } f = R_2$, f is called an **epimorphism** or an **onto homomorphism**, and then R_2 is called the **homomorphic image** of R_1.

Now let us look at some examples.

Example 1 : Let R be a ring. Show that the identity map I_R is a ring homomorphism. What are $\text{Ker } I_R$ and $\text{Im } I_R$?
Solution : Let $x, y \in R$. Then
$I_R(x + y) = x + y = I_R(x) + I_R(y)$, and
$I_R(xy) = xy = I_R(x)\, I_R(y)$.
Thus, $I_R(xy) = xy = I_R(x)\, I_R(y)$.
Thus, I_R is a ring homomorphism.

$$\begin{aligned}\text{Ker } I_R &= \{x \in R \mid I_R(x) = 0\}\\ &= \{x \in R \mid x = 0\}\\ &= \{0\}\\ \text{Im } I_R &= \{I_R(x) \mid x \in R\}\\ &= \{x \mid x \in R\}\\ &= R.\end{aligned}$$

Thus, I_R is a surjection, and hence an epimorphism.

Example 2 : Let $s \in N$. Show that the map $f : Z \to Z_s$ given by $f(m) = \overline{m}$ for all $m \in Z$ is a homomorphism. Obtain Ker f and Im f also.
Solution : For any $m, n \in Z$,
$f(m + n) = \overline{m + n} = \overline{m} + \overline{n} = f(m) + f(n)$, and
$f(mn) = \overline{mn} = \overline{m}\,\overline{n} = f(m)\, f(n)$.
Therefore, f is a ring homomorphism.

$$\begin{aligned}\text{Now, Ker } f &= \{m \in Z \mid f(m) = \overline{0}\}\\ &= \{m \in Z \mid \overline{m} = \overline{0}\}\\ &= \{m \in Z \mid m \equiv 0 \pmod s\}\\ &= sZ.\\ \text{Im } f &= \{f(m) \mid m \in Z\}\\ &= \{\overline{m} \mid m \in Z\}\\ &= Z_s,\end{aligned}$$

showing that f is an epimorphism.

Example 3 : Consider the map $f : Z_6 \to Z_3 : f(n \pmod 6) = n \pmod 3$. Show that f is a ring homomorphism. What is Ker f?
Solution : Firstly, for any $n, m \in Z$,

$$\begin{aligned}f(n \pmod 6 + m \pmod 6) &= f((n + m) \pmod 6) = (n + m) \pmod 3\\ &= n \pmod 3 + m \pmod 3\\ &= f(n \pmod 6) + f(m \pmod 6)\end{aligned}$$

You can similarly show that
$f(n \pmod 6 \cdot m \pmod 6) = f(n \pmod 6) \cdot f(m \pmod 6)$.
Thus, f is a ring homomorphism.

$$\begin{aligned}\text{Ker } f &= \{n \pmod 6 \mid n \equiv 0 \pmod 3\} = \{n \pmod 6 \mid n \in 3Z\}\\ &\{\overline{0}, \overline{3}\}, \text{ bar denoting 'mod 6'.}\end{aligned}$$

Before discussing any more examples, we would like to make a remark about terminology. In future we will use the term 'homomorphism' for 'ring homomorphism'. You may remember that we also did this in the case of group homomorphisms.

Now for some exercises.

E 1) If S is a subring of a ring R, then S itself is a ring with the same + and . of R. Show that the inclusion map $i : S \to R : i(x) = x$ is a homomorphism. What are Ker i and Im i?

E 2) Let R_1 and R_2 be two rings. Define $f : R_1 \to R_2 : f(x) = 0$. Show that f is a homomorphism. Also obtain Ker f and Im f. (This function is called the **trivial homomorphism.**)

E 3) Is $f : \mathbf{Z} \to 2\mathbf{Z} : f(x) = 2x$ a homomorphism? Why?

Note that using E 1 we know that $f : \mathbf{Z} \to \mathbf{Q}$ (or $\mathbf{R}$, or $\mathbf{C}$ or $\mathbf{Z} + i\mathbf{Z}$) given by $f(n) = n$ is a homomorphism.

Now let us look at some more examples.

Example 4 : Consider the ring $C[0, 1]$ of all real valued continuous functions defined on the closed interval $[0, 1]$.
Define $\phi : C[0, 1] \to \mathbf{R} : \phi(f) = f(1/2)$. Show that ϕ is a homomorphism.

Solution : Let f and $g \in C[0, 1]$
Then $(f + g)(x) = f(x) + g(x)$ and
$(fg)(x) = f(x)\,g(x)$ for all $x \in C[0, 1]$.
Now, $\phi(f + g) = (f + g)(1/2) = f(1/2) + g(1/2) = \phi(f) + \phi(g)$, and
$\phi(fg) = (fg)(1/2) = f(\frac{1}{2})\,g(\frac{1}{2}) = \phi(f)\,\phi(g)$.

ϕ is called the evaluation map at the point $x = \frac{1}{2}$.

Thus, ϕ is a homomorphism.

Example 5 : Consider the ring $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \; a, b \in \mathbf{R} \right\}$ under matrix addition and multiplication. Show that the map $f : \mathbf{Z} \to R : f(n) = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$ is a homomorphism.

Solution : Note that $f(n) = nI$, where I is the identity matrix of order 2. Now you can check that $f(n + m) = f(n) + f(m)$ and $f(nm) = f(n)\,f(m)$ $\forall$ $n, m \in \mathbf{Z}$. Thus, f is a homomorphism.

Example 6 : Consider the ring $\wp(X)$ of Example 4 of Unit 9.
Let Y be a non-empty subset of X.
Define $f : \wp(X) \to \wp(Y)$ by $f(A) = A \cap Y$ for all A in $\wp(X)$. Show that f is a homomorphism. Does $Y^c \in$ Ker f? What is Im f?
Solution : For any A and B in $\wp(X)$,

$$\begin{aligned} f(A \,\Delta\, B) &= f((A \setminus B) \cup (B \setminus A)) \\ &= ((A \setminus B) \cup (B \setminus A) \cap Y) \\ &= ((A \cap Y) \setminus (B \cap Y)) \cup ((B \cap Y) \setminus (A \cap Y)) \\ &= (f(A) \setminus f(B)) \cup (f(B) \setminus f(A)) \\ &= f(A) \,\Delta\, f(B), \text{ and} \\ f(A \cap B) &= (A \cap B) \cap Y \\ &= (A \cap B) \cap (Y \cap Y) \\ &= (A \cap Y) \cap (B \cap Y), \text{ since } \cap \text{ is associative and commutative.} \\ &= f(A) \cap f(B). \end{aligned}$$

So, f is a ring homomorphism from $\wp(X)$ into $\wp(Y)$.
Now, the zero element of $\wp(Y)$ is ϕ. Therefore,
Ker $f = \{A \in \wp(X) \mid A \cap Y = \phi\}$. $\therefore$ $Y^c \in$ Ker f.
We will show that f is surjective.
Now, Im $f = \{A \cap Y \mid A \in \wp(X)\}$
Thus, Im $f \subseteq \wp(Y)$. To show that $\wp(Y) \subseteq$ Im f, take any $B \in \wp(Y)$.
Then $B \in \wp(X)$ and $f(B) = B \cap Y = B$. Thus, $B \in$ Im f.
Therefore, Im $f = \wp(Y)$.
Thus, f is an onto homomorphism.
The following exercises will give you some more examples of homomorphisms.

E 4) Let A and B be two rings. Show that the projection map $p : A \times B \to A : p(x, y) = x$ is a homomorphism. What are Ker p and Im p?

E 5) Is $f : \mathbf{Z} + \sqrt{2}\mathbf{Z} \to \mathbf{Z} + \sqrt{2}\mathbf{Z}$ $f(a + \sqrt{2}b) = a - \sqrt{2}b$ a homomorphism?

E 6) Show that the map $\phi : C[0, 1] \to \mathbf{R} \times \mathbf{R}$, $\phi(f) = (f(0), f(1))$ is a homomorphism.

Having discussed many examples, let us obtain some basic results about ring homomorphisms.

11.3 PROPERTIES OF HOMOMORPHISMS

Let us start by listing some properties that show how a homomorphism preserves the structure of its domain. The following result is only a restatement of Theorem 1 of Unit 6.

Theorem 1 : Let $f : R_1 \to R_2$ be a homomorphism from a ring R_1 into a ring R_2. Then
a) $f(0) = 0$,
b) $f(-x) = -f(x)\ \forall\ x \in R_1$, and
c) $f(x - y) = f(x) - f(y)\ \forall\ x, y \in R_1$.

Proof : Since f is a group homomorphism from $(R_1, +)$ to $(R_2, +)$, we can apply Theorem 1 of Unit 6 to get the result.

In the following exercise we ask you to prove another property of homomorphisms.

E 7) Let $f : R_1 \to R_2$ be an onto ring homomorphism. If R_1 is with identity 1, show that R_2 is with identity $f(1)$.

Now, let us look at direct and inverse images of subrings under homomorphisms. (See Sec. 1.5 for the definition of an inverse image.)

Theorem 2 : Let $f : R_1 \to R_2$ be a ring homomorphism. Then
a) if S is a subring of R_1, $f(S)$ is a subring of R_2;
b) if T is a subring of R_2, $f^{-1}(T)$ is a subring of R_1.

Proof : We will prove (b) and leave the proof of (a) to you (see E 8). Let us use Theorem 1 of Unit 10.

Firstly, since $T \neq \phi$, $f^{-1}(T) \neq \phi$. Next, let $a, b \in f^{-1}(T)$. Then $f(a), f(b) \in T$.
$\Rightarrow f(a) - f(b) \in T$ and $f(a)\, f(b) \in T$
$\Rightarrow f(a - b) \in T$ and $f(ab) \in T$
$\Rightarrow a - b \in f^{-1}(T)$ and $ab \in f^{-1}(T)$
$\Rightarrow f^{-1}(T)$ is a subring.
To complete the proof of Theorem 2, try E 8.

E 8) Prove (a) of Theorem 2.

Now, it is natural to expect an analogue of Theorem 2 for ideals. But consider the inclusion $i : \mathbb{Z} \to \mathbb{R} : i(x) = x$. You know that $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. But is $i(2\mathbb{Z})$ (i.e., $2\mathbb{Z}$) an ideal of $\mathbb{R}$? No. For example, $2 \in 2\mathbb{Z}$, $\frac{1}{4} \in \mathbb{R}$, but $2.\frac{1}{4} = \frac{1}{2} \notin 2\mathbb{Z}$. Thus, the homomorphic image of an ideal need not be an ideal. But, all is not lost. We have the following result

Theorem 3 : Let $f : R_1 \to R_2$ be a ring homomorphism.
a) If f is surjective and I is an ideal of R_1, then $f(I)$ is an ideal of R_2.
b) If I is an ideal of R_2, then $f^{-1}(I)$ is an ideal of R_1 and $\text{Ker } f \subseteq f^{-1}(I)$.

Proof : Here we will prove (a) and leave (b) to you (see E 9)!

Firstly, since I is a subring of R_1, $f(I)$ is a subring of R_2.
Secondly, take any $f(x) \in f(I)$ and $r \in R_2$. Since f is surjective, $\exists\ s \in R$, such that $f(s) = r$. Then
$rf(x) = f(s)\, f(x) = f(sx) \in f(I)$ since $sx \in I$.
Thus, $f(I)$ is an ideal of R_2.
To finish the proof try E 9.

E 9) Prove (b) of Theorem 3.

Now, consider an epimorphism $f : R \to S$ and an ideal I in R. By Theorem 3 you know that $f(I)$ is an ideal of S and $f^{-1}(f(I))$ is an ideal of R. How are I and $f^{-1}(f(I))$ related? Clearly, $I \subseteq f^{-1}(f(I))$. Can $f^{-1}(f(I))$ contain elements of $R \setminus I$? Remember that $\text{Ker } f \subseteq f^{-1}(f(I))$ also. Thus, $I + \text{Ker } f \subseteq f^{-1}(f(I))$. In fact, $I + \text{Ker } f = f^{-1}(f(I))$. Let us see why.

Let $x \in f^{-1}(f(I))$. Then $f(x) \in f(I)$. Therefore, $f(x) = f(y)$ for some $y \in I$. Then
$f(x - y) = 0$.
$\therefore x - y \in \text{Ker } f$, i.e., $x \in y + \text{Ker } f \subseteq I + \text{Ker } f$.
$\therefore f^{-1}(f(I)) \subseteq I + \text{Ker } f$.
Thus, $f^{-1}(f(I)) = I + \text{Ker } f$.
This tells us that if $\text{Ker } f \subseteq I$, then
$f^{-1}(f(I)) = I$ (since $\text{Ker } f \subseteq I \implies I + \text{Ker } f = I$).

Now you may like to do an easy exercise.

E 10) Let $f : R \to S$ be an onto ring homomorphism. Show that if J is an ideal of S, then $f(f^{-1}(J)) = J$.

Our discussion so far is leading us to the following theorem.

Theorem 4 : Let $f : R \to S$ be an onto ring homomorphism. Then

a) if I is an ideal in R containing $\text{Ker } f$, $I = f^{-1}(f(I))$

b) themapping $I \to f(I)$ defines a one-to-one correspondence between the set of ideals of R containing $\text{Ker } f$ and the set of ideals of S.

