ALAGAPPA UNIVERSITY

[Accredited with 'A+' Grade by NAAC (CGPA:3.64) in the Third Cycle
and Graded as Category–I University by MHRD-UGC]

(A State University Established by the Government of Tamil Nadu)

KARAIKUDI – 630 003

Directorate of Distance Education

M.Sc. [Mathematics]

I - Semester

311 11

ALGEBRA - I

Reviewer	
Dr. M. Mullai	Assistant Professor Alagappa University, Karaikudi

Authors:

Vijay K Khanna & S K Bhambri, *Formerly Associate Professors, Department of Mathematics, Kirori Mal College, University of Delhi*
Units (1-10, 11.0-11.1, 11.3-11.8, 12.0-12.2, 13-14)

Surjeet Singh, *Former Professor, King Saud University, Riyadh, Saudi Arabia*
Qazi Zameeruddin, *Formerly Lecturer, Department of Mathematics, Kirori Mal College, University of Delhi*
Units (11.2, 12.3)

VIKAS® PUBLISHING HOUSE PVT. LTD.
E-28, Sector-8, Noida - 201301 (UP)
Phone: 0120-4078900 • Fax: 0120-4078999
Regd. Office: 7361, Ravindra Mansion, Ram Nagar, New Delhi 110 055
• Website: www.vikaspublishing.com • Email: helpline@vikaspublishing.com

Work Order No. AU/DDE/DE1-621/Printing of Course Materials/2019, dated 09.12.2019 Copies 200

SYLLABI-BOOK MAPPING TABLE

Algebra - I

Syllabi	Mapping in Book
BLOCK I: GROUPS AND NORMAL SUBGROUPS **UNIT - I** Set Theory - Mappings - The Integers - problems **UNIT - II** Group Theory - Definition of a group - Some examples of Groups - Some preliminary Lemmas - Subgroups **UNIT - III** A counting principle - Normal subgroups and Quotient groups **UNIT - IV** Homomorphisms - Automorphisms - Cayley's Theorem - Permutation Groups	**Unit 1:** Set Theory **(Pages 1-22);** **Unit 2:** Group Theory **(Pages 23-45);** **Unit 3:** A Counting Principle **(Pages 46-62);** **Unit 4:** Cayley's Theorem **(Pages 63-85)**
BLOCK II: SYLOW'S THEOREM AND RING THEORY **UNIT - V** Another counting Principle - Application - Related problems **UNIT - VI** Sylow's Theorem - Direct products - Problems **UNIT - VII** Finite Abelian Groups - Supplementary problems **UNIT - VIII** Ring Theory: Definition and examples of rings - Some special classes of Rings	**Unit 5:** Another Counting Principle **(Pages 86-100);** **Unit 6:** Sylow's Theorem **(Pages 101-129);** **Unit 7:** Finite Abelian Groups **(Pages 130-146);** **Unit 8:** Ring Theory **(Pages 147-162)**
BLOCK III: RING HOMOMORPHISM, IDEALS AND FIELDS **UNIT - IX** Ring Homomorphisms - Ideals and Quotient Rings - Problems **UNIT - X** More ideals and Quotient Rings - Related Problems **UNIT - XI** The field of quotients of an Integral Domain - Euclidean Rings - Related Problems	**Unit 9:** Ideals, Quotient Rings, Ring Homomorphism **(Pages 163-182);** **Unit 10:** More Ideals Rings **(Pages 183-201);** **Unit 11:** The Field of Quotients of an Integral Domain and Euclidean Rings **(Pages 202-225)**
BLOCK IV: EUCLIDEAN RING AND POLYNOMIAL RING **UNIT - XII** A Particular Euclidean Ring - Polynomial Rings **UNIT - XIII** Polynomials over the Rational Field - Related Problems **UNIT - XIV** Polynomial Rings over Commutative Rings - Supplementary Problems	**Unit 12:** A Particular Euclidean Ring **(Pages 226-235)** **Unit 13:** Polynomials Over the Rational Field **(Pages 236-251);** **Unit 14:** Polynomial Rings Over Commutative Rings **(Pages 252-264)**

CONTENTS

INTRODUCTION

NOTES

Algebra is a branch of mathematics dealing with symbols and the rules for manipulating those symbols. In elementary algebra, those symbols represent quantities without fixed values, known as variables. Just as sentences describe relationships between specific words, in algebra, equations describe relationships between variables. Building a solid conceptual understanding of algebra is absolutely fundamental.

This book, *Algebra I*, is divided into four blocks which have been further sub-divided into fourteen units. The first block comprising four units covers the topics like Groups and Normal Subgroups. The second block comprising four units deals with Sylow's Theorem and Ring Theory. Third block included Ring Homomorphism, Ideals and Fields. Euclidean Ring and Polynomial Ring are the subject areas of fourth block. Different concepts have been explained with the help of examples. A large number of problems with solutions have been provided to assist one get a firm grip on the ideas developed. There is plenty of scope for the reader to try and solve problems on his own. In all, a substantial variety of challenges (and rewards) is assured.

The book follows the self-instructional mode wherein each unit begins with an Introduction to the topic. The Objectives of units are then outlined before going on to the presentation of the detailed content in a simple and structured format. Check Your Progress questions are provided to test the student's understanding of the subject. A Summary, a list of Key Words and a set of Self- Assessment Questions and Exercises are provided at the end of each unit for recapitulation.

BLOCK - I

GROUPS AND NORMAL SUBGROUPS

NOTES

UNIT 1 SET THEORY

Structure

1.0 INTRODUCTION

In this unit, you will be acquainted with some basic concepts in mathematics. The unit explains the concepts of sets along with operations in sets and then goes on to define the all-important notion of a mapping/function, which finally leads you to the results of number theory.

1.1 OBJECTIVES

After going through this unit, you will be able to:

- Understand the basics of set theory
- Learn the operations in sets
- Know about mapping
- Discuss number theory
- Solve related problems

1.2 SET THEORY

The notion of a set is most fundamental in Mathematics, but it is not our endeavour in this text to enter into the axiomatic study of set theory. We'll, instead, borrow the word 'set' from the language and be content to refer to it as a collection of objects. To give it a more precise shape, by a set, we will mean a collection of

NOTES

objects such that given any object, it is possible to ascertain whether that object belongs to the given collection or not. For instance, we can talk of set of all natural numbers, set of all students in a particular class, etc. If x is an element (member) of a set A we say x belongs to A and express it as $x \in A$. If y is not a member of A we say y does not belong to A and write $y \notin A$. We shall use capital letters A, B, X, Y etc. for denoting sets and small letters, a, b, c, x, y etc. for the elements (or members or objects).

Two sets A and B are said to be *equal* if they contain precisely the same elements and we write $A = B$.

A set can be described in various ways. For example, if A is the set containing 1, 2, 3, 4, 5, 6, we can write it as

$$A = \{1, 2, 3, 4, 5, 6\}$$

$$A = \{1, 2, ..., 6\}$$

$$A = \{x \in \mathbf{N} \mid x \leq 6\}$$

where **N** is set of all natural numbers. The last notation reading as: those x in the set of natural numbers which satisfy the property that $x \leq 6$.

We do not repeat any element while writing the elements in a set. Again, the order in which the elements are written is immaterial. Thus {1, 2, 3} and {2, 1, 3} mean the same set.

A set having no element is called an *empty set* or a *null set* or a *void set*. It is denoted by Φ or φ. Obviously any two empty sets are equal. A set will be called *finite* if either it is empty or has finite number of elements, *i.e.,* the elements can be listed by natural numbers such that the process of listing stops after a certain definite stage. A set with infinite number of elements is referred to as an infinite set.

The set {1, 2, 3, ..., 1000} is a finite set, whereas the set of all integers is infinite. Again the set of all rational numbers whose square is 2 is an empty set.

We use the notation $o(S)$ or $|S|$ to mean the number of elements in the set S and read it as *order of S* (sometimes also called its *cardinality*).

Subsets

We say a set A is contained in a set B (in symbols $A \subseteq B$) if every element of A is in B. A is then called subset of B and B is called superset of A. If in addition to this there is at least one element in B which is not in A, we say A is strictly contained in B ($A \subset B$) and call A a proper subset of B. $A \not\subset B$ means A is not a subset of B. Also $A \subseteq B$ and $B \supseteq A$ mean the same.

It is clear then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Also, $A \subseteq A$, $\varphi \subseteq A$ for any set A.

Definition: By *union* of two sets A and B, we mean the set $A \cup B$ which contains all the elements of A as well as B. Thus $A \cup B = \{x \mid x \in A \text{ or } x \in B \text{ (or both)}\}$.

NOTES

By *intersection* of two sets A and B, we mean the set $A \cap B$ which contains all the elements of A and B. Thus $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

The *difference* of two sets A and B is defined to be the set

$$A - B = \{x \mid x \in A,\ x \notin B\}.$$

In case $B \subset A$, then $A - B$ is called the complement of B in A. If there is no confusion regarding the set A, complement of B in A is denoted by B'.

Example 1: Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$

Then $A \cap B = \{3\}$

$A \cup B = \{1, 2, 3, 4, 5, 6\}$

$A - B = \{1, 2\}$

Theorem 1: *If A, B, C are sets then the following results hold:*

(*i*) $A \cap A = A,\ A \cup A = A$

(*ii*) $A \cap \varphi = \varphi,\ A \cup \varphi = A$

(*iii*) $A \cap B = B \cap A,\ A \cup B = B \cup A,\ A \cap B \subseteq A \subseteq A \cup B$

(*iv*) $A \cap (B \cap C) = (A \cap B) \cap C,\ A \cup (B \cup C) = (A \cup B) \cup C$

(*v*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(*vi*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof: We will prove (*v*), and leave others for the reader to try as an exercise.