Proof : We have proved (a) in the discussion above. Let us prove (b) now.
Let A be the set of ideals of R containing $\text{Ker } f$, and B be the set of ideals of S.
Define $\phi : A \to B : \phi(I) = f(I)$.
We want to show that ϕ is one-one and onto.
ϕ is onto : If $J \in B$ then $f^{-1}(J) \in A$ and $\text{Ker } f \subseteq f^{-1}(J)$ by Theorem 3.
Now $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$, using E 10.
ϕ is one-one : If I_1 and I_2 are ideals in R containing $\text{Ker } f$, then
$\phi(I_1) = \phi(I_2) \implies f(I_1) = f(I_2)$
$\implies f^{-1}(f(I_1)) = f^{-1}(f(I_2))$
$\implies I_1 = I_2$, by (a).

Thus, ϕ is bijective.

Use this result for solving the following exercises.

E 11) Find the kernel of the homomorphism
$f : Z \to Z_{12} : f(z) = \overline{z}$.
Also find the ideals of Z_{12}.

E 12) Show that the homomorphism $f : Z \to Z \times Z : f(n) = (n, n)$ is not onto. Find an ideal in $Z \times Z$ which is not of the form $f(I)$, where I is an ideal of Z.

And now let us look closely at the sets $\text{Ker } f$ and $\text{Im } f$, where f is a ring homomorphism. In Unit 6 we proved that if $f : G_1 \to G_2$ is a group homomorphism then $\text{Ker } f$ is a normal subgroup of G_1 and $\text{Im } f$ is a subgroup of G_2. We have an analogous result for ring homomorphisms, which you may have already realised from the examples you have studied so far.

Theorem 5 : Let $f : R_1 \to R_2$ be a ring homomorphism. Then

a) $\text{Ker } f$ is an ideal of R_1.

b) $\text{Im } f$ is a subring of R_2

Proof : a) Since {0} is an ideal of R_2, by Theorem 3(b) we know that $f^{-1}(\{0\})$ is an ideal of R_1. But $f^{-1}(\{0\}) = \text{Ker } f$.
Thus, we have shown that Ker f is an ideal of R_1.

b) Since R_1 is a subring of R_1, $f(R_1)$ is a subring of R_2, by Theorem 2(a). Thus, Im f is a subring of R_2.

This result is very useful for showing that certain sets are ideals. For example, from Theorem 5 and Example 3 you can immediately say that $\{\bar{0}, \bar{3}\}$ is an ideal of Z_6. As we go along you will see more examples of this use of Theorem 5.

Let us look a little more closely at the kernel of a homomorphism. In fact, let us prove a result analogous to Theorem 4 of Unit 6.

An injective homomorphism is called a monomorphism.

Theorem 6 : Let $f : R_1 \to R_2$ be a homomorphism. Then f is injective iff Ker $f = \{0\}$.

Proof : f is injective iff f is an injective group homomorphism from $(R_1, +)$ into $(R_2, +)$. This is true iff Ker $f = \{0\}$, by Theorem 4 of Unit 6. So, our result is proved.

Using Theorem 6, solve the following exercise.

E 13) Which of the homomorphisms in Examples 1-6 are 1-1?

So far we have seen that given a ring homomorphism $f : R \to S$, we can obtain an ideal of R, namely, Ker f. Now, given an ideal I of a ring R can we define a homomorphism f so that Ker f = I?

The following theorem answers this question. Before going to the theorem recall the definition of quotient rings from Unit 10.

Theorem 7 : If I is an ideal of a ring R, then there exists a ring homomorphism $f : R \to R/I$ whose kernel is I.

Proof : Let us define $f : R \to R/I$ by $f(a) = a + I$ for all $a \in R$. Let us see if f is a homomorphism. For this take any $a, b \in R$. Then
$f(a + b) = (a + b) + I = (a + I) + (b + I) = f(a) + f(b)$, and
$f(ab) = ab + I = (a + I)(b + I) = f(a) f(b)$.

Thus, f is a homomorphism.
Further, Ker $f = \{ a \in R \mid f(a) = 0 + I \} = \{ a \in R \mid a + I = I \}$
$= \{ a \in R \mid a \in I \} = I$.
Thus, the theorem is proved.

Also note that the homomorphism f is onto.

We call the homomorphism defined in the proof above the canonical (or natural) homomorphism from R onto R/I.

Try this simple exercise now.

E 14) Let S be a subring of a ring R. Can we always define a ring homomorphism whose domain is R and kernel is S? Why?

Now let us look at the behaviour of the composition of homomorphisms. We are sure you find the following result quite unsurprising.

Theorem 8 : Let R_1, R_2 and R_3 be rings and $f : R_1 \to R_2$, and $g : R_2 \to R_3$ be ring homomorphisms. Then their composition $g \circ f : R_1 \to R_3$ given by $(g \circ f)(x) = g(f(x))$ for all $x \in R_1$ is a ring homomorphism.

The proof of this result is on the same lines as the proof of the corresponding result in Unit 6. We leave it to you (see the following exercise).

E 15) Prove Theorem 8.

E 16) In the situation of Theorem 8 prove that

a) if $g \circ f$ is $1-1$, then so is f.

b) if $g \circ f$ is onto, then so is g.

E 17) Use Theorem 8 to show that the function $h : Z \times Z \to Z_2$ defined by $h((n, m)) = \bar{m}$ is a homomorphism.

Now let us see what the ring analogue of a group isomorphism is.

11.4 THE ISOMORPHISM THEOREMS

In Unit 6 we discussed group isomorphisms and various results involving them. In this section we will do the same thing for rings. So, let us start by defining a ring isomorphism.

Definition : Let R_1 and R_2 be two rings. A function $f : R_1 \to R_2$ is called a **ring isomorphism** (or simply an isomorphism) if

i) f is a ring homomorphism,

ii) f is $1-1$, and

iii) f is onto.

Thus, a homomorphism that is bijective is an isomorphism.

An isomorphism of a ring R onto itself is called an **automorphism** of R.

If $f : R_1 \to R_2$ is an isomorphism, we say that R_1 is **isomorphic** to R_2, and denote it by $R_1 \cong R_2$.

Over here we would like to make the following remark.

Remark : Two rings are isomorphic if and only if they are algebraically identical. That is, isomorphic rings must have exactly the same algebraic properties. Thus, if R_1 is a ring with identity then it cannot be isomorphic to a ring without identity. Similarly, if the only ideals of R_1 are $\{0\}$ and itself, then any ring isomorphic to R_1 must have this property too.

Try the following exercises now. They will help you in becoming more familiar with isomorphisms.

E 18) Which of the following functions are ring isomorphisms?

a) $f : Z \to R : f(n) = n$

b) $f : Z \to 5Z : f(n) = 5n$

c) $f : C \to C : f(z) = \bar{z}$, the complex conjugate of z.

E 19) Let $\phi : R_1 \to R_2$ be a ring isomorphism. Then $\phi^{-1} : R_2 \to R_1$ is a well defined function since ϕ is bijective. Show that ϕ^{-1} is also an isomorphism.

$R_1 \cong R_2$ iff $R_2 \cong R_1$

E 20) Show that the composition of isomorphisms is an isomorphism.

And now, let us go back to Unit 6 for a moment. Over there we proved the Fundamental Theorem of Homomorphism for groups, according to which the homomorphic image of a group G is isomorphic to a quotient group of G. Now we will prove a similar result for rings, namely, the first isomorphism theorem or the Fundamental Theorem of Homomorphism for rings.

Theorem 9 (The Fundamental Theorem of Homomorphism) : Let $f : R \to S$ be a ring homomorphism. Then $R/\text{Ker } f \cong \text{Im } f$. In particular, if f is surjective, then $R/\text{Ker } f \cong S$.

Proof : Firstly, note that R/Ker f is a well defined quotient ring since Ker f is an ideal of R. For convenience, let us put Ker f = I. Let us define
$\psi : R/I \to S$ by $\psi(x + I) = f(x)$.

As in the case of Theorem 8 of Unit 6, we need to check that ψ is well defined, i.e., if $x + I = y + I$ then $\psi(x + I) = \psi(y + I)$.
Now, $x + I = y + I \Rightarrow x - y \in I = \text{Ker } f \Rightarrow f(x - y) = 0 \Rightarrow f(x) = f(y)$
$\Rightarrow \psi(x + I) = \psi(y + I)$.

Thus, ψ is well defined.

Now let us see whether ψ is an isomorphism or not.

i) ψ is a homomorphism : Let $x, y \in R$. Then
$$\psi((x + I) + (y + I)) = \psi(x + y + I) = f(x + y) = f(x) + f(y)$$
$$= \psi(x + I) + \psi(y + I), \text{ and}$$
$$\psi((x + I)(y + I)) = \psi(xy + I) = f(xy) = f(x) f(y)$$
$$= \psi(x + I)\psi(y + I)$$

Thus, ψ is a ring homomorphism.

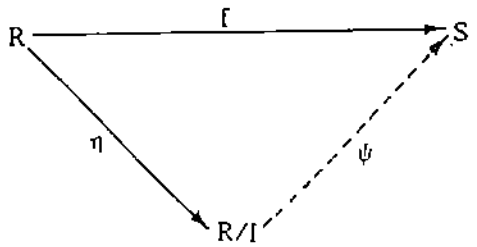
ii) Im ψ = Im f : Since $\psi(x + I) = f(x) \in \text{Im } f \; \forall \; x \in R$, Im $\psi \subseteq$ Im f. Also, any element of Im f is of the form $f(x) = \psi(x + I)$ for some $x \in R$. Thus, Im f $\subseteq$ Im ψ.
So, Im ψ = Im f.

iii) ψ is 1 − 1 : To show this let $x, y \in R$ such that
$\psi(x + I) = \psi(y + I)$. Then $f(x) = f(y)$,
so that $f(x - y) = 0$, i.e., $x - y \in \text{Ker } f = I$.
i.e., $x + I = y + I$.

Thus, ψ is 1 − 1.

So, we have shown that $R/\text{Ker } f \simeq \text{Im } f$.
Thus, if f is onto, then Im f = S and $R/\text{Ker } f \simeq S$.

Note that this result says that f is the composition $\psi \circ \eta$, where η is the canonical homomorphism $\eta : R \to R/I : \eta(a) = a + I$. This can be diagrammatically shown as



Let us look at some examples of the use of the Fundamental Theorem.

Consider $p : Z \to Z_m : p(n) = \bar{n}$. p is an epimorphism and Ker $p = \{ n \mid \bar{n} = \bar{0} \text{ in } Z_m \} = mZ$.
Therefore, $Z/mZ \simeq Z_m$.
(Note that we have often used the fact that Z/mZ and Z_m are the same.)

As another example, consider the projection map
$p : R_1 \times R_2 \to R_1 : p(a, b) = a$, where R_1 and R_2 are rings. Then p is onto and its kernel is $\{ (0, b) \mid b \in R_2 \}$, which is isomorphic to R_2.
Therefore, $(R_1 \times R_2)/R_2 \simeq R_1$.

Try this exercise now.

E 21) What does the Fundamental Theorem of Homomorphism say in each of the Examples 1 to 6?

Let us now apply Theorem 9 to prove that any ring homomorphism from a ring R onto Z is uniquely determined by its kernel. That is, we can't have two different ring homomorphisms from R onto Z with the same kernel. (Note that this is not true for group homomorphisms. In fact, you know that I_Z and $-I_Z$ are distinct homomorphisms from Z onto itself with the same kernel, {0}.) To prove this statement we need the following result.

Theorem 10 : The only non-trivial ring homomorphism from Z into itself is I_Z.

Proof : Let $f : Z \to Z$ be a non-trivial homomorphism. Let n be a positive integer. Then $n = 1 + 1 + \ldots + 1$ (n times). Therefore,
$f(n) = f(1) + f(1) + \ldots + f(1)$ (n times) $= n\, f(1)$.

On the other hand, if n is a negative integer, then $-n$ is a positive integer. Therefore, $f(-n) = (-n)\, f(1)$, i.e., $-f(n) = -nf(1)$, since f is a homomorphism. Thus, $f(n) = n\, f(1)$ in this case too.
Also $f(0) = 0 = 0f(1)$.
Thus, $f(n) = nf(1)\ \forall\ n \in Z$. ..... (1)

Now, since f is a non-trivial homomorphism, $f(m) \neq 0$ for some $m \in Z$.
Then, $f(m) = f(m \cdot 1) = f(m)\, f(1)$.
Cancelling f(m) on both sides we get $f(1) = 1$.
Therefore, from (1) we see that
$f(n) = n\ \forall\ n \in Z$, i.e., $f = I_Z$.
This theorem has an important corollary.

Corollary : Let R be a ring isomorphic to Z. If f and g are two isomorphisms from R onto Z, then $f = g$.

Proof : The composition $f \circ g^{-1}$ is an isomorphism from Z onto itself. Therefore, by Theorem 10, $f \circ g^{-1} = I_Z$, i.e., $f = g$.

We are now in a position to prove the following result.

Theorem 11 : Let R be a ring and f and g be homomorphisms from R onto Z such that Ker f = Ker g. Then $f = g$.

Proof : By Theorem 9 we have isomorphisms

$\psi_f : R/\text{Ker } f \to Z$ and $\psi_g : R/\text{Ker } g \to Z$.

Since Ker f = Ker g, ψ_f and ψ_g are isomorphisms of the same ring onto Z. Thus, by the corollary above, $\psi_f = \psi_g$.
Also, the canonical maps $\eta_f : R \to R/\text{Ker } f$ and $\eta_g : R \to R/\text{Ker } g$ are the same since Ker f = Ker g.
$\therefore\ f = \psi_f \circ \eta_f = \psi_g \circ \eta_g = g$.

We will now give you a chance to prove two applications of Theorem 9! They are analogous to Theorem 10 and 11 of Unit 6.

E 22) (Second isomorphism theorem) Let S be a subring and I be an ideal of a ring R. Show that $(S + I)/I \simeq S/(S \cap I)$.

E 23) (Third isomorphism theorem) Let I and J be ideals of a ring R such that $J \subseteq I$. Show that I/J is an ideal of the ring R/J and that $(R/J)/(I/J) \simeq R/I$.

Let us halt our discussion of homomorphisms here and briefly recall what we have done in this unit. Of course, we have not finished with these functions. We will be going back to them again and again in the future units.

11.5 SUMMARY

In this unit we have covered the following points.

1. The definition of a ring homomorphism, its kernel and its image, along with several examples.
2. The direct or inverse image of a subring under a homomorphism is a subring.

3. If $f : R \to S$ is a ring homomorphism, then
   i) Im f is a subring of S,
   ii) Ker f is an ideal of R,
   iii) $f^{-1}(I)$ is an ideal of R for every ideal I of S.
   iv) if f is surjective, then f(I) is an ideal of S.
4. A homomorphism is injective iff its kernel is {0}.
5. The composition of homomorphisms is a homomorphism.
6. The definition and examples of a ring isomorphism.
7. The proof and applications of the Fundamental Theorem of Homomorphism which says that if $f : R \to S$ is a ring homomorphism, then $R/\text{Ker } f \simeq \text{Im } f$.

11.6 SOLUTIONS/ANSWERS

E 1) For $x, y \in S$,
$i(x + y) = x + y = i(x) + i(y)$, and
$i(xy) = xy = i(x)\, i(y)$
$\therefore$ i is a homomorphism.
$\text{Ker } i = \{ x \in S \mid i(x) = 0 \} = \{0\}$
$\text{Im } i = \{i(x) \mid x \in S \} = S$

E 2) For any $x, y \in R_1$, $f(x + y) = 0 = 0 + 0 = f(x) + f(y)$, and
$f(xy) = 0 = 0.0 = f(x).f(y)$. $\therefore$ f is a homomorphism.
$\text{Ker } f = \{ x \in R_1 \mid f(x) = 0 \} = R_1$
$\text{Im } f = \{0\}$.

E 3) $f(2.3) = f(6) = 12$. But $f(2).f(3) = 4.6 = 24$
Thus, $f(2.3) \neq f(2)\, f(3)$.
$\therefore$ f is not a homomorphism.

E 4) For any $(a, b), (c, d) \in A \times B$,
$p((a, b) + (c, d)) = p(a + c, b + d) = a + c = p(a, b) + p(c, d)$,
$p((a, b)\,(c, d)) = p(ac, bd) = ac = p(a, b)\, p(c, d)$.
$\text{Ker } p = \{ (a, b) \in A \times B \mid a = 0 \} = \{0\} \times B$.
$\text{Im } p = \{ p(a, b) \mid (a, b) \in A \times B \} = \{ a \mid (a, b) \in A \times B \} = A$.

E 5) Yes, you can check it.

E 6) For $f, g \in C[0, 1]$,
$\phi(f + g) = ((f + g)(0), (f + g)(1))$
$= (f(0), f(1)) + (g(0), g(1))$
$= \phi(f) + \phi(g)$, and
$\phi(fg) = (fg(0), fg(1) = (f(0), g(0))\,(f(1), g(1))$
$= \phi(f)\, \phi(g)$.
$\therefore$ ϕ is a homomorphism.

E 7) Let $x \in R_2$. Since f is surjective, $\exists\ r \in R_1$ such that $f(r) = x$. Since
$r.1 = r$, $f(r)\, f(1) = f(r)$.
Thus, $xf(1) = x$. This is true for any $x \in R_2$.
$\therefore$ f(1) is the identity of R_2.

E 8) Again use Theorem 1 of Unit 10.

i) $S \neq \phi \implies f(S) \neq \phi$.

ii) Let $a', b' \in f(S)$. Then $\exists\ a, b \in S$ such that $f(a) = a'$, $f(b) = b'$
Now $a' - b' = f(a) - f(b) = f(a - b) \in f(S)$, since $a - b \in S$, and
$a'b' = f(a)\, f(b) = f(ab) \in f(S)$, since $ab \in S$.
$\therefore$ f(S) is a subring of R_2.

E 9) Since I is a subring of R_2, $f^{-1}(I)$ is a subring of R_1. Now, let $a \in f^{-1}(I)$ and $r \in R_1$.
We want to show that $ar \in f^{-1}(I)$.
Since $a \in f^{-1}(I)$, $f(a) \in I$. $\therefore$ $f(a)\, f(r) \in I$, i.e.,

$f(ar) \in I$. $\therefore ar \in f^{-1}(I)$.
Thus, $f^{-1}(I)$ is an ideal of R_1.
Also, if $x \in \text{Ker } f$, then $f(x) = 0 \in I$.
$\therefore x \in f^{-1}(I)$.
$\therefore \text{Ker } f \subseteq f^{-1}(I)$.

E 10) Let $x \in f(f^{-1}(J))$. Then $x = f(y)$, where $y \in f^{-1}(J)$, i.e., $f(y) \in J$, i.e., $x \in J$.
Thus, $f(f^{-1}(J)) \subseteq J$.
Now, let $x \in J$. Since f is surjective, $\exists\ y \in R$ such that $f(y) = x$.
Then $y \in f^{-1}(x) \subseteq f^{-1}(J)$.
$\therefore x = f(y) \in f(f^{-1}(J))$.
Thus, $J \subseteq f(f^{-1}(J))$.
Hence the result is proved.

E 11) $\text{Ker } f = \{ n \in \mathbf{Z} \mid n \equiv 0 \pmod{12} \} = 12\mathbf{Z}$.
Now, you know that any ideal of $\mathbf{Z}$ is a subgroup of $\mathbf{Z}$, and hence must be of the form $n\mathbf{Z}$, $n \in \mathbf{N}$. Thus, the ideals of $\mathbf{Z}$ containing Ker f are all those $n\mathbf{Z}$ such that $n \mid 12$, i.e., $\mathbf{Z}$, $2\mathbf{Z}$, $3\mathbf{Z}$, $4\mathbf{Z}$, $6\mathbf{Z}$, $12\mathbf{Z}$. Thus, by Theorem 4(b) the ideals of $\mathbf{Z}_{12}$ are
$\mathbf{Z}_{12}$, $\overline{2}\mathbf{Z}_{12}$, $\overline{3}\mathbf{Z}_{12}$, $\overline{4}\mathbf{Z}_{12}$, $\overline{6}\mathbf{Z}_{12}$ and $\{\overline{0}\}$.

E 12) For example, $(0, 1) \notin \text{Im } f$.
For any ideal I of $\mathbf{Z}$, $f(I) = I \times I$. Thus, the ideal $\mathbf{Z} \times \{0\}$ of $\mathbf{Z} \times \mathbf{Z}$ is not of the form $f(I)$, for any ideal I of $\mathbf{Z}$.

E 13) **The homomorphisms in Examples 1 and 5.**

E 14) No. For example, take the subring $\mathbf{Z}$ of $\mathbf{Q}$. Since $\mathbf{Z}$ is not an ideal of $\mathbf{Q}$, it can't be the kernel of any homomorphism from $\mathbf{Q}$ to another ring.

E 15) For any $x, y \in R_1$,

$$\begin{aligned} g \circ f(x + y) &= g(f(x + y)) = g(f(x) + f(y)) \\ &= g \circ f(x) + g \circ f(y), \text{ and} \\ g \circ f(xy) &= g(f(xy)) = g(f(x)\, f(y)) \\ &= g \circ f(x)\, g \circ f(y). \end{aligned}$$

Thus, $g \circ f$ is a homomorphism.

E 16) a) $x \in \text{Ker } f \implies f(x) = 0 \implies g \circ f(x) = 0 \implies x = 0$, since $g \circ f$ is $1 - 1$.
$\therefore \text{Ker } f = \{0\}$.
$\therefore f$ is $1 - 1$.

b) Let $x \in R_3$. Since $g \circ f$ is onto $\exists\ y \in R_1$ such that $g \circ f(y) = x$, i.e., $g(f(y)) = x$. Thus, g is onto.

E 17) h is the composite of the projection map $p : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} : p(n, m) = m$ and the map $f : \mathbf{Z} \to \mathbf{Z}_2 : f(r) = \overline{r}$. Both p and f are ring homomorphisms.
$\therefore h$ is a ring homomorphism.

E 18) a) f is not onto, and hence, not an isomorphism.

b) f is not a homomorphism.

c) See the appendix of Unit 2 for properties of elements of $\mathbf{C}$.
Then you can easily prove that f is an isomorphism.

E 19) Let $x, y \in R_2$ and $\phi^{-1}(x) = r$, $\phi^{-1}(y) = s$. Then $x = \phi(r)$ and $y = \phi(s)$. Therefore, $x + y = \phi(r) + \phi(s) = \phi(r + s)$ and $xy = \phi(rs)$.
$\therefore \phi^{-1}(x + y) = r + s = \phi^{-1}(x) + \phi^{-1}(y)$, and
$\phi^{-1}(xy) = rs = \phi^{-1}(x)\, \phi^{-1}(y)$.
Thus, ϕ^{-1} is a homomorphism.
You already know that it is bijective. Thus, ϕ^{-1} is an isomorphism.

E 20) Let $f : R_1 \to R_2$ and $g : R_2 \to R_3$ be ring isomorphisms. From Theorem 8 you know that $g \circ f$ is a homomorphism. For the rest, proceed as you did in E 12 of Unit 6.

E 21) Example 1 : $R \simeq R$.
Example 2 : What we have just done above, namely, $\mathbf{Z}/s\mathbf{Z} \simeq \mathbf{Z}$.
Example 3 : $\mathbf{Z}_6/\{\overline{0}, \overline{3}\} \simeq \mathbf{Z}_3$.

Example 4 : $\text{Ker}\,\phi = \{ f \in C[0, 1] \mid f\left(\frac{1}{2}\right) = 0 \}$.

$\text{Im}\,\phi = \mathbf{R}$ (because given any $r \in \mathbf{R}$ we can define the constant function $f_r : [0, 1] \to R : f_r(x) = r$. Then $f_r\left(\frac{1}{2}\right) = r$. Thus, $r = \phi(f_r) \in \text{Im}\,\phi$.)

Example 5 : $\mathbf{Z} \simeq \{ nI \mid n \in \mathbf{Z} \}$

Example 6 : $\wp(X)/\text{Ker}\, f \simeq \wp(Y)$.

E 22) Since I is an ideal of R and $I \subseteq S + I$, it is an ideal of $S + I$.
Thus, $(S + I)/I$ is a well defined ring.
Define $f : S \to (S + I)/I : f(x) = x + I$.
Then, you can check that $f(x + y) = f(x) + f(y)$, and
$f(xy) = f(x) f(y)\ \forall\ x, y \in S$.

As you did in Theorem 10 of Unit 6, you can check that f is surjective and $\text{Ker}\, f = S \cap I$. Thus, $S/(S \cap I) \simeq (S + I)/I$.

E 23) Define $f : R/J \to R/I : f(r + J) = r + I$.

As you did in Theorem 11 of Unit 6, you can check that f is well defined, f is surjective and $\text{Ker}\, f = I/J$.

Thus, I/J is an ideal of R/J and $(R/J)/(I/J) \simeq R/I$.

UTTAR PRADESH
RAJARSHI TANDON OPEN UNIVERSITY

UGMM – 06
Abstract Algebra

Block

4

INTEGRAL DOMAINS AND FIELDS

INTEGRAL DOMAINS AND FIELDS

In this block we will continue our discussion on ring theory. We will start by introducing you to two special types of rings, namely, integral domains and fields. Then we will discuss their properties in some detail.

In the second unit of this block we shall discuss rings whose elements may be familiar to you, namely, polynomials in one variable. We will discuss various properties of polynomials over any integral domain or field. Apart from its mathematical interest, the theory of polynomials over a field has several applications. In fact, because of this, linear and quadratic polynomials over Q were dealt with in considerable depth by the ancient Indian mathematicians Aryabhata I, Sridhar, Bhaskara II and others. Nowadays, this theory is used in coding theory and in mathematical modelling of problems from the social sciences and the physical sciences.

In the third unit of this course we introduce you to three kinds of integral domains, the best known examples of which are Z and polynomial rings over a field. The domains are Euclidean domains, principal ideal domains and unique factorisation domains. We will discuss some of their properties in detail and show you how these domains are related.

Finally, in the last unit of this course we shall look at those polynomials over Q which do not have any proper factors. Using such polynomials we can get field extensions of Q. In this unit we will also discuss these and other field extensions, as well as subfields. Then we will look at finite fields and their properties. These fields play an important role in coding theory.

With this block we come to the end of the course. After you finish studying it, please do the second assignment of the course, which deals with Block 3 and this block.

Notation and Symbols

$C[0,1]$	ring of continuous functions from $[0,1]$ to $\mathbf{R}$
$\wp(X)$	set of all subsets of X
Z_n	ring of integers modulo n
char R	characteristic of a ring R
Ra, <a>	principal ideal of R generated by a
R[x]	ring of polynomials in one variable over R
deg f(x)	degree of the polynomial f(x)
max $(a_1, ..., a_n)$	the maximum among the integers $a_1, ..., a_n$
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
g.c.d	greatest common divisor
(a,b)	the g.c.d of a and b
l.c.m	lowest common multiple

Also look at the notations given in the previous blocks.

UNIT 12 THE BASICS

Structure

12.1 INTRODUCTION

In Unit 9 we introduced you to rings, and then to special rings whose speciality lay in the properties of their multiplication. In this unit we will introduce you to yet another type of ring, namely, an integral domain. You will see that an integral domain is a ring with identity in which the product of two non-zero elements is again a non-zero element. We will discuss various properties of such rings.