Let $x \in A \cap (B \cup C)$ be any element.

Then $x \in A$ and $x \in B \cup C$

$\Rightarrow x \in A$ and $x \in B$ or $x \in C$.

If $x \in B$, then as $x \in A$, $x \in A \cap B$

If $x \in C$, then as $x \in A$, $x \in A \cap C$.

i.e. $x \in A \cap B$ or $x \in A \cap C$ (or both, of course)

$\Rightarrow x \in (A \cap B) \cup (A \cap C)$

$\Rightarrow A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ ... (1)

Again, $y \in (A \cap B) \cup (A \cap C)$

$\Rightarrow y \in A \cap B$ or $y \in A \cap C$

$\Rightarrow y \in A$ and B or $y \in A$ and C

$\Rightarrow y \in A$ and $y \in B$ or C

$\Rightarrow y \in A$ and $y \in B \cup C$

$\Rightarrow y \in A \cap (B \cup C)$

$\Rightarrow (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ ...(2)

(1) and (2) give us the result.

Theorem 2: (*DeMorgan's laws*). *For sets A, B in a set X,*

(*i*) $X - (A \cup B) = (X - A) \cap (X - B)$ *or* $(A \cup B)' = A' \cap B'$

(*ii*) $X - (A \cap B) = (X - A) \cup (X - B)$ *or* $(A \cap B)' = A' \cup B'$

NOTES

Proof: (*i*) Let $x \in X - (A \cup B)$ be any element.

Then $x \in X,\ x \notin A \cup B$

$\Rightarrow x \in X,\ x \notin A,\ x \notin B$

$\Rightarrow x \in X - A, x \in X - B$

$\Rightarrow x \in (X - A) \cap (X - B)$

$\Rightarrow X - (A \cup B) \subseteq (X - A) \cap (X - B)$ ...(1)

Again $y \in (X - A) \cap (X - B)$

$\Rightarrow y \in X - A,$ and $y \in X - B$

$\Rightarrow y \in X,\ y \notin A$ and $y \in X,\ y \notin B$

$\Rightarrow y \in X$ and $y \notin A \cup B$

$\Rightarrow y \in X - (A \cup B)$

$\Rightarrow (X - A) \cap (X - B) \subseteq X - (A \cup B)$ ...(2)

(1) & (2) give us the result.

(*ii*) Prove similarly.

Definition: Given two elements $a,\ b$ of a set of X, we define the ordered pair $(a,\ b)$ to be the set $\{\{a\},\ \{a,\ b\}\}$. a is called the first component (or first co-ordinate) and b is called the second component (or second co-ordinate).

We show $(a,\ b) = (c,\ d) \Leftrightarrow a = c,\ b = d$

If $a = c,\ b = d$ then the result is obvious.

Conversely, $(a,\ b) = (c,\ d)$

$\Rightarrow \{\{a\}, \{a,\ b\}\} = \{\{c\}, \{c, d\}\}$

Since the two sets are equal, they contain same elements.

Thus, $\{a\} = \{c\}$ or $\{a\} = \{c,\ d\}$

If $\{a\} = \{c\},$ then $\{a,\ b\} = \{c,\ d\}$

$\Rightarrow a = c$ and $b = d$ (as $a = c$)

Again, if $\{a\} = \{c,\ d\}$ then $\{a,\ b\} = \{c\}$

$\Rightarrow a = c,\ a = d,\ a = c,\ b = c$

$\Rightarrow a = c = b = d$

$\Rightarrow a = c,\ b = d$

Hence the result follows.

We thus notice, the order in which the elements are written is important in as much as (a, b) is not same as (b, a) unless $a = b$, whereas, of course, the two sets $\{a, b\}$ and $\{b, a\}$ are same.

Relations

NOTES

Definition: Given two sets A and B, the cartesian product $A \times B$ is defined by $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$. Thus it is the set of all ordered pairs of elements from A and B.

As an example, if $A = \{1, 2\},\ B = \{3, 4, 5\},$ then

$$A \times B = \{(1, 3),\ (1, 4),\ (1, 5),\ (2, 3),\ (2, 4),\ (2, 5)\}$$

Also, then $B \times A = \{(3, 1),\ (3, 2),\ (4, 1),\ (4, 2),\ (5, 1),\ (5, 2)\}$

thus $A \times B$ may not equal $B \times A$.

One can, of course, talk of $A \times A$, which we also write as A^2. Similarly, we can talk of A^3, A^4 and so on. In fact, $A^n = \{(a_1, a_2, ..., a_n) \mid a_i \in A\}$, the set of all n-tuples $(a_1, a_2, ..., a_n)$, $a_i \in A$.

Any subset of $A \times B$ is called a (binary) relation from A to B, *e.g.*,

$$R_1 = \{(1,\ 3),\ (1,\ 4),\ (1,\ 5)\}$$

$$R_2 = \{(1,\ 3)\},\ R_3 = \{(2,\ 3),\ (1,\ 5)\}$$

are all relations from A to B.

A relation from A to A is called a relation in A (or on A).

If R is a relation from A to B and $(a, b) \in R$, then we also express this fact by writing aRb and say a is R-related to b.

If R_1 is a relation from A to B and R_2 is a relation from C to D then R_1 and R_2 are said to be equal if $A = C,\ B = D$ and $aR_1b \Leftrightarrow aR_2b,\ a \in A,\ b \in B$.

Let now, A be a non empty set. A relation R in A is called

Reflexive: if $(a, a) \in R$ for all $a \in A$

Symmetric: if whenever $(a, b) \in R$ then $(b, a) \in R$

Anti-Symmetric: if $(a, b) \in R,\ (b, a) \in R \Rightarrow a = b$

Transitive: if whenever $(a, b),\ (b, c) \in R$ then $(a, c) \in R$

A relation R is called an *equivalence relation* if it is reflexive, symmetric and transitive.

A relation R on a set A is called a *partial order* relation, if it is reflexive, anti-symmetric and transitive.

Example 2: If $A = \{1, 2, 3\}$ then

$R_1 = \{(1, 1),\ (2, 2),\ (3, 3),\ (1, 3)\}$ is reflexive

$R_2 = \{(1, 1),\ (2, 2)\}$ is not reflexive

$R_3 = \{(1, 2),\ (2, 1)\}$ is symmetric but not reflexive

$R_4 = \{(1,\ 1),\ (1,\ 2)\}$ is neither reflexive nor symmetric, but is transitive.

NOTES

Example 3: Let A be the set of all lines in a plane. Let $R \subseteq A \times A$ where

$$R = \{(l, m) \mid l, m \in A, l \parallel m\}$$ then R is

Reflexive: as $(l, l) \in R$ for all $l \in A$

as $l \parallel l$ for all $l \in A$

Symmetric: as if $(l, m) \in R$ then $l \parallel m$

$\Rightarrow m \parallel l$

$\Rightarrow (m, l) \in R$

Transitive: as if $(l, m) \in R$, $(m, n) \in R$

then $l \parallel m$, $m \parallel n$

$\Rightarrow \quad l \parallel n \Rightarrow (l, n) \in R$

Thus relation of parallelism is an equivalence relation.

Equivalence Classes

Let X be a non-empty set and let $\sim$ be an equivalence relation on X. For any $a \in X$, we define equivalence class of a by

$$cl(a) = \{x \in X \mid x \sim a\}$$

i.e., equivalence class of a contains all those members of X, which are related to a under the relation $\sim$. The following theorem gives us certain important properties of equivalence classes.

Theorem 3: *Let $\sim$ be an equivalence relation on a non-empty set X. Then for any $a, b \in X$*

(*i*) $cl(a) \neq \varphi$

(*ii*) *Either* $cl(a) \cap cl(b) = \varphi$ *or* $cl(a) = cl(b)$

i.e., two equivalence classes are either equal or have no element in common.

(*iii*) $X = \bigcup_{a \in X} cl(a)$

Proof: (*i*) Since $a \sim a$, by reflexivity

$$a \in cl(a), \quad \therefore cl(a) \neq \varphi.$$

(*ii*) Let $cl(a) \cap cl(b) \neq \varphi$

Then $\exists$ some $x \in cl(a) \cap cl(b)$

$\Rightarrow x \in cl(a) \quad \& \quad x \in cl(b)$

$\Rightarrow x \sim a \quad \& \quad x \sim b$

$\Rightarrow a \sim x \quad \& \quad x \sim b$

$\Rightarrow a \sim b.$

Now if $y \in cl(a)$ be any element

then $y \sim a$ and as $a \sim b$ we find $y \sim b$

$\Rightarrow y \in cl(b)$

thus $cl(a) \subseteq cl(b)$

Similarly $cl(b) \subseteq cl(a)$

Hence $cl(a) = cl(b)$.

NOTES

(*iii*) Clearly any element $x \in X$ will be in at least one class, namely $cl(x)$ and hence is a member of $\underset{a \in X}{\cup} cl(a)$.

Again, if $t \in \underset{a \in X}{\cup} cl(a)$ then $t \in cl(x)$ for some x and as $cl(x) \subseteq X$, $t \in X$

Showing that X equals the union of all equivalence classes of X.