Next, we will look at rings like $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $\mathbf{Z}_p$ (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 $\mathbf{Q}$ is constructed from $\mathbf{Z}$. 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.

Objectives

After reading 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.

12.2 INTEGRAL DOMAINS

You know that the product of two non-zero integers is a non-zero integer, i.e., if $m, n \in \mathbf{Z}$ such that $m \neq 0$, $n \neq 0$, then $mn \neq 0$. Now consider the ring $\mathbf{Z}_6$. We find that $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$, yet $\bar{2}.\bar{3} = \bar{0}$. So, we find that the product of the non-zero elements $\bar{2}$ and $\bar{3}$ in $\mathbf{Z}_6$ is zero. As you will soon realise, 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 is.

Definition: A non-zero element a 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 $n \in N$ and $m \mid n$, $1 < m < n$. Then show that $\bar{m}$ is a zero divisor in Z_n.

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

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

Let us define $g : [0,1] \to \mathbf{R}$ by

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

Then $g \in C[0,1]$, $g \neq 0$ and $(fg)(x) = 0 \ \forall \ x \in [0,1]$. 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 $a \neq 0$ in A, (a,0) is a zero divisor in $A \times B$. This is because, for any $b \neq 0$ in B, $(a,0)(0,b) = (0,0)$.

Now let us look at 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 in Z.

E 3) For which rings with unity will 1 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 ideal 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 is a non-zero element.

Several authors often shorten the term 'integral domains' to 'domains'. We will do so too.

This kind of ring gets its name from the set of integers, one of its best known examples. Other examples of domains that immediately come to mind are Q, R and C. What about C[0,1]? 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 : Z_p 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, supppose $\bar{a}, \bar{b} \in Z_p$ satisfy $\bar{a}\,\bar{b} = \bar{0}$. Then $\overline{ab} = \bar{0}$, i.e., $p \mid ab$. Since p is a prime number, using E 25 of Unit 1 we see that $p \mid a$ or $p \mid b$. Thus, $\bar{a} = \bar{0}$ 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 without zero divisors, and hence, is 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 $m \mid p$, then by E 1 you know that $\bar{m} \in Z_p$ is a zero divisor. Thus, Z_p 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, $2Z$, $Z + iZ$, $R \times R$, $\{0\}$.

Now consider a ring R. We know that the cancellation law for addition holds in R, i.e., whenever a+b = a+c in R, then b = c. But, does ab = ac imply b = c? It need not. For example, 0.1 = 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 $a \neq 0$ and ab = ac. Then a(b–c) = ab – ac = 0. As $a \neq 0$, and R has no zero divisors, we get b – c = 0, i.e., b = c.

Thus, if ab = ac and $a \neq 0$, then b = c.

Conversely, assume that the cancellation law for multiplication holds in R. Let $a \in R$ 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 law holds for multiplication in an integral domain.

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

---

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

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 know that $4x = \bar{0}\ \forall\ x \in Z_4$. In fact, $8x = \bar{0}$ and $12x = \bar{0}$ 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 characteristic of 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 $(R \times R)$?

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 $a \neq 0$ in R.

Proof: We will prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b) : We know that $m\,1 = 0$.

Thus, for any $a \in R$, $ma = m(1a) = (m1)(a) = 0a = 0$, i.e., (b) holds.

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

(c) $\Rightarrow$ (a) : Let $ma = 0$ for some $a \neq 0$ in R. Then $0 = ma = m(1a) = (m1)a$. 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 only need to look at the set $\{n.1 \mid n \in N\}$.**

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 peculiarity 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 is 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 $m.1 = 0 \Rightarrow (st).1 = 0 \Rightarrow (s.1)(t.1) = 0$. As R is without zero divisors, we get $s.1 = 0$ 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 exercises.

E 10) Let R be an integral domain of characteristic p. Prove 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 a subring of R.

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

d) if R is a finite integral domain, then ϕ 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.

12.3 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 $(R\setminus\{0\},.)$ 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 $(R\setminus\{0\},.)$ 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

iiii) 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 **skew 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 19th century through the research of the German mathematicians Richard Dedekind and Leopold Kronecker in algebraic number theory. Dedekind used the German word Körper, which means field, for this concept. This is why you will often find that a field is denoted by K.

As you may have realised, 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 $Q + \sqrt{2}Q = \{a + \sqrt{2}b \mid a, b \in Q\}$ is a field.

Solution : From Unit 9 you know that $F = Q + \sqrt{2}Q$ is a commutative ring with identity $1 + \sqrt{2}.0$.

Now, let $a + \sqrt{2}b$ be a non-zero element of F. Then either $a \neq 0$ or $b \neq 0$. Now, using the rationalisation process, we see that

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

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

(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 happ to be integral domains also? This is not a coincidence. In fact, we have the following re

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 $a \neq 0$. As $a \neq 0$ 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?

$2Z,\ Z_5,\ Z_6, Q \times Q$

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 $R = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_n\}$ 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 $j \neq 0$, $a_j \neq 0$; and since $a \neq 0$, we get $aa_j \neq 0$.

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

Also, $aa_1, aa_2, \ldots, aa_n$ are all distinct elements of the set $\{a_1, \ldots, a_n\}$, since $aa_j = aa_K \Rightarrow a_j = a_K$, using the cancellation law for multiplication.

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

In particular, $a_1 = aa_j$, i.e., $1 = aa_j$ 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.

A field whose underlying set is finite is called a finite 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 is 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	0	1	a	1+a
1	1	0	1+a	a
a	a	1+a	0	1
1+a	1+a	a	1	0

and

.	0	1	a	1+a
0	0	0	0	0
1	0	1	a	1+a
a	0	a	1+a	1
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 R and {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 R and {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 homomorphisms** (i.e., ring homomorphisms from one field to another). We give them to you in the form of an exercise.

E 16) Let $f : F \to K$ 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.

12.4 PRIME AND MAXIMAL IDEALS

In Z we know that if p is a prime number and p divides the product of two integers a and b, then either p divides a or p divides b. In other words, if $ab \in pZ$, then either $a \in pZ$ 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

Example 2: Let R be an integral domain. Show that $I = \{(0,x) \mid x \in R\}$ is a prime ideal of $R \times R$.

Solution : Firstly, you know that I is an ideal of $R \times R$. Next, it is a proper ideal since $I \neq R \times R$. Now, let us check if I is a prime ideal or not. For this let $(a_1,b_1), (a_2,b_2) \in R \times R$ such that $(a_1,b_1)(a_2,b_2) \in I$. Then $(a_1a_2,b_1b_2) = (0,x)$ for some $x \in R$. So $a_1a_2 = 0$, i.e., $a_1 = 0$ or $a_2 = 0$, since R is a domain. Therefore, $(a_1,b_1) \in I$ or $(a_2,b_2) \in I$. 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 $I = \{f \in C[0,1] \mid f(0) = 0\}$ is a prime ideal of C[0,1].

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 iff m is a prime number. Can we generalise this relationship between prime numbers and prime ideals in Z to any integral domain? To answer this let us first try and suitably generalise 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, or 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 $\in$ 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

x $\in$ R has a multiplicative inverse iff Rx = R.

$\Rightarrow$ 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. Thus, 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 finding 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 $f : R \to S$ be a ring epimorphism with kernel N. Show that

a) if J is a prime ideal in S, then $f^{-1}(J)$ is a prime ideal in R.

b) if I is a prime ideal in R containing N, then f(I) is a prime ideal in S.

c) the map ø between the set of prime ideals of R that contain N and the set of all prime ideals of S given by $ø(I) = f(I)$ is a bijection.

E 21) If I_1 and I_2 are ideals of a ring such that neither I_1 nor I_2 contains the other, then show that the ideal $I_1 \cap I_2$ 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 I = 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 characterisation of such ideals.

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 enough to prove that R/M has no non-zero proper ideals (see Theorem 9). So, let I be an ideal of R/M. Consider the canonical homomorphism $\eta : R \to R/M : \eta(r) = r + M$. Then, from Theorem 3 of Unit 11, you know that $\eta^{-1}(I)$ is an ideal of R containing M, the kernel of η. 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 $\bar{0} = 0 + M = M$. Thus, R/M 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.

E 22) 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 $Z \cong Z/\{0\}$, $Z/\{0\}$ 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 ideal 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 $Z/mZ \simeq Z_m$. 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}, whereas $\{\bar{0},\bar{4},\bar{8}\}$ is not.

Solution : You know that $Z_{12} \simeq Z/12Z$ and $\bar{2}Z_{12} \simeq 2Z/12Z$. Thus, by E 23 of Unit 11, we see that $Z_{12}/\bar{2}Z_{12} \simeq (Z/12Z)/(2Z/12Z) = Z/2Z \simeq Z_2$, 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, $\{\bar{0},\bar{4},\bar{8}\} = \bar{4}Z_{12} \subsetneq \bar{2}Z_{12} \subsetneq Z_{12}$.

Therefore, $\{\bar{0},\bar{4},\bar{8}\}$ is not maximal in 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.

12.5 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 $(a,b) \in Z \times Z^*$. Now, in Q we know that $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. Let us put a similar relation on the elements of $Z \times Z^*$.

Now, we also know that the operations on Q are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \; \forall \; \frac{a}{b}, \frac{c}{d} \in Q.$$

Keeping these in mind we can define operations on $Z \times Z^*$. Then we can suitably define an equivalence relation on $Z \times Z^*$ 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) ∈ K such that (a,b) ~ (c,d) and (c,d) ~ (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) ~ (u,v). Thus, ~ is transitive.

Hence, ~ is an equivalence relation.

Let us denote the equivalence class that contains (a,b) by [a,b]. Thus,
[a,b] = {(c,d) | c,d ∈ R, d ≠ 0 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. (It might help you 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 ≠ 0 and d ≠ 0 in the integral domain R imply bd ≠ 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) (b′d′) – (bd) (a′c′)

= 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] ∈ 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 commutative : For [a,b], [c,d] ∈ F,

[a,b] + [c,d] = [ad+bc,bd] = [cb+da,db] = [c,d] + [a,b]

iii) [0,1] is the additive identity for F : For [a,b] ∈ F,

[0,1] + [a,b] = [0.b+1.a, 1.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 $f : R \to F : f(a) = [a,1]$. We want to show that f is a monomorphism.

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

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

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

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

Thus, f is a ring homomorphism.

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

Thus, f is a monomorphism.

So, Im 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.

A ring R is embedded in a ring S if there is a ring monomorphism from R to S.

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 $f : R \to K$ is a monomorphism of an integral domain R into a field K, then there exists a monomorphism

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

We will not prove this result here, since it is a little technical. But let us 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 Z_p is 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.

12.6 SUMMARY

In this unit we have covered the following points.

1. The definition and examples of an integral domain.
2. The definition and examples of a field.
3. Every field is a domain.
4. A finite domain is a field.
5. The characteristic of any domain or field is either zero or a prime number.
6. The definition and examples of prime and maximal ideals.
7. 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).
8. Every maximal ideal is a prime ideal.
9. An element p of an integral domain R is prime iff the principal ideal pR is a prime ideal of R.
10. Z_n is a field iff n is a prime number.
11. The construction of the field of quotients of an integral domain.

12.7 SOLUTIONS/ANSWERS

E 1) Let $n = mr$, where $r \in N$.

Then $\bar{m}\,\bar{r} = \bar{n} = \bar{0}$ in Z_n.

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

Thus $\bar{m} \in Z_n$ 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 that $ab = 0$. Then, for any $r \in R$, $(ra)b = r(ab) = 0$. Thus, every element of Ra is a zero divisor.

E 5) Z_4, since $\bar{2}$ is a zero divisor.

2Z, since $1 \notin 2Z$.

$R \times R$, since $(1,0)$ is a zero divisor.

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

E 6) $x^2 = x \Rightarrow x(x-1) = 0 \Rightarrow x = 0$ or $x-1 = 0$

$\Rightarrow x = 0$ 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 $A \subseteq X$,

$2A = A \Delta A = (A \setminus A) \cup (A \setminus A) = \phi$

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

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

E 9) Let char $(R \times R) = n$. We know that $nr = 0$ $\forall$ $r \in R$.

Now, let (r,s) be any element of $R \times R$.

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

Thus, $n \leq m$. .....(1)

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

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

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

i.e., $nr = 0$.

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

$\therefore m \leq n$. .....(2)

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

E 10) a) By the binomial expansion (E 11 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 $p \mid {}^pC_n \; \forall\, n = 1, \ldots, p-1$, ${}^pC_n x = 0 \; \forall\, x \in R$ and $\forall\, n = 1, \ldots, p-1$.

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

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

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

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

Firstly, $S \neq \emptyset$.

Secondly, let $\alpha,\beta \in S$. 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) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$,

$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\,\phi(b)$.

Thus, ϕ is a ring homomorphism.

ϕ 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 ϕ is surjective.

Let R have n elements. Since ϕ is 1–1, Im ϕ also has n elements.

Also Im $\phi \subseteq R$. Thus, Im $\phi = R$.

Hence, ϕ is surjective.

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

Ker $f = \{n \in Z \mid n.1 = 0\}$

$= m\mathbb{Z}$, since char R = m.

E 12) char $(Z_3 \times Z_4)$ = l.c.m. of char Z_3 and char Z_4 = 12

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

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

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

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

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

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

$\mathbf{Z}_6$, since it is not a domain.

$\mathbf{Q} \times \mathbf{Q}$, since it is not a domain.

E 14) No. For example, $\mathbf{Z}$ is a subring of $\mathbf{Q}$, $\mathbf{Q}$ is a field, but $\mathbf{Z}$ 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 $2x = 0\ \forall\ x \in R^*$ and $1.x \neq 0$ for some $x \in R$.