Definition: Let X be a non-empty set. Let K = set of non-empty subsets of X such that every two distinct members of K are disjoint, then K is called a *partition* of X, if X equals the union of all members of K.

In view of this definition, we can say that if X be a non-empty set, with an equivalence relation defined on it, then the set of all equivalence classes of X partitions the set X.

1.3 MAPPING

Let A and B be two non-empty sets. A relation f from A to B is called a mapping (or a map or a function) from A to B if for each $a \in A$, $\exists$ a unique $b \in B$ s.t., $(a, b) \in f$(and in that case we write $b = f(a)$ and b is called *image* of a under f and a is called *pre-image* of b under f). We express this by writing $f : A \to B$.

Thus mapping is that relation from A to B in which each member of A is related to some member of B and no member of A is related to more than one member of B, although more than one member of A can be related to the same member of B. A is called the *domain* of f and B is called the *co-domain* of f. A mapping $f : A \to A$ is also sometimes called a *transformation* of the set A.

The subset of B which contains only those members which have pre images in A is called *range* of f.

One can, of course, have more than one mapping from A to B.

A mapping $f : A \to B$ is called *one–one* (1–1) *or injective* mapping, if

$$f(x) = f(y) \Rightarrow x = y$$

or if $$x \neq y \Rightarrow f(x) \neq f(y)$$

Thus under one–one mapping all members of A are related to different members of B.

A mapping $f : A \to B$ is called *onto* or *surjective* mapping, if range of f equals B, *i.e.*, each member of B has a preimage under f.

NOTES

A map which is both 1–1 and onto is sometimes referred to as a one-to-one correspondence or a *bijective* map.

To check whether a map $f: A \to B$ is well defined or not, we need verify that $x = y \Rightarrow f(x) = f(y)$.

Example 4: Let **N** = set of natural numbers. Define a map $f: \mathbf{N} \to \mathbf{N}$ s.t., each $a \in \mathbf{N}$ is connected to its square. Since each natural number has a unique square in **N** itself, we find *f* will be a well-defined mapping. We express this by writing

$$f: \mathbf{N} \to \mathbf{N}, \text{ s.t.,}$$
$$f(x) = x^2 \quad \text{for all } x \in \mathbf{N}$$

We notice that in the notation of our definition

$$f = \{(1, 1), (2, 4), (3, 9), (4, 16), ...\}$$
$$= \{(x, x^2) \mid x \in \mathbf{N}\}$$

Example 5: For any set *A*, the mapping $f: A \to A$, s.t.,

$$f(x) = x \quad \text{for all } x \in A$$

is called the *identity* map. It is trivially a well defined one-one map. It is also onto.

Example 6: If **Z** = set of integers, then the map $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 2x$$

is 1–1 but not onto. $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$

But $1 \in \mathbf{Z}$ has no pre image.

Example 7: The map $f: \mathbf{N} \to \{1\}$, s.t.,

$$f(x) = 1 \quad \text{for all } x \in \mathbf{N}$$

where **N** = set of naturals is onto map but not 1–1.

Equality of Mappings

Two mappings *f* and *g* from *A* to *B should* be equal if they 'behave' exactly in the same way. We formalise this in

Theorem 4: *Two maps* $f: A \to B$ *and* $g: A \to B$ *are equal if* $f(x) = g(x)$ *for all* $x \in A$.

Proof: Let $f = g$.

Let $a \in A$ be any element and let $f(a) = b$.

then $(a, b) \in f \Rightarrow (a, b) \in g$

$$\Rightarrow b = g(a)$$

or that $f(x) = g(x)$ for all x.

Conversely, let $f(a) = g(a)$ for all $a \in A$

Let $x \in f$ be any element, then $x = (a, f(a))$ for some $a \in A$.

NOTES

Since $f(a) = g(a), \quad x = (a, g(a)) \in g$

i.e., $x \in f \Rightarrow x \in g$

or that $f \subseteq g$

Similarly, $g \subseteq f$

and hence $f = g$.

Definition: Let $f : A \to B$ be a mapping and suppose C and D are subsets of A and B respectively, s.t., $f(x) \in D$ for all $x \in C$. We say f induces the map $g : C \to D$ where $g(x) = f(x)$ for all $x \in C$ and in that case g is called a *restriction* of f.

Composition of Mappings

Let $f : A \to B$ and $g : B \to C$ be two mappings.

We define a mapping (to be denoted by *gof*) from A to C by the rule

$$gof(x) = g(f(x)) \quad \text{for all } x \in A$$

That it is well defined is confirmed by the fact that

$$x = y$$
$$\Rightarrow f(x) = f(y)$$
$$\Rightarrow g(f(x)) = g(f(y))$$
$$\Rightarrow (gof)x = (gof)y$$

One can, of course, extend this idea to more than two mappings.

Remark: *gof* is also denoted by *gf*.

Theorem 5: *If* $f : A \to B$ and $g : B \to C$ *are one-one* (*onto*) *mappings then so is gof.*

Proof: Let f and g be one-one

Since $(gof)\, x = (gof)\, y$

$$\Rightarrow g(f(x)) = g(f(y))$$
$$\Rightarrow f(x) = f(y) \qquad [\text{as } g \text{ is } 1-1]$$
$$\Rightarrow x = y \qquad [\text{as } f \text{ is } 1-1]$$

We find *gof* is one-one.

Again, if f, g are onto, and $c \in C$ be any element, then $\exists\, b \in B$ s.t., $g(b) = c$
(g being onto). Again, for this $b \in B$, $\exists$ some $a \in A$ s.t.,

$f(a) = b$ as f is onto

Now $(gof)\, a = g(f(a)) = g(b) = c$

Hence *gof* is onto.

The converse of the above theorem does not hold (see exercises).

NOTES

Theorem 6: *A map f is invertible iff it is one-one onto.*

Remark: If g is a mapping such that gof is identity map, then g is called left inverse of f. Similarly, one can define right inverse of f.

If $f : X \to X$ has both right and left inverses then it is easily seen that the two are equal.

Problem 1: *Let X be a non empty set. Show that* $f : X \to X$ *is one-one iff f has a left inverse.*

Solution: Suppose f is one-one.

Let $x_0 \in X$ be any fixed element

Define $g : X \to X$, s.t.,

$g(x) = y$ if $\exists\ y \in X$ s.t., $f(y) = x$

$= x_0$ otherwise.

Suppose $g(x) = y$ and $g(x) = y'$, then $f(y) = x$ and $f(y') = x$, *i.e.,* $f(y) = f(y')$ $\Rightarrow y = y'$ as f is 1–1 and so y is uniquely determined. Thus $g: X \to X$ is well defined mapping.

Since $gof(y) = g(f(y)) = g(x) = y$, $\forall\ y \in X$, g is left inverse of f.

Conversely, let g be a left inverse of f

Let $f(x_1) = f(x_2)$

Then $x_1 = (gof)x_1 = g(f(x_1)) = g(f(x_2)) = (gof)x_2 = x_2$ or that f is 1–1.

Remark: One can show that f is onto iff it has a right inverse.

Definition: Let $f : A \to B$ be a function. Let $X \subseteq A$ then we define $f(X) = \{f(x) \mid x \in X\}$, which is, of course, a subset of B, it is called image of X.

Again, if $Y \subseteq B$ then $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, which is a subset of A. (f^{-1} here is only a notation and not essentially the inverse function). It is called pre-image of Y.

Theorem 7: *Let* $f : X \to Y$ *be a function then*

(*i*) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$

(*ii*) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

(*iii*) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

(*iv*) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

(*v*) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

(*vi*) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$

where A_1, A_2 *are subsets of X and* B_1, B_2 *are subsets of Y.*

Proof: We leave it for the reader to try.

Theorem 8: *If* $f : A \to B$, $g : B \to C$, $h : C \to D$ *be maps then*

(*i*) $ho(gof) = (hog)of$

(*ii*) *If* $i : A \to A$, $j : B \to B$ *be identity maps then* $foi = f$ *and* $jof = f$

Proof: (*i*) $ho(gof)$ and $(hog)of$ are both maps from $A \to D$

Since for any $x \in A$

$[(hog)of]\ x = (hog)(f(x)) = h\ (gf(x)))$

$[ho(gof)]\ x = h(gof)x) = h\ (g(f(x)))$

$h((gof)x) = (ho(gof))x$

we get result (*i*).

(*ii*) Since foi and f are both maps from $A \to B$ and also for any $x \in A$

$(foi)x = f(i(x)) = f(x)$, we find $foi = f$

Again, jof and f are maps from $A \to B$ and for any $x \in A$

$(jof)x = j(f(x)) = f(x)$

$\Rightarrow jof = f$

Cor.: If $f : A \to A$ be any mapping and $i : A \to A$ be identity map, then $foi = iof = f$.

1.4 THE INTEGERS - PROBLEMS

In this section we discuss a few results pertaining to numbers although we do not plan to go through their axiomatic construction.

Definition: A non zero integer a is said to divide an integer b if $b = ac$ for some integer c and we express it as $a \mid b$.

The following results can then be proved

(*i*) $a \mid b,\ b \mid c$ then $a \mid c$

(*ii*) $a \mid b,\ a \mid c$ then $a \mid b + c$

(*iii*) $a \mid 0,\ a \mid a$

We now prove a well known result through

Theorem 9: (Euclid's Algorithm)

Let $k > 0$ *be an integer and j be any integer. Then* $\exists$ *unique integers q and r such that* $j = kq + r$, *where* $0 \le r < k$.