Thus, char R = 2.

E 16) Ker f 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 $\phi : F \to R$ be an isomorphism. Then $\phi(1)$ is the identity of Im ϕ = R. Also, since F is commutative, so is R. Now, let $r \in R$, $r \neq 0$. Since ϕ is onto, $\exists\ a \in F$ such that $\phi(a) = r$. Since $r \neq 0$, $a \neq 0$. Since F is a field, $\exists\ b \in F$ such that $ab = 1$.

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

Thus, R is a field.

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

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

$T \in C[0,1], f \in I \Rightarrow Tf \in I$.)

Secondly, since any non–zero constant function is in

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

Finally, let $fg \in I$. 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 ideal of C[0,1].

E 19) R is a ring with identity. Thus, we need to show that R is without zero divisors iff {0} is a prime 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 surjective and $J \neq S$, $f^{-1}(J) \neq R$.

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 $1 \notin I$ 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 $S = \text{Im } f$, $\exists\ a,b \in R$ 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) ϕ is $1-1$: $\phi(I) = \phi(J) \Rightarrow f(I) = f(J)$

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

ϕ 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, $J \in \text{Im } \phi$.

E 21) Let $x \in I_1 \setminus I_2$ and $y \in I_2 \setminus I_1$. 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) $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\} = \bar{2}\mathbf{Z}_{10}$ and $\mathbf{Z}_{10}/\bar{2}\mathbf{Z}_{10} \simeq \mathbf{Z}_2$, a field.

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

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

$\therefore C[0,1]/\text{Ker } \phi \simeq R$, a field.

Thus, Ker ϕ 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 $c+d\sqrt{2} \neq 0$, $a,b,c,d \in \mathbf{Z}$.

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

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

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

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

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

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

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

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

UNIT 13 POLYNOMIAL RINGS

Structure

13.1 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 turn out to be a domain also, with a lot of useful properties. In particular, 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.

Objectives

After reading 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.

13.2 RING OF POLYNOMIALS

As we have said above, you may already be familiar with expressions of the type $1 + x$, $2 + 3x + 4x^2$, $x^5 - 1$, 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

$$a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n,$$

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

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

i) write x^0 as 1, so that we will write a_0 for $a_0 x^0$,

ii) write x^1 as x,

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

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

Thus, the polynomial $2 + 3x^2 - 1.x^3$ 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.)

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

We will also often denote a polynomial $a_0 + a_1 x + \ldots + a_n x^n$ 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.

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 $f(x) = a_0 + a_1x + .. + a_n x^n$ 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

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + .. + (a_n + b_n) x^n + b_{n+1}x^{n+1} + .. + b_m x^m.$$

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

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

$$\deg (f(x) + g(x)) \leq \max (\deg f(x), \deg g(x))$$

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

Now let us define the product of polynomials.

Definition : If $f(x) = a_0 + a_1x + .. + a_n x^n$ and $g(x) = b_0 + b_1 x + .. + b_m x^m$ 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 $c_i = a_ib_0 + a_{i-1} b_1 + \ldots + a_0 b_i \;\forall\; i = 0, 1, \ldots, m + n$.

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 Z[x] :

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

Here $a_0 = 1$, $a_1 = -1$, $a_2 = 0$, $a_3 = 2$, $b_0 = 2$, $b_1 = 5$, $b_2 = 7$.

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 $p(x).\ q(x) \in Z[x]$, and deg $(p(x)\ q(x)) = 5 = \deg p(x) + \deg q(x)$.

As another example, consider

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

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

$$\deg\ (f(x)\ g(x)) \leq \deg\ f(x) + \deg\ g(x)$$

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

E 3) Calculate

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

b) $(\bar{6} + \bar{2}x^2) + (\bar{1} - \bar{2}x + \bar{5}x^3)$ in $Z_7[x]$.

c) $(1 + x)(1 + 2x + x^2)$ in $Z[x]$.

d) $(\bar{1} + x)(\bar{1} + \bar{2}x + x^2)$ in $Z_3[x]$

e) $(2 + x + x^2)(5x + x^3)$ in $Z[x]$

By now you must have got used to addition and multiplication of polynomials. We would like to prove that for 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 R1 – 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 $p(x) = a_0 + a_1x + \ldots + a_nx^n$, and

$q(x) = b_0 + b_1x + \ldots + b_mx^m$ be in R[x].

Then, $p(x) + q(x) = c_0 + c_1x + \ldots + c_tx^t$,

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

Similarly,

$q(x) + p(x) = d_0 + d_1x + \ldots + d_sx^s$,

where $d_i = b_i + a_i$, $s = \max(n,m) = t$.

Since addition is commutative in R, $c_i = d_i\ \forall\ i \geq 0$.

So we have

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

Two polynomials $f(x) = a_0 + a_1x + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + \ldots + b_mx^m$ are equal if $a_i = b_i\ \forall\ i \geq 0$.

ii) Addition is associative : Again by using the associativity 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 $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$,

$$\begin{aligned} 0 + p(x) &= (0 + a_0) + (0 + a_1) x + \ldots + (0 + a_n) x^n \\ &= a_0 + a_1 x + \ldots + a_n x^n \\ &= p(x) \end{aligned}$$

iv) Additive inverse : For $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$, consider the polynomial $-p(x) = -a_0 - a_1 x - \ldots - a_n x^n$, $-a_i$ being the additive inverse of a_i in R. Then

$$\begin{aligned} p(x) + (-p(x)) &= (a_0 - a_0) + (a_1 - a_1) x + \ldots + (a_n - a_n) x^n \\ &= 0 + 0.x + 0.x^2 + \ldots + 0.x^n \\ &= 0. \end{aligned}$$

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

v) Multiplication is associative :

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

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

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

Then

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

$c_k = a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k \; \forall \; k = 0,1,\ldots.s.$

Therefore,

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

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

$$\begin{aligned} e_k &= c_k d_0 + c_{k-1} d_1 + \ldots + c_0 d_k \\ &= (a_k b_0 + \ldots + a_0 b_k) d_0 + (a_{k-1} b_0 + \ldots + a_0 b_{k-1}) d_1 + \ldots + a_0 b_0 d_k. \end{aligned}$$

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

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

$= e_k$, 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 $p(x) = a_0 + a_1 x + \ldots + a_n x^n$,

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

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

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

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

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 $\forall \; k > 0$.

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.

13.3 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, so is R [x].

b) If R has identity, so does R [x].

Proof : a) Let $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ and

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

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

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

$= b_k a_0 + b_{k-1} a_1 + \ldots + b_1 a_{k-1} + b_0 a_k$, since both addition and multiplication are commutative in R.

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

Thus, for every $i \geq 0$ the coefficients of x^i 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 1. We will prove that the constant polynomial 1 is the identity of R [x]. Take any

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

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

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

Thus, $1.p(x) = p(x)$.

Similarly, $p(x).1 = p(x)$.

This shows that 1 is the identity of R [x].

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 if R [x] is a domain. This result follows just from the definition of multiplication of polynomials.

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 $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \neq 0$,

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

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

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

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

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 $a_n b_m = 0$. 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 $q(x) = b_0 + b_1 x + \ldots + b_m x^m$

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

Then, in Theorem 3 we have 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 b 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 $f: R \to S$ be a ring homomorphism. Show that the map

$\phi : R[x] \to S[x] : \phi(a_0 + a_1 x + \ldots + a_n x^n) = f(a_0) + f(a_1) x + \ldots + f(a_n) x^n$ is a homomorphism.

Now, you have seen that many properties of the ring R carry over to R [x]. 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) ∈ F [x] and deg f (x) = n > 0. Suppose g (x) ∈ 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) ≥ 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.

13.4 THE DIVISION ALGORITHM

In Sec. 1.6.2 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. Let f(x) and g(x) be two polynomials in F [x], with g(x) ≠ 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) ≥ 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) ≠ 0. Now

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

f(x) = $(a_0 b_0^{-1}) b_0 + 0$ = 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 ≤ n − 1 and try to establish that it is true for f(x). Consider the polynomial

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

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

Thus, the coefficient of x^n in $f_1 (x)$ is zero; and hence,

deg $f_1(x) \leq n-1$.

By the induction hypothesis, there exist $q_1 (x)$ and r (x) in

F[x] such that $f_1 (x) = q_1 (x) g(x) + r(x)$, where deg r(x) < deg g(x).

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

$f(x)-a_n b_m^{-1} x^{n-m} g(x) = q_1(x) g(x)+r(x)$,

i.e., $f(x) = \{a_n b_m^{-1} x^{n-m}+q_1(x)\} g(x)+r(x)$

$= q(x) g(x)+r(x)$, where $q(x) = a_n b_m^{-1} x^{n-m}+q_1(x)$

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 $r_1(x) <$ deg $g(x)$.

and

$f(x) = q_2(x) g(x)+r_2(x)$, where deg $r_2(x) <$ deg $g(x)$.

Then

$q_1(x) g(x)+r_1(x) = q_2(x) g(x)+r_2(x)$, so that

$\{q_1(x) - q_2(x)\} g(x) = r_2(x) - r_1(x)$ .....(1)

Now if $q_1(x) \neq q_2(x)$, then deg $\{q_1(x) - q_2(x)\} \geq 0$, so that

deg $[\{q_1(x) - q_2(x)\} g(x)] \geq$ 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 (1) 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 $r_1(x) = r_2(x)$.

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

$f(x) = a_0 +a_1 x+\ldots+a_n x^n$.

Then, for any $r \in R$, we define

$f(r) = a_0+a_1 r+\ldots+a_n r^n \in R$,

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 there exists a 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 $g(x) = 1$.

Since 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

$f(b) = (b-b)\,q(b) + a$

$= 0.q(b)+a = a$

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, $\deg q(x) = \deg f(x)-1$.

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

Example 1 : Express $x^4+x^3+5x^2 - x$ as

$(x^2+x+1)\,q(x)+r(x)$ in $Q[x]$.

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

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

Now, since the degree of the remainder $-5x-4$ is less than $\deg (x^2+x+1)$, we stop the process. We get

$x^4+x^3+5x^2 - x = (x^2+x+1)\,(x^2+4) - (5x+4)$.

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

Now you can try some exercises.

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

a) $f = x^4+1$, $g = x^3$ in $Q[x]$

b) $f = x^3 + \bar{2}x^2 - x+\bar{1}$, $g = x+\bar{1}$ in $Z_3[x]$.

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 for elements of $F[x]$?

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

13.5 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 $q(x) \in F[x]$ such that

$f(x) = q(x)\,g(x)$.

We write $g(x) \mid f(x)$ for '$g(x)$ divides $f(x)$', and $g(x) \nmid f(x)$ 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 5 say when $g(x) \mid f(x)$? It does. We find that $g(x) \mid f(x)$ if $r(x) = 0$ in Theorem 5.

In the following 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 $x^2-1 \in \mathbf{R}[x]$, since $1^2-1 = 0$.

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

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

Note 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 $(x-a) \mid f(x)$.

We can generalise 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

$f(x)$ if $(x-a)^m \mid f(x)$, but $(x-a)^{m+1} \nmid f(x)$.

For example, 3 is a root of multiplicity 2 of the polynomial $(x-3)^2(x+2) \in \mathbf{Q}[x]$; 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, $-a^{-1}b$. This is because $ax+b = 0$ iff $x = -a^{-1}b$.

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 $f(x) = x^5-2x+1 \in R[x]$. Then, we try out $x = 1$ and find $f(1) = 0$. So, we find that 1 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) $f(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 3 \in \mathbf{Q}[x]$

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) ϕ 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) has at most n roots in F.

Proof : If n = 0, then f(x) is a non-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 f(x) = 1, then

$f(x) = a_0 + a_1x$, where $a_0, a_1 \in F$ and $a_1 \neq 0$.

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 roots 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–1.

Hence, by the induction hypothesis g(x) has at most n–1 roots in F, say $a_1, \ldots, a_{n-1}$. Now,

a_i is a root of $g(x) \Rightarrow g(a_i) = 0 \Rightarrow f(a_i) = (a_i - a)\, g(a_i) = 0$

$\Rightarrow a_i$ is a root of f(x) $\forall\ i = 1, \ldots, n-1$.

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

Now, $b \in F$ is a root of f(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, $x^3 - 1 \in Q[x]$ 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 $a_1, \ldots, a_{n+1}$ in F such that $f(a_i) = g(a_i)\ \forall\ i = 1, \ldots, n+1$, 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 $a_1, \ldots, a_{n+1}$.

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

$$f(\bar{0}) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{5}).$$

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 $x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \ldots (x - \overline{p-1})$.

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

Find this factorisation.

So far, we have been saying that a polynomial of degree n over F has at most n roots in F. It 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.

Now let us end this unit by seeing what we have covered in it

13.6 SUMMARY

In this unit we have covered the following points.

1) The definition and examples of polynomials over a ring.
2) The ring structure of R[x], where R is a ring.
3) R is a commutative ring with identity iff R[x] is a commutative ring with identity.
4) R is an integral domain iff R[x] is an integral domain.
5) 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 $g(x)$.
6) $a \in F$ is a root of $f(x) \in F[x]$ iff $(x-a) \mid f(x)$.
7) A non-zero polynomial of degree n over a field F can have at most n roots.

13.7 SOLUTIONS/ANSWERS

E 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 (f) are in Z[x].

E 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. 0 has no leading coefficient.

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

b) $(\bar{6}+\bar{1}) - \bar{2}x+\bar{2}x^2+\bar{5}x^3 = -\bar{2}x+\bar{2}x^2+\bar{5}x^3$, since $\bar{7} = \bar{0}$.

c) $1+3x+3x^2+x^3$

d) $\bar{1}+x^3$, since $\bar{3} = \bar{0}$.

e) $10x+5x^2+7x^3+x^4+x^5$

E 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.