Proof: Let $S = \{j - kq \mid q$ is an integer, $j - kq \ge 0\}$.

Then $S \neq \varphi$, as take $q = -|j|$.

Now when $j > 0$, then $j - kq = j + kj > 0 \Rightarrow j - kq \in S$

and if $j < 0$, then $j - kq = j - kj$

$= j\ (1 - k) \ge 0$

$\Rightarrow j - kq \in S$

NOTES

$j = 0$, then $j - kq = j - k.0$

$= j = 0$

$\Rightarrow j - kq \in S$

NOTES

In any case, $S \neq \varphi$.

By well ordering principle, S has least element, say $r \in S$.

$r \in S \Rightarrow r = j - kq$ for some integer q

$\Rightarrow j = kq + r$. Also $r \geq 0$

Suppose $r \geq k$

Then $j - kq \geq k$

$\Rightarrow j - k(q + 1) \geq 0$

$\Rightarrow j - k(q + 1) \in S$

But $j - k(q + 1) < j - kq$ as $k > 0$, contradicting $r = j - kq$ is least element of S.

$\therefore 0 \leq r < k$.

Uniqueness: Suppose $j = kq + r = kq' + r'$, $0 \leq r, r' < k$. Then $k(q - q') = r' - r$. Suppose $r' > r$. Then $r' - r > 0$. But $k \mid r' - r \Rightarrow k \leq r' - r$. Since $r, r' < k$, $r' - r < k$, a contradiction.

$\therefore r' \not> r$. Similarly $r \not> r'$ $\therefore r = r' \Rightarrow kq = kq' \Rightarrow q = q'$.

An important application of this result is the *basis representation theorem*.

Theorem 10: (Basis Representation Theorem).

Let $b > 0$ be an integer and let $N > 1$ be any integer. Then N can be expressed as

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b + a_0,$$

where m and a_is are integers such that $m > 0$ and $0 \leq a_i < b$. Also then these a_is are uniquely determined. (*b is called base of representation of N*).

Proof: If $N < b$,

then $N = 0b^m + 0b^{m-1} + \ldots + 0b + N$

is the representation of N as required.

Let $N \geq b > 0$. By Euclid's algorithm $\exists$ integers q, r such that

$N = bq + r$, $0 \leq r < b \leq N$

Since $N - r > 0$, $bq > 0 \Rightarrow q > 0$ as $b > 0$.

If $q < b$, then $N = bq + r$ is the required representation of n.

If $q \geq b > 0$, then as above by Euclid's algorithm $\exists$ integers q_1, r_1 such that

$q = bq_1 + r_1$, $0 \leq r_1 < b \leq q$

Since $q - r_1 > 0$, $bq_1 > 0 \Rightarrow q_1 > 0$ as $b > 0$.

Now $N = bq + r = b(bq_1 + r_1) + r$

$\Rightarrow N = b^2q_1 + br_1 + r$

If $q_1 < b$, then it is the required representation of N. In this way, after finite number of steps, we shall get

$$N = a_m b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0$$

where $a_i's$ are integers such that

$$0 \le a_i < b \quad \text{for all } i = 1,\ldots, m.$$

Uniqueness of $a_i s$ follows as:

Suppose $N = c_m b^m + c_{m-1} b^{m-1} + \ldots + c_1 b + c_0$ where each c_i is an integer such that $0 \le c_i < b$. We can choose same m in both the representations of N because if one representation of N has lesser terms we can always insert zero coefficients and thus make the number of terms to be same.

$\therefore \quad 0 = (a_m - c_m)b^m + \ldots + (a_1 - c_1)b + (a_0 - c_0)$

Let $a_i - c_i = d_i$.

Then $d_m b^m + \ldots + d_1 b + d_0 = 0$.

We have to show that $d_i = 0$ for all i.

Suppose for some i, $d_i \neq 0$. Let k be the least subscript such that $d_k \neq 0$

Then $d_k b^k + d_{k+1}b^{k+1} + \ldots + d_m b^m = 0$

$\Rightarrow d_k b^k = -(d_{k+1}b^{k+1} + \ldots + d_m b^m)$

$\Rightarrow d_k = -(d_{k+1}b + d_{k+2}b^2 + \ldots + d_m b^{m-k})$

$\Rightarrow d_k = -b(d_{k+1} + d_{k+2}b + \ldots + d_m b^{m-k-1})$

$\Rightarrow b \mid d_k$

$\Rightarrow b \mid \mid d_k \mid$

$\Rightarrow b \le \mid d_k \mid$

But $a_k, c_k < b \Rightarrow \mid a_k - c_k \mid < b$

$\Rightarrow \mid d_k \mid < b,$

So, we get a contradiction

$\therefore \quad d_i = 0$ for all $i = 1,\ldots, m$

$\therefore \quad a_i = c_i$ for all $i = 1,\ldots, m$

Note: When the integer N is expressed as

$$N = a_m b^m + \ldots + a_1 b + a_0, \quad 0 \le a_i < b,$$

we write $N = (a_m\, a_{m-1} \ldots a_1 a_0)b$

and say that N is $a_m a_{m-1} \ldots a_0$ to the base b.

For example,

$132 = 1.10^2 + 3.10 + 2$ (Here base is 10)

NOTES

NOTES

Then as above

$$132 = (132)_{10}$$

So, numbers that we usually write are to the base 10.

Again, if we want to write 132 to the base 2, we first write

$1\ 3\ 2 = 2^7 + 2^2 = 2^7 + 0.2^6 + 0.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 0.2 + 0$

and by basis representation theorem, then

$$132 = (10000100)_2$$

Problem 11: *If a, b are integers with $b \neq 0$, show that there exist unique integers q and r satisfying $a = bq + r$ where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$.*

Solution: By Euclid's algorithm, there exist unique integers q', r' such that

$$a = q'|b| + r', \quad \text{where } 0 \leq r' < |b|$$

(as $|b| > 0$ when $b \neq 0$).

Case 1: $0 \leq r' \leq \frac{1}{2}|b|$

Take $r' = r,\ q' = q$ (if $b > 0$), $q' = -q$ (if $b < 0$)

Since $-\frac{1}{2}|b| < 0 \leq r' = r \leq \frac{1}{2}|b|$,

$$-\tfrac{1}{2}|b| < r \leq \tfrac{1}{2}|b|$$

Also $a = q'|b| + r'$ becomes

$a = qb + r$ if $b > 0$

and $a = (-q)(-b) + r$ if $b < 0$

$= qb + r$

where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$

Case 2: $\frac{1}{2}|b| < r' < |b|$

Take $r' = r + |b|$

$q' = q - 1$ if $b > 0$

$= -q - 1$ if $b < 0$

Now $\frac{1}{2}|b| < r' = r + |b|$

$\Rightarrow -\frac{1}{2}|b| < r$

Also $r' = r + |b| < |b|$

$\Rightarrow r < 0 < \frac{1}{2}|b|$

$\therefore \quad -\frac{1}{2}|b| < r < \frac{1}{2}|b|$

Again $a = |b|\ q' + r'$ becomes

$a = b(q - 1) + r + b$ when $b > 0$

$= bq + r$

Also, when $b > 0$, $a = |b|q' + r'$ becomes

$a = -b\ (-q - 1) + r - b$

$= bq + r$

where $-\frac{1}{2}|b| < r < \frac{1}{2}|b|$.

NOTES

The Greatest Common Divisor

A special case in Euclid's algorithm arises when the remainder is zero. We discuss it in this section.

Definition: An integer $d > 0$ is called greatest common divisor (g.c.d.) of two integers a, b (non zero) if

(*i*) $d \mid a,\ d \mid b$

(*ii*) If $c \mid a,\ c \mid b$ then $c \mid d$

We write d = g.c.d.$(a,\ b)$ or simply $d = (a,\ b)$.

Remarks:

(*i*) $(a,\ 0) = |a|,\ (0,\ b) = |b|$

Clearly, $|a| \mid a,\ |a| \mid 0$

If $c \mid a$, then $c \mid |a| \Rightarrow (a, 0) = |a|$

Similarly $(0,\ b) = |b|$

(*ii*) If $a \mid b$, then $(a,\ b) = |a|$

$|a| \mid a$, and $a \mid b \Rightarrow |a| \mid b$

If $c \mid a,\ c \mid b$, then $c \mid |a|$

$\therefore\ (a,\ b) = |a|$

(*iii*) g.c.d. of a and b does not depend on signs of a and b

i.e., $(a,\ b) = (-a,\ b) = (a, -b) = (-a, -b)$

Let $d = (a,\ b)$. Then $d \mid a,\ d \mid b \Rightarrow d \mid -a,\ d \mid b$

$c \mid -a,\ c \mid b \Rightarrow c \mid a,\ c \mid b \Rightarrow c \mid d$

$\therefore\ d = (-a,\ b)$. Similarly for others.

We now show the existence and uniqueness of g.c.d. of integers a and b.

Theorem 11: *Let a, b be two integers. Suppose either $a \neq 0$ or $b \neq 0$. Then $\exists$ greatest common divisor d of a, b such that*

$$d = ax + by \text{ for some integers } x, y.$$

d is uniquely determined by a and b.

NOTES

Proof: Let $S = \{au + bv \mid u, v \text{ are integers and } au + bv > 0\}$.

If $a > 0$, then $a = a.1 + b.0 > 0 \Rightarrow a \in S$.

If $a < 0$, then $-a = a(-1) + b.0 > 0 \Rightarrow -a \in S$.

Similarly, if $b > 0$ then $b \in S$ and if $b < 0$ then $-b \in S$. Since one of a and b is non zero, either $\pm a \in S$ or $\pm b \in S$. In any case $S \neq \varphi$.

By well ordering principle S has a least element, say d.

Now $d \in S \Rightarrow d = ax + by$ for some integers x and y. Also $d > 0$.

Let $a = dq + r$, $0 \leq r < d$.

Let $r \neq 0$. Since $r = a - dq$

$$= a - (ax + by)q$$

$$= a(1 - xq) + b(-yq) > 0$$

$$\Rightarrow r \in S.$$

But $r < d$, contradicting the fact that d is least element of S. So, $r = 0$.

Therefore, $a = dq \Rightarrow d \mid a$.

Similarly, $d \mid b$.

Suppose, $c \mid a,\ c \mid b \Rightarrow c \mid ax + by = d$.

So, d is a greatest common divisor of a and b.

If d' is also greatest common divisor of a and b, then $d' \mid a$, $d' \mid b$, $\Rightarrow d \mid d'$ Similarly, $d \mid a, d \mid b \Rightarrow d' \mid d$. Since $d, d' > 0$, $d = d'$. So d is uniquely determined by a and b.

Definition: If g.c.d.$(a, b) = 1$, then a and b are said to be *relatively prime* or *coprime.*

Cor: Two integers a, b are relatively prime if and only if $\exists$ integers x, y such that $ax + by = 1$.

Proof: Suppose a, b are relatively prime. Then g.c.d.$(a, b) = 1$. By above theorem $\exists$ integers x, y such that $ax + by = 1$.

Conversely, let $ax + by = 1$ for some integers x, y. Let d = g.c.d.(a, b). Then $d \mid a, d \mid b \Rightarrow d \mid ax, d \mid by \Rightarrow d \mid ax + by = 1 \Rightarrow d = 1$.

So, a, b are relatively prime.

Definition: The *least common multiple* of two non zero integers a and b, denoted by l.c.m.(a, b) is the positive integer m s.t.,

(*i*) $a \mid m,\ b \mid m$

(*ii*) if $a \mid c,\ b \mid c$, with $c > 0$, then $m \mid c$.

Theorem 12: *For positive integers a and b*

$$\text{g.c.d.}(a, b) \times \text{l.c.m.}(a, b) = ab$$

Proof: Let d = g.c.d.(a, b)

Now $\frac{ab}{d} = a.\frac{b}{d} \Rightarrow a \left| \frac{ab}{d} \right.$ as $\frac{b}{d}$ is integer

Also $\frac{ab}{d} = b.\frac{a}{d} \Rightarrow b \left| \frac{ab}{d} \right.$ as $\frac{a}{d}$ is integer

Let $m = \frac{ab}{d}$, then $a \mid m$ and $b \mid m$

Suppose now $a \mid c$, $b \mid c$. Since $(a, b) = d$, $\exists$ integers x, y s.t., $d = ax + by$.

$$\therefore \quad \frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = \text{integer}$$

$$\Rightarrow m \mid c.$$

Thus m = l.c.m. (a, b), *i.e.*, $\frac{ab}{d}$ = l.c.m. (a, b)

or that ab = g.c.d. $(a, b) \times$ l.c.m. (a, b).

Problem 2: *Let* g.c.d. $(a, b) = 1$.

Show that g.c.d.$(a + b, a^2 - ab + b^2) = 1$ *or* 3.

Solution: Let g.c.d.$(a + b, a^2 - ab + b^2) = d$

Then $d \mid a + b$, $d \mid a^2 - ab + b^2$

$\Rightarrow d \mid (a + b)^2 = a^2 + b^2 + 2ab$, $d \mid a^2 - ab + b^2$

$\Rightarrow d \mid 3ab$

Let g.c.d.$(d, a) = e$

Then $e \mid d \mid a + b \Rightarrow e \mid a + b$ and $e \mid a$

$\therefore$ $e \mid (a + b) - a = b$

So, $e \mid$ g.c.d.$(a, b) = 1 \Rightarrow e = 1$

$\therefore$ g.c.d.$(d, a) = 1$

Similarly, g.c.d.$(d, b) = 1$

$\therefore$ $d \mid 3 \Rightarrow d = 1$ or 3.

Prime Numbers

An integer $p > 1$ is called a *prime number* if 1 and p are the only divisors of p.

Theorem 13: *If a prime number p divides ab, then either p divides a or p divides b.*

Proof: Let $ab = pc$ for some integer c.

Suppose p does not divide a.

Then g.c.d.$(a, p) = 1$

NOTES

$\therefore \quad p \mid ab$ and g.c.d.$(a, p) = 1$

$\Rightarrow p \mid b$

Composite Numbers

NOTES

A composite number is an integer $n > 1$ such that n is not prime.

Problem 3: *Prove that if* $2^n - 1$ *is prime, then n is prime.*

Solution: Let $2^n - 1 = p$ = prime.

Let n be not prime.

Then $n = rs$, $1 < r, s < n$

$$\therefore \quad p = 2^n - 1$$
$$= 2^{rs} - 1 = (2^r)^s - 1$$
$$= x^s - 1, \; x = 2^r > 2 \text{ as } r > 1$$
$$= (x - 1)(x^{s-1} + x^{s-2} + \ldots + x + 1)$$

Either $x - 1 = 1$ or $x^{s-1} + \ldots + x + 1 = 1$

$x - 1 = 1 \Rightarrow x = 2$, which is not true

and $x^{S-1} + \ldots + x + 1 = 1$

$\Rightarrow x^{s-1} + \ldots + x = 0$, which is not true

$\therefore \quad n$ is prime.

Congruences

Let $a, b, c, (c > 0)$ be integers. We say a is congruent to b modulo c if c divides $a - b$ and we write this as $a \equiv b \pmod{c}$. This relation '$\equiv$' on the set of integers is an equivalence relation as seen earlier.

Addition, subtraction and multiplication in congruences behave naturally.

Let $a \equiv b \pmod{c}$

$a_1 \equiv b_1 \pmod{c} \Rightarrow c \mid a - b, \; c \mid a_1 - b_1$

$\Rightarrow c \mid (a + a_1) - (b + b_1)$

$\Rightarrow a + a_1 \equiv b + b_1 \pmod{c}$

Similarly $a - a_1 \equiv b - b_1 \pmod{c}$

Also $c \mid a - b, \; c \mid a_1 - b_1$

$\Rightarrow c \mid aa_1 - ba_1, \; c \mid ba_1 - bb_1$

$\Rightarrow c \mid (aa_1 - ba_1) + (ba_1 - bb_1)$

$\Rightarrow c \mid aa_1 - bb_1$

$\Rightarrow aa_1 \equiv bb_1 \pmod{c}$

We may, however, not be able to achieve the above result in case of division.

Indeed $\frac{a}{a_1}$ or $\frac{b}{b_1}$ may not even be integers.

Again, cancellation in congruences in general may not hold.

i.e., $ad \equiv bd \pmod{c}$ need not essentially imply

$a \equiv b \pmod{c}$

For example, $2.2 \equiv 2.1 \pmod{2}$

but $2 \not\equiv 1 \pmod{2}$

However, cancellation holds if g.c.d.$(d, c) = 1$.

i.e., if $ad \not\equiv bd \pmod{c}$

and g.c.d.$(d, c) = 1$

then $a \equiv b \pmod{c}$.

Proof: $ad \equiv bd \pmod{c}$

$\Rightarrow c \mid ad - bd$

$\Rightarrow c \mid d\,(a - b)$

$\Rightarrow c \mid a - b$ as g.c.d.$(c, d) = 1$

$\Rightarrow a \equiv b \pmod{c}$.

Problem 4: *If* $a \equiv b$ (*mod* n), *prove that* g.c.d.$(a, n) =$ g.c.d.(b, n).

Solution: Let d = g.c.d.(a, n)

Then $d \mid a,\ d \mid n$. But $n \mid a - b$

$\therefore$ $d \mid a - b,\ d \mid a$

$\Rightarrow d \mid a - (a - b) = b$

$\therefore$ $d \mid b,\ d \mid n$

Let $c \mid b,\ c \mid n \quad \Rightarrow c \mid b,\ c \mid a - b$ as $n \mid a - b$

$\Rightarrow c \mid a - b + b = a$

$\Rightarrow c \mid a,\ c \mid n$

$\Rightarrow c \mid d$ as d = g.c.d.$(a,\ n)$

$\Rightarrow$ g.c.d.$(b,\ n) = d$

Problem 5: *Find the remainder obtained by dividing* $1! + 2! + 3! + 4! + \ldots + 100!$ *by* 12.

Solution: Each number 4! onwards is a multiple of 12.

$\therefore\ 1! + 2! + 3! + 4! + \ldots + 100! \equiv 1! + 2! + 3! + 0 + \ldots + 0 \pmod{12}$

$\Rightarrow\ 1! + 2! + 3! + 4! + \ldots + 100! \equiv 9 \pmod{12}$

$\Rightarrow$ 9 is the required remainder.

NOTES

NOTES

Check Your Progress

1. What is an empty set?
2. What is an equivalence relation?
3. What is injective mapping?
4. State Euclid's theorem.

1.5 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. A set having no element is called an empty set or a null set or a void set.
2. A relation R is called an equivalence relation if it is reflexive, symmetric and transitive.
3. A mapping $f: A \to B$ is called *one–one* (1–1) *or* injective mapping, if $f(x) = f(y) \Rightarrow x = y$
4. Let $k > 0$ be an integer and j be any integer. Then $\exists$ unique integers q and r such that $j = kq + r$, where $0 \leq r < k$.