E 5) (a) and (b)

E 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 such that n.1 = 0. Since 1 is also the identity of R[x], the same theorem of Unit 12 tells us that char R[x] = n = char R.

E 7) Let $p(x) = a_0+a_1x+\ldots+a_nx^n$, $q(x) = b_0+b_1x+\ldots+b_mx^m \in R[x]$.

Then $\phi\ (p(x)+q(x)) = \phi\ (\sum_{i=0}^{t} (a_i+b_i)x^i)$, where $t = \max(m,n)$

$$= \sum_{i=0}^{t} f(a_i+b_i)x^i$$

$$= \sum_{i=0}^{t} [f(a_i)+f(b_i)]x^i$$

$$= \sum_{i=0}^{t} f(a_i)x^i + \sum_{i=0}^{t} f(b_i)x^i$$

$$= \phi\ (p(x)) + \phi\ (q(x)), \text{ since } f(a_i) = 0 = f(b_j)$$

whenever $a_i = 0$, $b_j = 0$.

Also, $\phi\ (p(x)q(x)) = \phi\ (\sum_{i=0}^{m+n} c_ix^i)$, where $c_i = a_ib_0+a_{i-1}b_1+\ldots+a_0b_i$

$$= \sum_{i=0}^{m+n} f(c_i)\ x^i$$

$$= \sum_{i=0}^{m+n} [f(a_i)\ f(b_0) + f(a_{i-1})\ f(b_1) + \ldots + f(a_0)\ f(b_i)]\ x^i,$$

since f is a ring homomorphism.

$$= \phi\ (p(x))\ \phi\ (q(x)).$$

Thus, ϕ is a ring homomorphism.

E 8) a) $f = x.g+1$, $q = x$, $r = 1$.

b)
$$x+\bar{1}\ \overline{)\ x^3+\bar{2}x^2-x+\bar{1}}\ \ x^2+x-\bar{2}$$
$$x^3+x^2$$
$$x^2-x+\bar{1}$$
$$x^2+x$$
$$-\bar{2}x+\bar{1}$$
$$-\bar{2}x-\bar{2}$$
$$\bar{3}$$

Thus, $f = (x^2 + x-\bar{2})\, g + \bar{0}$, since $\bar{3} = \bar{0}$.

c) $f = (x^2 + x + 1)g + 0$

E 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

$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$, where $\deg r(x) < \deg g(x)$.

E 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.,
$(x-a) \mid f(x)$ iff $f(a) = 0$.

E 11) a) 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 Z_3.

Thus, $\bar{1}$ is the only zero, and its multiplicity is 2.

c) By trial, one zero is $\bar{1}$. 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 $x^3+\bar{3}x^2+\bar{3}x+\bar{1}$. Applying long division, we see that

$x^3+\bar{3}x^2+\bar{3}x+\bar{1} = (x+\bar{1})^3$.

Thus, $x^4+\bar{2}x^3-\bar{2}x-\bar{1} = (x-\bar{1})\,(x+\bar{1})^3$

This shows that $\bar{1}$ is a root of multiplicity 1 and $-\bar{1}$ $(= \bar{4})$ is a root of multiplicity 3.

E 12) a) Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$.

Then $\phi(f(x)+g(x)) = \phi\left(\sum_{i=0}^{t} (a_i+b_i)\, x^i\right)$, where $t = \max(m,n)$.

$$= \sum_{i=0}^{t} (a_i + b_i)a^i$$
$$= \sum_{i=0}^{t} a_i a^i + \sum_{i=0}^{t} b_i a^i$$
$$= f(a)+g(a)$$
$$= \phi(f(x))+\phi(g(x)), \text{ and}$$

$$\phi(f(x)\,g(x)) = \phi\left(\sum_{i=0}^{m+n}(a_ib_0+a_{i-1}b_1+\ldots+a_0b_i)x^i\right)$$

$$= \sum_{i=0}^{m+n}(a_ib_0+a_{i-1}b_1+\ldots+a_0b_i)a^i$$

$$= f(a)\,g(a)$$

$$= \phi(f(x))\,\phi(g(x)).$$

Thus, ϕ 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., $\phi(f(x)) = b$.

Thus, ϕ is surjective.

b) This is what we have shown in the previous two lines.

c) $f(x) \in \text{Ker}\,\phi$ iff $\phi(f(x)) = 0$ iff $f(a) = 0$

iff $(x-a) \mid f(x)$ iff $f(x) \in \langle x-a\rangle$.

Thus, Ker $\phi = \langle x-a\rangle$

The Fundamental Theorem of Homomorphism says that $F[x]/\langle x-a\rangle \simeq F$.

E 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 $p-1$ roots in Z_p, we find that the $(p-1)$ elements of Z_p^* are the only roots of $x^{p-1}-\bar{1}$.

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

E 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 14 SPECIAL INTEGRAL DOMAINS

Structure

14.1 INTRODUCTION

In this unit we shall look at 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 13 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. 14.2.

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 app. [illegible] called unique factorisation domains. While discussing them we shall introduce you [illegible] reducible 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.

Objectives

After studying 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.

14.2 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 $d : R \setminus \{0\} \to N \cup \{0\}$ is a Euclidean valuation on R if the 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 $\mathbf{Z}$ is a Euclidean domain.

Solution : Define, $d : \mathbf{Z} \to \mathbf{N} \cup \{0\} : d(n) = |n|$.

Then, for any $a,b \in \mathbf{Z} \setminus \{0\}$,

$$d(ab) = |ab| = |a|\,|b| \geq |a| \text{ (since } |b| \geq 1 \text{ for } b \neq 0)$$

$$= d(a),$$

i.e., $d(a) \leq d(ab)$.

Further, the division algorithm in $\mathbf{Z}$ (see Sec.1. 6.2) says that if $a, b \in \mathbf{Z}$, $b \neq 0$, then $\exists\, q, r \in \mathbf{Z}$ such that

$$a = bq+r, \text{ where } r = 0 \text{ or } 0 < |r| < |b|,$$

i.e., $a = bq+r$, where $r = 0$ or $d(r) < d(b)$.

Hence, d is a Euclidean valuation and $\mathbf{Z}$ 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 $d(a) = 1 \;\forall\; a \in F \setminus \{0\}$, is a Euclidean domain.

E 2) Let F be a field. Define the function

$$d : F[x] \setminus \{0\} \to \mathbf{N} \cup \{0\} : d(f(x)) = \deg f(x).$$

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 $\mathbf{Z}$ 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 $\mathbf{Z}$.

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 $F \setminus \{0\}$. 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 $F \setminus \{0\}$. Thus, the units of F[x] are the non-zero elements 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. Then there exists

$c+d\sqrt{-5} \in R$ such that

$$(a+b\sqrt{-5})\ (c+d\sqrt{-5}) = 1$$

$\Rightarrow$ $(ac-5bd)+(bc+ad)\sqrt{-5} = 1$

$\Rightarrow$ $ac-5bd = 1$ and $bc+ad = 0$

$\Rightarrow$ $abc-5b^2d = b$ and $bc+ad = 0$

$\Rightarrow$ $a(-ad)-5b^2d = b$, substituting $bc=-ad$.

$\Rightarrow$ $(a^2+5b^2)d = -b$.

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) Z_6, c) Z/5Z, d) Z+iZ.

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 $a \in R \setminus \{0\}$ 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, $d(r) < d(1)$ can't happen.

Thus, the only possibility for r is $r = 0$.

Therefore, $1 = aq$, so that a is a unit.

Conversely, assume that a is a unit in R. Let $b \in R$ 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 $n \in Z$ is a unit in Z iff $|n| = |1| = 1$. Thus, the only units 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 $I \setminus \{0\}$ is non-empty. Consider the set $\{ d(a) \mid a \in I \setminus \{0\}\}$. By the well ordering principle (see Sec. 1.6.1) this set has a minimal element. Let this be d(b), where $b \in I \setminus \{0\}$. 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 $I \subseteq R$ and 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 $d(b)$, $d(r) < d(b)$ is not possible.

Therefore, $r = 0$, and hence, $a = bq \in Rb$.

Thus, $I \subseteq Rb$. ...(2)

From (1) and (2) we get

$I = Rb$.

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 $\{d(x) \mid x \in I \setminus \{0\}\}$.

We also denote the principal ideal Ra by $< a >$.

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

$S = \{a \in R \setminus \{0\} \mid d(a) > d(1)\} \cup \{0\}$ is not an ideal of the Euclidean domain R with Euclidean valuation d.

Theorem 2 leads us to a concept that we shall discuss now.

14.3 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.

Every Euclidean domain is a PID.

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 PIDs. 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 a Euclidean domain. The proof of this is 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 $f(x) \in Z[x]$.

On the contrary, suppose that $\exists\, f(x) \in Z[x]$ such that $<2,x> = <f(x)>$. Clearly, $f(x) \neq 0$. Also, $\exists\, g(x), h(x) \in Z[x]$ 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 f(x) = 0, i.e., f(x) ∈ Z, say f(x) = n.

Then (2) shows that deg h(x) = 1. Let h(x) = ax+b with a,b ∈ 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 = ± 1.

Therefore, 1 ∈ < f(x) > = < x,2>. Thus, we can write

$1 = x(a_0+a_1x+...+a_rx^r) + 2(b_0+b_1x+...+b_sx^s)$, where $a_i, b_j \in Z \; \forall$ i = 0, 1,.....,r and j = 0,1,....,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, Z[x] is not a P.I.D.

Now, try the following exercises.

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 ∈ R, with a ≠ 0, then a **divides** b if there exists c ∈ R such that b = ac.

Now we would like to generalise 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 ∈ R is a **common divisor** of a and b if c|a and c|b.

An element d ∈ R is a **greatest common divisor** (g.c.d. in short) of a, b ∈ R if

i) d | a and d|b, and

ii) for any common divisor c of a and b, c|d.

For example, in Z a g.c.d of 5 and 15 is 5 , and a g.c.d of 5 and 7 is 1.

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 b, then d=ud' , for some unit u. For this we need a result that you can prove in the following exercise.

Two elements a and b in a domain R are called associates if a = bu for some unit u in R

E 9) Let R be an integral domain. Show that

a) u is a unit in R iff u | 1.

b) for a, b ∈ 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 ∈ 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 $d \mid d'$. Similarly, we get $d' \mid d$. 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 $R \times R$. But there should be no cause for confusion. The context will clarify what we are using the notation for.)

How do 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

$q(x) = 6x^2-10x-4$.

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 $q(x) = 2(x-2)(3x+1)$.

The g.c.d of p(x) 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 $Z / \langle 8 \rangle$,

b) $x^2+8x+15$ 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 ideal $\langle a,b \rangle$. Since R is a PID, this ideal must be principal also. Let $d \in R$ such that $\langle a,b \rangle = \langle d \rangle$. We will show that the g.c.d of a and b is d.

Since $a \in \langle d \rangle$, $d \mid a$. Similarly, $d \mid b$.

Now suppose $c \in R$ such that $c \mid a$ and $c \mid b$.

Since $d \in \langle a,b \rangle$, $\exists\ x, y \in R$ such that $d = ax+by$.

Since $c \mid a$ and $c \mid b$, $c \mid (ax+by)$, i.e., $c \mid d$.

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 4.

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 $a(x), b(x) \in F[x]$.

For example, in E 10 (c), $(x-1) = \frac{1}{5}(x^3-2x^2+6x-5)+\frac{(-x+2)}{5}(x^2-2x+1)$.

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 $a \mid bc$. Show that if $(a,b) = 1$, then $a \mid c$.

(Hint : By Theorem 4, $\exists\ x,y \in R$ such that $ax+by = 1$.)

Let us now discuss a concept related to that 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 R[x] and C[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 root 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.

A corollary to this result is

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) $x^2-2x+1 \in R[x]$

b) $x^2+x+1 \in C[x]$,

c) $x-i \in C[x]$

d) $x^3-3x^2+2x+5 \in R[x]$.

Let us now discuss the relationship between 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 $x \nmid a$. 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 $p \mid ab$. If $p \mid a$, 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 primeness) 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 10 of Unit 1. 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 $I_1, I_2, \ldots$ be an infinite sequence of ideals of R satisfying

$I_1 \subseteq I_2 \subseteq \ldots$

Then $\exists\, m \in N$ such that $I_m = I_{m+1} = I_{m+2} = \ldots$

Proof : Consider the set $I = I_1 \cup I_2 \cup \ldots = \bigcup_{n=1}^{\infty} I_n$. We will prove that I is an ideal of R.

Firstly, $I \neq \phi$, since $I_1 \neq \phi$ and $I_1 \subseteq I$.

Secondly, if $a,b \in I$, then $a \in I_r$ 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 an ideal of R. Since R is a PID, $I = \langle a \rangle$ 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, $I_m \subseteq I_{m+1} \subseteq I = I_m$. Therefore, $I_m = I_{m+1}$.

Similarly, $I_m = I_{m+2}$, and so on. Thus, $I_m = I_{m+1} = I_{m+2} \ldots$

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 $\langle p \rangle$ 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 PID. An ideal $\langle a \rangle$ is a maximal ideal of R iff a is a prime element of R.

Proof : If $\langle a \rangle$ 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 $\langle a \rangle \subseteq I$. Since R is a PID, $I = \langle b \rangle$ for some $b \in R$. We will show that b is a unit in R; and hence, by E 4, $\langle b \rangle = R$, i.e., $I = R$.