1.6 SUMMARY

- If x is an element (member) of a set A we say x belongs to A and express it as $x \in A$. If y is not a member of A we say y does not belong to A and write $y \notin A$.
- Two sets A and B are said to be equal if they contain precisely the same elements and we write $A = B$.
- If A is the set containing 1, 2, 3, 4, 5, 6, we can write it as $A = \{1, 2, 3, 4, 5, 6\}$
- A set having no element is called an empty set or a null set or a void set.
- A set will be called finite if either it is empty or has finite number of elements. A set with infinite number of elements is referred to as an infinite set.
- *o(S)* or $|S|$ denotes the number of elements in the set S and read it as order of S (sometimes also called its cardinality).
- If every element of A is in B *then* A is a subset of B and B is called superset of A.
- U*nion* of two sets A and B, set $A \cup B$ which contains all the elements of A as well as B.
- I*ntersection* of two sets A and B, set $A \cap B$ which contains all the elements of A and B.

NOTES

- Relation is the set of all ordered pairs of elements from set A and set B.
- A relation R is called an equivalence relation if it is reflexive, symmetric and transitive.
- Mapping is that relation from A to B in which each member of A is related to some member of B and no member of A is related to more than one member of B, although more than one member of A can be related to the same member of B. A is called the domain of f and B is called the co-domain of f.
- If $k > 0$ be an integer and j be any integer. Then $\exists$ unique integers q and r such that $j = kq + r$, where $0 \leq r < k$.
- d = g.c.d.(a, b), d is greatest common divisor.
- An integer $p > 1$ is called a prime number if 1 and p are the only divisors of p.
- A composite number is an integer n > 1 such that n is not prime.
- Let $a, b, c, (c > 0)$ be integers. We say a is congruent to b modulo c if c divides $a - b$ and we write this as $a \equiv b \ (mod\ c)$. This relation '≡' on the set of integers is an equivalence relation.

1.7 KEY WORDS

- **Cardinality**: The number of elements in a set or other grouping, as a property of that grouping.
- **Equivalence**: The condition of being equal or equivalent in value, worth, function, etc.
- **Domain**: The set of possible values of the independent variable or variables of a function.
- **Co-domain**: The codomain of a function is the set Y into which all of the output of the function is constrained to fall. It is the set Y in the notation $f: X \to Y$. The codomain is also sometimes referred to as the range.

1.8 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. If A, B, C are sets, then show that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2. Define Relations.
3. For sets A, B in a set X, show that

   $X - (A \cup B) = (X - A) \cap (X - B)$ *or* $(A \cup B)' = A' \cap B'$
4. Define equivalence classes.

NOTES

Long Answer Questions

1. Show that the relation of equality on integers is an equivalence relation.
2. Let X be a non-empty set. Show that $f: X \to X$ is one-one iff f has a left inverse.
3. Prove that if $2^n - 1$ is prime, then n is prime.
4. Prove Basis Representation Theorem.

1.9 FURTHER READINGS

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Dasgupta, Abhijit. 2013. *Set Theory: With an Introduction to Real Point Sets*. Berlin: Springer Science & Business Media.

UNIT 2 GROUP THEORY

NOTES

Structure

2.0 INTRODUCTION

In this unit, you will study different algebraic structures or algebraic compositions, which means a non-empty set with one or more binary compositions. The unit starts with groups which occupy a very important seat in the study of abstracts of algebra.

2.1 OBJECTIVES

After going through this unit, you will be able to:

- Define a Group
- Discuss some examples of Groups
- Learn preliminary lemmas
- Know about Subgroups

2.2 DEFINITION OF A GROUP

Definition: A non empty set G, together with a binary composition * (star) is said to form a group, if it satisfies the following postulates

(*i*) *Associativity*: $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$

(*ii*) *Existence of Identity*: $\exists$ an element $e \in G$, s.t.,

$$a * e = e * a = a \quad \text{for all } a \in G$$

(e is then called *identity*)

NOTES

(*iii*) *Existence of Inverse*: For every $a \in G, \exists\ a' \in G$ (depending upon a) s.t.,

$$a * a' = a' * a = e$$

(a' is then called inverse of a)

Remarks: (*i*) Since * is a binary composition on G, it is understood that for all $a, b \in G$, $a * b$ is a unique member of G. This property is called *closure property*.

(*ii*) If, in addition to the above postulates, G also satisfies the *commutative law*

$$a * b = b * a \quad \text{for all } a, b \in G$$

then G is called an *abelian group* or *a commutative group*.

(*iii*) Generally, the binary composition for a group is denoted by '.' (dot) which is so convenient to write (and makes the axioms look so natural too).

If the set G is finite (i.e., has finite number of elements) it is called a *finite group* otherwise, it is called an *infinite group*.

We shall always (unless stated otherwise) use the symbols e for identity of a group and a^{-1} for inverse of element a of the group.

Definition: By order of a group, we will mean the number of elements in the group and shall denote it by $o(G)$ or $|\ G\ |$.

2.3 SOME EXAMPLES OF GROUPS

Example 1: The set **Z** of integers forms an abelian group w.r.t. the usual addition of integers.

It is easy to verify the postulates in the definition of a group as sum of two integers is a unique integer (thus closure holds). Associativity of addition is known to us. 0 (zero) will be identity and negatives will be the respective inverse elements. Commutativity again being obvious.

Example 2: One can easily check, as in the previous example, that sets **Q** of rationals, **R** of real numbers would also form abelian groups w.r.t. addition.

Example 3: Set of integers, w.r.t. usual multiplication does not form a group, although closure, associativity, identity conditions hold.

Note 2 has no inverse w.r.t. multiplication as there does not exist any integer a s.t., $2.a = a.2 = 1$.

Example 4: The set G of all +ve irrational numbers together with 1 under multiplication does not form a group as closure does not hold. Indeed $\sqrt{3}\ .\ \sqrt{3} = 3 \notin G$, although one would notice that other conditions in the definition of a group are satisfied here.

NOTES

Example 5: Let G be the set $\{1, -1\}$. Then it forms an abelian group under multiplication. It is again easy to check the properties.

1 would be identity and each element is its own inverse.

Example 6: Set of all 2×2 matrices over integers under matrix addition would be another example of an abelian group.

Example 7: Set of all non zero complex numbers forms a group under multiplication defined by

$$(a + ib)\ (c + id) = (ac - bd) + i\ (ad + bc)$$

$1 = 1 + i.0$ will be identity,

$\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}$ will be inverse of $a + ib$.

Note $a + ib$ non zero means that not both a & b are zero.

Thus $a^2 + b^2 \neq 0$.

Example 8: Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

then G forms a group. G is not abelian as $ij \neq ji$.

This is called the ***Quaternion Group***.

Example 9: Let $G = \{(a, b) \mid a, b$ rationals, $a \neq 0\}$. Define * on G by

$$(a, b) * (c, d) = (ac, ad + b)$$

Closure follows as $a, c \neq 0 \Rightarrow ac \neq 0$

$$[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f)$$
$$= (ace, acf + ad + b)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d)$$
$$= (ace, acf + ad + b)$$

proves associativity.

$(1, 0)$ will be identity and $(1/a, -b/a)$ will be inverse of any element (a, b).

G is not abelian as

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$
$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

Example 10 (a): The set G of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over reals, where $ad - bc \neq 0$, i.e., with non zero determinant forms a non abelian group under matrix multiplication.

NOTES

It is called the **general linear group** of 2×2 matrices over reals and is denoted by $GL(2, \mathbf{R})$.

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will act as identity and

the matrix $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ will be inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

one can generalise and prove

(b) If G be the set of all $n \times n$ invertible matrices over reals, then G forms a group under matrix multiplication.

(c) The set of 2×2 matrices over **R** with determinant value 1 forms a non abelian group under matrix multiplication and is called the **special linear group**, denoted by $SL(2, \mathbf{R})$.

One can take any field (e.g., **Q**, **C** or $\mathbf{Z}_p$) in place of **R** in the above examples.

Example 11: *Group of Residues* : Let $G = \{0, 1, 2, 3, 4\}$. Define a composition $\oplus_5$ on G by $a \oplus_5 b = c$ where c is the least non –ve integer obtained as remainder when $a + b$ is divided by 5. For example. $3 \oplus_5 4 = 2$, $3 \oplus_5 1 = 4$, etc. Then $\oplus_5$ is a binary composition on G (called addition modulo 5). It is easy to verify that G forms a group under this.

One can generalise this result to

$$G = \{0, 1, 2, ..., n - 1\}$$

under addition modulo n where n is any positive integer.

We thus notice

$$a \oplus_n b = \begin{cases} a + b & \text{if } a + b < n \\ a + b - n & \text{if } a + b \geq n \end{cases}$$

Also, in case there is no scope of confusion we drop the sub suffix n and simply write $\oplus$. This group is generally denoted by $\mathbf{Z}_n$.

Example 12: Let $G = \{x \in \mathbf{Z} \mid 1 \leq x < n, x, n \text{ being co-prime}\}$ where **Z** = set of integers and x, n being co-prime means H.C.F of x and n is 1.

NOTES

We define a binary composition $\otimes$ on G by $a \otimes b = c$ where c is the least +ve remainder obtained when $a \,.\, b$ is divided by n. This composition $\otimes$ is called multiplication modulo n.

We show G forms a group under $\otimes$.

Closure: For $a, b \in G$, let $a \otimes b = c$. Then $c \neq 0$, because otherwise $n \mid ab$ which is not possible as a, n and b, n are co-prime.

Thus $c \neq 0$ and also then $1 \leq c < n$.

Now if c, n are not co-prime then $\exists$ some prime no. p s.t., $p|c$ and $p|n$.

Again as $ab = nq + c$ for some q

We get $p|ab$ $\quad [p|n \Rightarrow p|nq, p|c \Rightarrow p|nq + c]$

$\Rightarrow p|a$ or $p|b$ (as p is prime)

If $p|a$ then as $p|n$ it means a, n are not co-prime.

But a, n are co-prime.

Similarly $p|b$ leads to a contradiction.

Hence c, n are co-prime and thus $c \in G$, showing that closure holds.

Associativity: Let $a, b, c \in G$ be any elements.

Let $a \otimes b = r_1$, $(a \otimes b) \otimes c = r_1 \otimes c = r_2$

then r_2 is given by $r_1 c = nq_2 + r_2$

Also $a \otimes b = r_1$ means

$$ab = q_1 n + r_1$$

thus $$ab - q_1 n = r_1$$

$$\Rightarrow (ab - q_1 n)c = r_1 c = nq_2 + r_2$$

$$\Rightarrow (ab)c = r_2 + nq_2 + nq_1 c = n(q_1 c + q_2) + r_2$$

or that r_2 is the least non-negative remainder got by dividing $(ab)c$ by n.

Similarly, if $a \otimes (b \otimes c) = r_3$ then we can show that r_3 is the least non –ve remainder got by dividing $a(bc)$ by n.

But since $a(bc) = (ab)c$, $r_2 = r_3$

Hence $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.

Existence of Identity: It is easy to see that

$$a \otimes 1 = 1 \otimes a = a \quad \text{for all } a \in G$$

or that 1 will act as identity.

Existence of Inverse: Let $a \in G$ be any element then a and n are co-prime and thus we can find integers x and y s.t., $ax + ny = 1$

By division algorithm, we can write

$$x = qn + r, \quad \text{where } 0 \leq r < n$$

$$\Rightarrow ax = aqn + ar$$

$$\Rightarrow ax + ny = aqn + ar + ny$$

$$\Rightarrow 1 = aqn + ar + ny$$

NOTES

or that $ar = 1 + (-aq - y)n$

i.e., $a \otimes r = 1$. Similarly $r \otimes a = 1$. If r, n are co-prime, r will be inverse of a.

If r, n are not co-prime, we can find a prime number p s.t., $p \mid r, p \mid n$

$$\Rightarrow p \mid qn \text{ and } p \mid r$$

$$\Rightarrow p \mid qn + r$$

$$\Rightarrow p \mid x$$

$$\Rightarrow p \mid ax \text{ also } p \mid ny$$

$$\Rightarrow p \mid ax + ny = 1$$

which is not possible. Thus r, n are co-prime and so $r \in G$ and is the required inverse of a.

It is easy to see that G will be abelian. We denote this group by U_n or $U(n)$ and call it the group of integers under multiplication modulo n.

Remark: Suppose $n = p$, a prime, then since all the integers 1, 2, 3, ..., $p - 1$ are co-prime to p, these will all be members of G. Again, one can show that

$$G' = \{2, 4, 6, ..., 2(p - 1)\}$$

where $p > 2$ is a prime forms an abelian group under multiplication modulo $2p$.

2.4 SOME PRELIMINARY LEMMAS

Lemma: *In a group G,*

(1) *Identity element is unique.*

(2) *Inverse of each $a \in G$ is unique.*

(3) $(a^{-1})^{-1} = a$, *for all* $a \in G$, *where* a^{-1} *stands for inverse of a.*

(4) $(ab)^{-1} = b^{-1} a^{-1}$ *for all* $a, b \in G$

(5) $ab = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$ *for all* $a, b, c \in G$

(called the cancellation laws).

Proof: (1) Suppose e and e' are two elements of G which act as identity.

Then, since $e \in G$ and e' is identity,

$$e'e = ee' = e$$

and as $e' \in G$ and e is identity

$$e'e = ee' = e'$$

NOTES

The two $\Rightarrow e = e'$

which establishes the uniqueness of identity in a group.

(2) Let $a \in G$ be any element and let a' and a'' be two inverse elements of a, then

$$aa' = a'a = e$$

$$aa'' = a''a = e$$

Now $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.

Showing thereby that inverse of an element is unique. We shall denote inverse of a by a^{-1}.

(3) Since a^{-1} is inverse of a

$$aa^{-1} = a^{-1}a = e$$

which also implies a is inverse of a^{-1}

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

(4) We have to prove that ab is inverse of $b^{-1}a^{-1}$ for which we show

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

Now $(ab)\,(b^{-1}a^{-1}) = [(ab)\,b^{-1}]\,a^{-1}$

$= [(a(bb^{-1})]\,a^{-1}$

$= (ae)\,a^{-1} = aa^{-1} = e$

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

and thus the result follows.

(5) Let $ab = ac$, then

$b = eb = (a^{-1}a)b$

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

$= (a^{-1}\,a)c = ec = c$

Thus $ab = ac \Rightarrow b = c$

which is called the left cancellation law.

One can similarly, prove the right cancellation law.

Theorem 1: *For elements a, b in a group G, the equations ax = b and ya = b have unique solutions for x and y in G.*

Proof: Now $ax = b$

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

$\Rightarrow ex = a^{-1}b$

or $x = a^{-1}b$

which is the required solution of the equation $ax = b$.

NOTES

Suppose $x = x_1$ and $x = x_2$ are two solutions of this equation, then

$$ax_1 = b \text{ and } ax_2 = b$$

$$\Rightarrow ax_1 = ax_2$$

$$\Rightarrow x_1 = x_2 \quad \text{by left cancellation}$$

Showing that the solution is unique.

Similarly $y = ba^{-1}$ will be unique solution of the equation $ya = b$.

Theorem 2: *A non empty set G together with a binary composition '.' is a group if and only if*

(1) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(2) *For any* $a, b \in G$, *the equations* $ax = b$ *and* $ya = b$ *have solutions in G.*

Proof: If G is a group, then (1) and (2) follow by definition and previous theorem.

Conversely, let (1) and (2) hold. To show G is a group, we need prove existence of identity and inverse (for each element).

Let $a \in G$ be any element.

By (2) the equations $ax = a$

$$ya = a$$

have solutions in G.

Let $x = e$ and $y = f$ be the solutions.

Thus $\exists\ e, f \in G$, s.t., $ae = a$

$$fa = a$$

Let now $b \in G$ be *any* element then again by (2) $\exists$ some x, y in G s.t.,

$$ax = b$$

$$ya = b.$$

Now $ax = b \Rightarrow f.(a\,.\,x) = f\,.\,b$

$$\Rightarrow (f\,.\,a)\,.\,x = f\,.\,b$$

$$\Rightarrow a\,.\,x = f\,.\,b$$

$$\Rightarrow b = f\,.\,b$$

Again $y.a = b \Rightarrow (y\,.\,a)\,.\,e = b\,.\,e$

$$\Rightarrow y\,.\,(a\,.\,e) = b\,.\,e$$

$$\Rightarrow y\,.\,a = be$$

$$\Rightarrow b = be$$

thus we have $b = fb$ ...(*i*)

$b = be$ ...(*ii*)

for any $b \in G$

NOTES

Putting $b = e$ in (i) and $b = f$ in (ii) we get

$$e = fe$$
$$f = fe$$
$$\Rightarrow e = f.$$

Hence $ae = a = fa = ea$

i.e., $\exists\ e \in G$, s.t., $ae = ea = a$

$\Rightarrow$ e is identity.

Again, for any $a \in G$, and (the identity) $e \in G$, the equations $ax = e$ and $ya = e$ have solutions.

Let the solutions be $x = a_1$, and $y = a_2$

then $aa_1 = e, \quad a_2a = e$

Now $a_1 = ea_1 = (a_2a)a_1 = a_2(aa_1) = a_2e = a_2.$

Hence $aa_1 = e = a_1a$ for any $a \in G$

i.e., for any $a \in G$, $\exists$ some $a_1 \in G$ satisfying the above relations $\Rightarrow$ a has an inverse. Thus each element has inverse and, by definition, G forms a group.

Remark: While proving the above theorem we have assumed that equations of the type $ax = b$ and $ya = b$ have solutions in G. The result may fail, if only one type of the above equations has solution.

Definition: A non empty set G together with a binary composition '.' is called a *semi-group* if

$$a\ .\ (b\ .\ c) = (a\ .\ b)\ .\ c \quad \text{for all } a, b, c \in G$$

Obviously then every group is a semi-group. That the converse is not true follows by considering the set **N** of natural numbers under addition.

Theorem 3: *Cancellation laws may not hold in a semi-group.*

Proof: Consider M the set of all 2×2 matrices over integers under matrix multiplication, which forms a semi-group.

If we take $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$, $C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$

then clearly $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

But $B \neq C$.

Set of natural numbers under addition is an example of a semi-group in which cancellation laws hold.

Theorem 4: *A finite semi-group in which cancellation laws hold is a group.*

Proof: Let $G = \{a_1, a_2, ..., a_n\}$ be a finite semi-group in which cancellation laws hold.

Let $a \in G$ be any element, then by closure property

$$aa_1, aa_2, ..., aa_n$$

are all in G.