Now, $\langle a \rangle \subseteq \langle b \rangle \Rightarrow a = bc$ for some $c \in R$. Since a is irreducible, either b is an associate of a or b is a unit in R. But if b is an associate of a, then $\langle b \rangle = \langle a \rangle$, a contradiction. Therefore, b is a unit in R. Therefore, $I \neq R$.

Thus, $\langle a \rangle$ is a maximal ideal of R.

What Theorem 9 says is that **the prime ideals and maximal ideals coincide in a PID.**

Try the following exercise now.

E 14) Which of the following ideals are maximal? Give reasons for your choice.

a) $\langle 5 \rangle$ in Z,

b) $\langle x^2-1 \rangle$ in Q [x].

c) $\langle x^2+x+1 \rangle$ in R[x],

d) $\langle x \rangle$ in Z[x].

Now, take any integer n. Then we can have n = 0, or n = ± 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 PID 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 can write $a = a_1b_1$, where neither a_1 nor b_1 is an associate of a. Then $< a > \subsetneq < a_1 >$. 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 $< a_1 > \subsetneq < a_2 >$. Continuing in this way we get an increasing chain

$$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq \ldots\ldots$$

By Theorem 8, this chain stops with some $< a_n >$. Then a_n will 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 $p_1 | a$ 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, $< a > \subsetneq < a_1 >$. Similarly, $< a_1 > \subsetneq < a_2 >$. So, as the process continues we get an increasing chain of ideals,

$$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq \ldots\ldots$$

in the PID R. Just as in the proof of Theorem 10, this chain ends at $< a_m >$ for some $m \in \mathbb{N}$, 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 factorisation is the following result that you have already proved for $\mathbb{Z}$ in Unit 1.

Theorem 12 : Let R be a PID and $a \neq 0$ be non-invertible in R. Let $a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$, 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 R and if $p | a_1a_2 \ldots a_n$ (where $a_1, a_2, \ldots, a_n \in R$), then $p | a_i$ for some $i = 1, 2, \ldots, n$.

Now let us start the proof of Theorem 12.

Proof : Since $p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$, $p_1 | q_1q_2 \ldots q_m$.

Thus, by E 15, $p_1 | q_j$ for some $j = 1, \ldots, m$. By changing the order of the q_j, if necessary, we can assume that j = 1, i.e., $p_1 | q_1$. 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. Now we have

$$p_1p_2 \ldots p_n = (p_1u_1)\, q_2 \ldots q_m.$$

Cancelling 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

$1 = u_1 u_2 \ldots u_n q_{n+1} \ldots q_m$.

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_j, and vice versa.

What Theorem 12 says is that **any two prime factorisations 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, $x^2-1 \in R[x]$ can be written as $(x-1)(x+1)$ or $(x+1)(x-1)$ or $[\frac{1}{2}(x+1)][2(x-1)]$ in $R[x]$.

Now you can try the following exercise.

E 16) Give the prime factorisation of $2x^2-3x+1$ in $Q[x]$ and $Z_2[x]$.

The property that we have shown for a PID in Theorems 11 and 12 is true for several other domains also. Let us discuss such rings now.

14.4 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 $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$ be two factorisations into irreducibles, then $n = m$ and each p_i is an 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 Theorems 11 and 12 help? Of course! In them we have proved that **every PID is a UFD.**

Every Euclidean domain 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 field 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 $Z[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in Z\}$ is not a UFD.

Solution : Let us define a function

$f : Z[\sqrt{-5}] \to N \cup \{0\}$ 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

$f(\alpha\beta) = f(\alpha)\, f(\beta)\ \forall\ \alpha,\beta \in Z[\sqrt{-5}]$.

Now, 9 has two factorisations in $Z[\sqrt{-5}]$, namely,

$9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$.

In Example 3, you have already shown that the only units of $Z[\sqrt{-5}]$ 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 $\alpha,\beta \in Z[\sqrt{-5}]$.

Applying the function f we see that

$f(2+\sqrt{-5}) = f(\alpha)\, f(\beta)$.

i.e., $9 = f(\alpha)\, f(\beta)$.

Since $f(\alpha),\ f(\beta) \in N$ and α, β 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 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 factorisation of 9 as a product of irreducible elements is not unique. Therefore, $Z[\sqrt{-5}]$ 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 $2+\sqrt{-5} \nmid 3$. 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 $Z[\sqrt{-5}]$.

Now let us discuss some properties of a UFD. 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 that any element a in a UFD R can be written as

$$a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$$

where the p_is 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 ∈ R.

Let $a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$

where $p_1, p_2, \ldots, p_n$ are distinct irreducible elements of R and r_i and s_i are 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 $20 = 2^2 \times 3^0 \times 5^1$ and $15 = 2^0 \times 3^1 \times 5^1$.)

Now, let $t_i = \min(r_i, s_i)$ $\forall$ i = 1, 2,....,n.

Then $d = p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}$ divides a as well as b, since $t_i \le r_i$ and $t_i \le s_i$ $\forall$ 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, $c = p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}$, where $m_i \le r_i$ and $m_i \le s_i$ $\forall$ i = 1,2,...,n. Thus, $m_i \le t_i$ $\forall$ i = 1,2,...,n.

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 element. 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 E13 we know that every prime in R is irreducible. So let us prove the converse.

Let a ∈ R be irreducible and let a|bc, where b,c ∈ 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∤b. Let bc = ad, where d ∈ R.

Let $b = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $c = q_1^{s_1} q_2^{s_2} \ldots q_n^{s_n}$ be irreducible factorisations of b and c. Since bc = ad and a is irreducible, a must be one of the p_is or one of the q_js. Since a∤b, $a \ne p_i$ 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 to Example 4 for a moment. Over there we gave you an example of a PID R, for which R[x] is not a PID. You may ask what happens to 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. You can use it to solve the following exercises.

E 20) Give an example of a UFD which is not a PID.

E 21) If p is an irreducible element 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.

14.5 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 are 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 roots in 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 and F[x] are UFDs, for any field F.
11) In a UFD (and hence, in a PID) an element is prime iff it is irreducible.
12) Any two elements in a UFD have a g.c.d.
13) If R is a UFD, then so is R[x].

14.6 SOLUTIONS/ANSWERS

E 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.

E 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.

E 3) a) $m \in \mathbb{Z}$ is a unit iff $\exists\ n \in \mathbb{Z}$ such that $mn = 1$, i.e., iff $m = \pm 1$.

b) Let $\bar{m} \in \mathbb{Z}_6$ be a unit. Then $\exists\ \bar{n} \in \mathbb{Z}_6$ such that $\bar{m}\,\bar{n} = \bar{1}$.

Thus, from Sec. 1.6.2 we see that m is a unit if the g.c.d of m and 6 is 1.

$\therefore\ \bar{m} = \bar{1}$ or $\bar{5}$.

c) $\mathbb{Z}/5\mathbb{Z}$ is a field. Thus, the units are all its non-zero elements.

d) Let a+ib be a unit. Then $\exists$ c+id $\in \mathbb{Z}+i\mathbb{Z}$ such that

$(a+ib)(c+id) = 1$.

$\Rightarrow (ac-bd)+(ad+bc)i = 1$

$\Rightarrow ac-bd = 1$ and $ad+bc = 0$.

$\Rightarrow b = 0$, as in Example 3.

Thus, $a+ib = 1$ or -1, using (a) above.

E 4) Let $u \in R$ be a unit. Then $\exists\ v \in R$ such that $vu = 1$. Thus, for any $r \in R$, $r = r.1 = r(vu) = (ry)u \in Ru$.

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.

E 5) Apply Theorem 2 to the Euclidean domain F[x].

E 6) Let $R = \mathbb{Z}$. Then $S = \{n \in \mathbb{Z}^* \mid |n| > 1\} \cup \{0\}$.

Then $2 \in S$, $3 \in S$ but $2-3 \notin S$ since $|2-3| \not> 1$.

Thus, S is not even a subring of R.

E 7) For example, $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$, which is a PID. But $\mathbb{Z}[x]$ is not a PID.

E 8) $\mathbb{Z}$ is a PID. But $\mathbb{Z}/6\mathbb{Z}$ is not even a domain. Thus, it is not a PID.

E 9) a) u is a unit iff $uv = 1$ for some $v \in R$ iff $u \mid 1$.

b) $a \mid b$ and $b \mid a$

$\Rightarrow b = ac$ and $a = bd$ for some $b, d \in R$.

$\Rightarrow b = bdc$

$\Rightarrow b = 0$ 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 b are associates.

Conversely, let a and b be associates in R, say $a = bu$, where u is a unit in R. Then $b \mid a$. Also, let $v \in R$ such that $uv = 1$. Then $av = buv = b$.

Thus, $a \mid b$.

E 10) a) $\bar{2}$.

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) $x^3-2x^2+6x-5 = (x-1)(x^2-x+5)$, $x^2-2x+1 = (x-1)^2$.

Thus, their g.c.d is $x-1$.

E 11) $\exists\ x,y \in R$ such that $ax+by = 1$.

Then $c = 1.c = (ax+by)c = acx+bcy$

Since $a \mid ac$ and $a \mid bc$, $a \mid (acx+bcy) = c$.

E 12) (c) is, because of Theorem 5'.

(a) is not, since it is $(x-1)^2$.

(b) is not, because of Theorem 5'.

(d) is not, because of Theorem 6.

E 13) Let $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Suppose $p \nmid a$. 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.

E 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 $Z[x]/\langle x \rangle \simeq Z$, which is not a field.

E 15) The result is clearly true for $n = 1$. Assume that it holds for all $m < n$, i.e., whenever $m < n$ and $p \mid a_1a_2....a_m$, then $p \mid a_i$ for some $i = 1,2,....,m$.

Now let $p \mid a_1a_2...a_n$. Then $p \mid (a_1a_2.....a_{n-1})a_n$.

Since p is a prime element, we find that $p \mid a_1a_2 ...a_{n-1}$ or $p \mid a_n$.

If $p \mid a_1a_2....a_{n-1}$, then $p \mid a_i$ for some $i = 1,....,n-1$ by our assumption.

If $p \nmid a_1.... a_{n-1}$, $p \mid a_n$.

Thus, in either case, $p \mid a_i$ for some $i = 1,...., n$.

So, our result is true for n.

Hence, it is true $\forall\ n \in N$.

E 16) $2x^2-3x+1 = (2x-1)(x-1)$ in Q[x].

In $Z_2[x]$ the given polynomial is $x+\bar{1}$, since $\bar{2} = \bar{0}$ and $-\bar{3} = \bar{1}$.

This polynomial is linear, and hence, irreducible over Z_2.

Thus, its prime factorisation is just $x+\bar{1}$.

E 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 $g_1(x) = f_2(x)g_2(x)$. Then deg $g_2(x) <$ deg $g_1(x)$. 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 $f_i(x)$ is prime in F[x].

Now, to show that the factorisation is unique you go along the lines of the proof of Theorem 12.

E 18) $10 = 2 \times 5 = 5 \times 2$.

E 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 $\mathbf{Z}[\sqrt{-5}]$.

E 20) $\mathbf{Z}[x]$.

E 21) No. For example, x is irreducible in $\mathbf{Z}[x]$; but $\bar{x}$ is zero in $\mathbf{Z}[x]/\langle x \rangle \simeq \mathbf{Z}$.

E 22) The quotient ring of a domain need not be a domain. For example, $\mathbf{Z}$ is a UFD, but $\mathbf{Z}/\langle 4 \rangle$ is not.

Also, even if the quotient ring is a domain, it may not be a UFD. For example, $\mathbf{Z}[\sqrt{-5}] \simeq \mathbf{Z}[x]/\langle x^2+5 \rangle$ is not a UFD, while $\mathbf{Z}[x]$ is.

E 23) No. For example, $\mathbf{Z}[\sqrt{-5}]$ is a subring of $\mathbf{C}$, a UFD. But $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

UNIT 15 IRREDUCIBILITY AND FIELD EXTENSIONS

Structure

15.1 INTRODUCTION

In the previous unit we discussed various kinds of integral domains, including unique factorisation 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 is a field extension of Q or Z_p for some prime p. Because of this we call Q and the Z_ps prime fields. We will discuss these fields briefly.

Finally, we will look at finite fields. These fields were introduced by the young French mathematician Evariste Galois (Fig. 1) while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them.

Fig. 1: Evariste Galois (1811–1832)

Before reading this unit we suggest that you go through the definitions of irreducibility from Unit 14. 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 simple.

Objectives

After reading this unit, you should be able to

- prove and use Eisenstein's criterion for irreducibility in Z[x] and Q[x];
- obtain field extensions of a field F from F[x];
- obtain the prime field of any field;
- use the fact that any finite field F has p^n elements, where char F = p and $\dim_{Z_p} F = n$.

15.2 IRREDUCIBILITY IN Q[X]

In Unit 14 we introduced you to irreducible 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 1 or degree 2. Thus, any polynomial over R of degree more than 2 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 discovered by the nineteenth century mathematician Ferdinand Eisenstein. In this section we will build up the theory for proving this useful criterion.

Let us start with a definition.

Definition: Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$. We define the content of f[x] to be the g.c.d of the integers $a_0, a_1, \ldots, a_n$.

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) $5(2x^2 - 1)(x + 2)$.

E 2) Prove that any polynomial $f(x) \in Z[x]$ can be written as $dg(x)$, where d is the content of f(x) and g(x) is a primitive polynomial.

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 $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$ and

$g(x) = b_0 + b_1x + \ldots + b_mx^m \in Z[x]$, where the

g.c.d of $a_0, a_1, \ldots, a_n$ is 1 and the g.c.d of $b_0, b_1, \ldots, b_m$ is 1. Now

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

where $c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0$.

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 $c_0, c_1, \ldots, c_{m+n}$ is greater than 1, and hence some prime p must divide it. Thus, $p \mid c_i \; \forall \; i = 0, 1, \ldots, m+n$. 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

$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + \ldots + a_rb_s + \ldots + a_{r+s}b_0$

$= a_rb_s + (a_0b_{r+s} + a_1b_{r+s-1} + \ldots + a_{r-1}b_{s+1} + a_{r+1}b_{r-1} + \ldots + a_{r+s}b_0)$

By our choice of r and s, $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$, and $p \mid b_0, p \mid b_1, \ldots, p \mid b_{s-1}$. Also $p \mid c_{r+s}$.

Therefore, $p \mid c_{r+s} - (a_0b_{r+s} + \ldots + a_{r-1}b_{s+1} + a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)$

i.e., $p \mid a_rb_s$.

$\Rightarrow p \mid a_r$ or $p \mid b_s$, since p is a prime.

But $p \nmid a_r$ 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 l.c.m 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? We get

$30f(x) = 45x^3 + 6x^2 + 90x + 10 \in Z[x]$

Using the same process, we can multiply any $f(x) \in Q[x]$ by a suitable integer d so that $df(x) \in Z[x]$. We will use this fact while relating irreducibility in Q[x] with irreducibility in Z[x].

Theorem 2: If $f(x) \in Z[x]$ 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 $g(x) \in Q[x]$, $\exists\ m \in Z$ such that $mg(x) \in Z[x]$. Similarly, $\exists\ n \in Z$ such that $nh(x) \in Z[x]$. Then,

$$mnf(x) = mg(x)\ nh(x) \qquad \ldots (1)$$

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

$$mnrf_1(x) = stg_1(x)\ h_1(x) \qquad \ldots(2)$$

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 Z[x], where neither $rg_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that f(x) is irreducible in Z[x].

Thus, our supposition is false. Hence, f(x) must be irreducible in Q[x].

What this result says is that to check irreducibility of a polynomial in Q[x], it is enough to check it in Z[x]. And, for checking it in Z[x] we have the terrific Eisenstein's criterion, that we mentioned at the beginning of this section.

Theorem 3 (Eisenstein's Criterion) : Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$. Suppose that for some prime number p,

i) $p \nmid a_n$,

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 Z[x] (and hence in Q[x]).

Proof: Can you guess our method of proof? By contradiction, once again! So suppose f(x) is reducible in Z[x].

Let $f(x) = g(x)h(x)$,

where $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, $m > 0$ 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 $a_0 = b_0c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0c_0 \Rightarrow p \mid b_0$ 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, $a_k = (b_0 c_k + .. + b_{k-1} c_1) + b_k c_0$.

Since $p \mid a_k$ and $p \mid b_0$, $p \mid b_1$, ... $p \mid b_{k-1}$, we see that $p \mid a_k - (b_0 c_k + ... + b_{k-1} c_1)$, i. e., $p \mid b_k c_o$. But $p \nmid b_k$ and $p \nmid c_0$. So we reach a contradiction.

Thus, f(x) must be irreducible in Z[x].

Let us illustrate the use of this criterion.

Example 1: Is $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ irreducible in 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, $Q[x]/\langle x^3-p \rangle$ 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

$f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ 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, $f(x) = \dfrac{x^p - 1}{x - 1}$.

$$\therefore \quad f(x+1) = \frac{(x+1)^p - 1}{x}$$

$$= \frac{1}{x}\left(x^p + {}^pC_1 x^{p-1} + \ldots + {}^pC_{p-1} x + 1 - 1\right), \text{ (by the binomial theorem)}$$

$$= x^{p-1} + {}^pC_1 x^{p-2} + \ldots + {}^pC_{p-1}$$

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 $a_0 + a_1 x + ... + a_n x^n \in Z[x]$ is irreducible in 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 Z[x] are irreducible over 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., $b^2 \nmid a$ for any $b \in Z$. Show that $Z[x]/\langle x^p+a \rangle$ is an integral domain.

E 7) Show that $x^p + \bar{a} \in Z_p[x]$ is not irreducible for any $\bar{a} \in Z_p$.

(**Hint:** Does E 13 of Unit 13 help?)

So far we have used the fact that if $f(x) \in Z[x]$ 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 $f(x) \in R[x]$ 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.

15.3 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 called 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) $a \in S, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

Why don't you use Theorem 5 to do the following exercise now.

E 8) Show that

a) $Q + iQ$ is a subfield of C.

b) $Z + \sqrt{2}Z$ is not a subfield of 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 Unit 12). 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 $f(x), g(x) \in F[x]$ and $g(x) \neq 0$.

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, $F[x]/\langle f(x)\rangle$ is a field iff $f(x)$ is irreducible over F.

Now, given any $f(x) \in F[x]$, such that deg $f(x) > 0$, we will show that there is a field monomorphism from F into $F[x]/\langle f(x)\rangle$. This will show that $F[x]/\langle f(x)\rangle$ contains an isomorphic copy of F; and hence, we can say, that it contains F.
So, let us define $\phi : F \to F[x]/\langle f(x)\rangle$: $\phi(a) = a + \langle f(x)\rangle$.

Then $\phi(a+b) = \phi(a) + \phi(b)$, and

$\phi(ab) = \phi(a)\,\phi(b)$.

Thus, ϕ is a ring homomorphism.

What is Ker ϕ ?

$\text{Ker}\,\phi = \{a \in F \mid a + \langle f(x)\rangle = \langle f(x)\rangle\}$

$= \{a \in F \mid a \in \langle f(x)\rangle\}$

$= \{a \in F \mid f(x) \mid a\}$

$= \{0\}$, since deg $f > 0$ and deg $a \leq 0$.

Thus, ϕ is 1–1, and hence an inclusion.

Hence, F is embedded in $F[x]/\langle f(x)\rangle$.

Thus, if $f(x)$ is irreducible in F[x], then $F[x]/\langle f(x)\rangle$ is a field extension of F.

Now for a related exercise !

E 9) Which of the following rings are field extensions of Q?

a) $Q[x]/\langle x^3 + 10\rangle$,

b) $R[x]/\langle x^2 + 2\rangle$,

c) Q.

d) $Q[x]/\langle x^2 - 5x + 6\rangle$.

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.

15.3.1 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 going into the proof we suggest that you do a quick revision of Theorems 3, 4 and 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

$f : Z \to F : f(n) = n.1 = 1 + 1 + \ldots + 1$ (n times).

In E 11 of Unit 12 you have shown that f is a ring homomorphism and Ker f = pZ, where p is the characteristic of F.

Now, 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. $\therefore$ $Z \simeq f(Z)$. 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 p is a prime number, Z/pZ is a field.

Also, by applying the Fundamental Theorem of Homomorphism to f, we get $Z/pZ \simeq f(Z)$.

Thus, f(Z) is isomorphic to Z_p and is contained in F. Hence, F has a 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 Z_p (where p is a prime number) we call these fields **prime fields.**

Thus, the prime fields are Q, Z_2, Z_3, Z_5, etc.

We call the subfield isomorphic to a prime field (obtained in Theorem 6), the **prime subfield** of the given field.

Let us again reword Theorem 6 in terms of field extensions. What it says is that **every field is a field extension of a prime 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 is a field extension of K, the unity of F and K is the same, namely, 1. Therefore, the least positive integer n such that n.1 = 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_5 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 Z_p.

15.3.2 Finite Fields

You have dealt a lot with the finite fields Z_p. Now we will look at field extensions of these fields. You know that any finite field F has characteristic p, for some prime p. And then F is

an extension of 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 that 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' $\cdot : K \times V \to V$ 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 know that (F, +) is an abelian group. We also know that the multiplication in F will satisfy all the conditions that the scalar multiplication should satisfy. Thus, F is a vector space over Z_p. Since F is a finite field, it has a finite dimension over Z_p.
Let $\dim_{Z_p} F = n$. Then we can find $a_1, \ldots, a_n \in F$ such that

$$F = Z_p a_1 + Z_p a_2 + \ldots + Z_p a_n.$$

We will show that F has p^n elements.

Now, any element of F is of the form

$b_1 a_1 + b_2 a_2 + \ldots + b_n a_n$, where $b_1, \ldots, b_n \in Z_p$.

Now, since $o(Z_p) = p$, b_1 can be any one of its p elements.

Similarly, each of $b_2, b_3, \ldots, b_n$ 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
$p \times p \times \ldots \times p$ (n times) $= p^n$.

The order of a finite field is the number of elements in it.

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 $n \in N$, there exists a field with p^n elements. Moreover, any two finite fields having the same number of elements are isomorphic.

Now, you can utilise your knowledge of finite fields to solve the following exercises. The first exercise is a generalisation of E 13 in Unit 13.

E 14) Let F be a finite field with p^n elements. Show that $a^{p^n} = a\ \forall\ a \in F$. 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 $p^n - 1$.)

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 an automorphism of F of order n, i.e., f is an isomorphism such that $f^n = I$, and $f^r \neq I$ for $r < n$.

f is called the Frobenius automorphism of F, after the mathematician Georg Frobenius (1848–1917).

E 16) Let F be a field such that $a \in F$ iff a is a root of $x^{27} - x \in F[x]$.

a) What is char F?

b) Is $Z_2 \subseteq F$?

c) Is $Q \subseteq F$?

d) Is $F \subseteq Q$? Why?

E 17) 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.

15.4 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 irreducibility criterion for polynomials over $\mathbf{Z}$ and $\mathbf{Q}$. This states that if $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbf{Z}[x]$ and there is a prime $p \in \mathbf{Z}$ such that

   i) $p \mid a_i \ \forall \ i = 0, 1, \ldots, n-1$.

   ii) $p \nmid a_n$, and

   iii) $p^2 \nmid a_0$.

   then f(x) is irreducible over $\mathbf{Z}$ (and hence over $\mathbf{Q}$).

3) For any $n \in \mathbf{N}$, we can obtain an irreducible polynomial over $\mathbf{Q}$ 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 $\mathbf{Q}$ or 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 $x^{p^n} - x$ 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.

15.5 SOLUTIONS/ANSWERS

E 1) a) 1, b) 7, c) 5

E 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,

$f(x) = db_0 + db_1 x + \ldots + db_n x^n = d(b_0 + b_1 x + \ldots + b_n x^n) = d\, g(x)$.

E 3) $f(x) = x^n - p = a_0 + a_1 x + \ldots + a_n x^n$,

where $a_0 = -p$, $a_1 = 0 = \ldots = a_{n-1}$, $a_n = 1$

Thus, $p \mid a_i \forall i = 0, 1, \ldots, n-1$, $p^2 \nmid a_0$, $p \nmid a_n$.

So, by the Eisenstein criterion, f(x) is irreducible over Q.

E 4) Not necessarily.

For example, there is no p that satisfies the conditions for f(x) in Example 3.

E 5) All of them, (a) and (b), because of Eisenstein's criterion; and (c), because any linear polynomial is irreducible.

E 6) Since $a \neq 0, \pm 1$, $\exists$ a prime q such that $q \mid a$. 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, $< x^p + a >$ is a prime ideal of Z[x].

Hence the result.

E 7) By E 13 of Unit 13 we know that $\bar{a}^p = \bar{a} \quad \forall \ \bar{a} \in Z_p$. Now consider

$x^p + \bar{a} \in Z_p[x]$.

$\overline{p-a}$ is a zero of this polynomial, since

$(\overline{p-a})^p + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0}$ in Z_p.

Thus, $x^p + \bar{a}$ is reducible over Z_p.

E 8) a) Q + iQ is a non-empty subset of C.

Now, let a+ib and c+id be in Q+iQ.

Then $(a + ib) - (c + id) = (a - c) + i(b - d) \in Q + iQ$.

Further, let $c + id \neq 0$, so that $c^2 + d^2 \neq 0$.

Then $(c + id)^{-1} = \frac{c - id}{c^2 + d^2}$

Thus, $(a + ib)(c + id)^{-1} = (a + ib)\frac{(c - id)}{c^2 + d^2}$

$= \frac{(ac + bd)}{c^2 + d^2} + i\frac{(bc - ad)}{c^2 + d^2} \in Q + iQ$.

Thus, Q + iQ is a subfield of C.

b) $2 \in Z + \sqrt{2}Z$ but $2^{-1} \notin Z + \sqrt{2}Z$. Therefore,

$Z + \sqrt{2}Z$ is not a field, and hence not a subfield of R.

E 9) (a), (b) and (c).

E 10) Let F be a field and 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 subfield. Hence, this is the smallest subfield of F.

E 11) F must contain a prime subfield. But it contains no proper subfield. Hence, it must be its own prime subfield. That is, F must be isomorphic to a prime field.

E 12) Q, Z_5, Z_2, since their characteristics are 0,5 and 2, respectively.

E 13) Let 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.

E 14) Since $(F\setminus\{0\},.)$ is a group of order $p^n - 1$, $a^{p^n-1} = 1$

$\forall\ a \in F\setminus\{0\}$.

$\therefore a^{p^n} = a\ \forall\ a \in F\setminus\{0\}$. 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 $x^{p^n} - x$.

$$\therefore x^{p^n} - x = \prod_{a_i \in F} (x - a_i).$$

E 15) $f(a + b) = (a + b)^p = a^p + b^p$ (using E 10 of Unit 12)

$= f(a) + f(b)$.

$f(ab) = (ab)^p = a^p b^p = f(a)\ f(b)$.

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 $f \subseteq F$ $\therefore$ 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 $x^{p^r} - x \in F[x]$ has more than p^r 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., $a^{3^3} = a$.

a) Char F = 3.

b) No, since char $Z_2 \neq$ char F.

c) No.

d) No, since $F \subseteq Q \Rightarrow$ char F = char Q = 0.

E 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.

NOTES