NOTES

Suppose any two of these elements are equal

say, $aa_i = aa_j$ for some $i \neq j$

then $a_i = a_j$ by cancellation

But $a_i \neq a_j$ as $i \neq j$

Hence no two of $aa_1, aa_2, ..., aa_n$ can be equal.

These being n in number, will be distinct members of G (Note $o(G) = n$).

Thus if $b \in G$ be any element then

$$b = aa_i \quad \text{for some } i$$

i.e., for $a, b \in G$ the equation $ax = b$ has a solution ($x = a_i$) in G.

Similarly, the equation $ya = b$ will have a solution in G.

G being a semi-group, associativity holds in G.

Hence G is a group (by theorem 2).

Remark: The above theorem holds only in finite semi-groups. The semi-group of natural numbers under addition being an example where cancellation laws hold but which is not a group.

Theorem 5: *A finite semi-group is a group if and only if it satisfies cancellation laws.*

Proof: Follows by previous theorem.

Definition: A non empty set G together with a binary composition '.' is said to form a *monoid* if

(*i*) $a(bc) = (ab)c \quad \forall\ a, b, c \in G$

(*ii*) $\exists$ an element $e \in G$ s.t., $ae = ea = a \quad \forall\ a \in G$

e is then called identity of G. It is easy to see that e is unique.

So all groups are monoids and all monoids are semi-groups.

When we defined a group, we insisted that $\exists$ an element e which acts both as a right as well as a left identity and each element has both sided inverse. We show now that it is not really essential and only one sided identity and the *same* sided inverse for each element could also make the system a group.

Theorem 6: *A system $< G, . >$ forms a group if and only if*

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(*ii*) $\exists\ e \in G$, *s.t.*, $ae = a$ *for all* $a \in G$

(*iii*) *for all* $a \in G, \exists\ a' \in G$, *s.t.*, $aa' = e$.

Proof: If G is a group, we have nothing to prove as the result follows by definition.

Conversely, let the given conditions hold.

All we need show is that $ea = a$ for all $a \in G$

and $a'a = a$ for any $a \in G$

Let $a \in G$ be any element.

By (*iii*) $\exists\ a' \in G$, s.t., $aa' = e$

$\therefore$ For $a' \in G,\ \exists\ a'' \in G,$ s.t., $a'a'' = e$ (using (*iii*))

Now $a'a = a'(ae) = (a'a)e = (a'a)(a'a'')$

$= a'(aa')a'' = a'(e)a'' = (a'e)a'' = a'a'' = e.$

Thus for any $a \in G,\ \exists\ a' \in G,$ s.t., $aa' = a'a = e$

Again $ea = (aa')a = a(a'a) = ae = a$

$\therefore$ $ae = ea = a$ for all $a \in G$

i.e., e is identity of G.

A Notation: Let G be a group with binary composition '.'. If $a \in G$ be any element then by closure property $a \,.\, a \in G$. Similarly $(a \,.\, a) \,.\, a \in G$ and so on.

It would be very convenient (and natural!) to denote $a \,.\, a$ by a^2 and $a \,.\, (a \,.\, a)$ or $(a \,.\, a) \,.\, a$ by a^3 and so on. Again $a^{-1} \,.\, a^{-1}$ would be denoted by a^{-2}. And since $a \,.\, a^{-1} = e$, it would not be wrong to denote $e = a^0$. It is now a simple matter to understand that under our notation

$$a^m \,.\, a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

where m, n are integers.

In case the binary composition of the group is denoted by +, we will talk of sums and multiples in place of products and powers. Thus here $2a = a + a$, and $na = a + a + \ldots + a$ (n times), if n is a +ve integer. In case n is –ve integer then $n = -m$, where m is +ve and we define $na = -ma = (-a) + (-a) + \ldots + (-a)$ m times.

Problem 1: *If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \le r \le n$, s.t., $a^r = e$.*

Solution: Since $o(G) = n$, G has n elements.

Let $a \in G$ be any element. By closure property $a^2, a^3, \ldots$ all belong to G.

Consider $e, a, a^2, \ldots, a^n$

These are $n + 1$ elements (all in G). But G contains only n elements.

$\Rightarrow$ at least two of these elements are equal. If any of $a, a^2, \ldots, a^n$ equals e, our result is proved. If not, then $a^i = a^j$ for some i, j, $1 \le i, j \le n$. Without any loss of generality, we can take $i > j$

NOTES

NOTES

then $a^i = a^j$

$\Rightarrow a^i \cdot a^{-j} = a^j \cdot a^{-j}$

$\Rightarrow a^{i-j} = e$ where $1 \le i - j \le n$.

Putting $i - j = r$ gives us the required result.

Problem 2: *Suppose* $(ab)^n = a^n b^n$ *for all* $a, b \in G$ *where* $n > 1$ *is a fixed integer.*

Show that(*i*) $(ab)^{n-1} = b^{n-1}a^{n-1}$

(*ii*) $a^n\ b^{n-1} = b^{n-1}a^n$

(*iii*) $(aba^{-1}b^{-1})^{n(n-1)} = e$ *for all* $a, b \in G$

Solution: (*i*) We have

$[b^{-1}(ba)b]^n = b^{-1}(ba)^n b$

and $[b^{-1}(ba)b]^n = (ab)^n$

$(ab)^n = b^{-1}(ba)^n b$

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

$\Rightarrow (ab)^{n-1} = b^{n-1}a^{n-1}$ for all $a, b \in G$

(*ii*) Now $(a^{-1}b^{-1}ab)^n = a^{-n}b^{-n}a^n b^n$

and $(a^{-1}b^{-1}ab)^n = a^{-n}(b^{-1}ab)^n$

$= a^{-n}b^{-1}a^n b$

$\therefore\quad a^{-n}b^{-n}a^n b^n = a^{-n}b^{-1}a^n b$

$\Rightarrow a^n b^{n-1} = b^{n-1}a^n$ for all $a, b \in G$

(*iii*) Consider $(aba^{-1}b^{-1})^{n(n-1)}$

$= [(aba^{-1}b^{-1})^{n-1}]^n$

$= [(ba^{-1}b^{-1})^{n-1}a^{n-1}]^n$ by (*i*)

$= [ba^{-(n-1)}b^{-1}a^{n-1}]^n = [b(a^{-(n-1)}b^{-1}a^{n-1})]^n$

$= b^n(a^{-(n-1)}b^{-1}a^{n-1})^n = b^n a^{-(n-1)}b^{-n}a^{n-1}$

$= a^{-(n-1)}b^n b^{-n}a^{n-1}$ by (*ii*)

$= e$ for all $a, b \in G$.

2.5 SUBGROUPS

We have seen that **R**, the set of real numbers, forms a group under addition, and **Z**, the set of integers, also forms a group under addition. Also **Z** is a subset of **R**. It is one of the many situations which prompts us to make

Definition: A non empty subset H of a group G is said to be a subgroup of G, if H forms a group under the binary composition of G.

NOTES

Obviously, if H is a subgroup of G and K is a subgroup of H, then K is subgroup of G.

If G is a group with identity element e then the subsets $\{e\}$ and G are trivially subgroups of G and we call them the *trivial* subgroups. All other subgroups will be called non-trivial (or proper subgroups).

Thus it is easy to see that the even integers form a subgroup of $(\mathbf{Z}, +)$, which is a subgroup of $(\mathbf{Q}, +)$ which is a subgroup of $(\mathbf{R}, +)$.

Again the subset $\{1, -1\}$ will be a subgroup of $G = \{1, -1, i, -i\}$ under multiplication.

Notice that $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ mod 5 is not a subgroup of $\mathbf{Z}$ under addition as addition modulo 5 is not the composition of $\mathbf{Z}$. Similarly, $\mathbf{Z}_5$ is not a subgroup of $\mathbf{Z}_6$ etc.

We sometimes use the notation $H \leq G$ to signify that H is a subgroup of G and $H < G$ to mean that H is a proper subgroup of G.

It may be a little cumbersome at times to check whether a given subset H of a group G is a subgroup or not by having to check all the axioms in the definition of a group. The following two theorems (especially the second one) go a long way in simplifying this exercise.

Theorem 7: *A non empty subset H of a group G is a subgroup of G iff*

(*i*) $a, b \in H \Rightarrow ab \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let H be a subgroup of G then by definition it follows that (*i*) and (*ii*) hold.

Conversely, let the given conditions hold in H.

Closure holds in H by (*i*).

Again $a, b, c \in H \Rightarrow a, b, c \in G \quad \Rightarrow \quad a(bc) = (ab)c$

Hence associativity holds in H.

Also for any $a \in H$, $a^{-1} \in H$ and so by (*i*)

$aa^{-1} \in H \Rightarrow e \in H$

thus H has identity.

Inverse of each element of H is in H by (*ii*).

Hence H satisfies all conditions in the definition of a group and thus it forms a group and therefore a subgroup of G.

Theorem 8: *A non void subset H of a group G is a subgroup of G iff* $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: If H is a subgroup of G then, $a, b \in H \Rightarrow ab^{-1} \in H$ (follows easily by using definition).

NOTES

Conversely, let the given condition hold in H.

That associativity holds in H follows as in previous theorem.

Let $a \in H$ be any element ($H \neq \varphi$)

then $a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

So H has identity.

Again, for any $a \in H$, as $e \in H$

$$ea^{-1} \in H \Rightarrow a^{-1} \in H$$

i.e., H has inverse of each element.

Finally, for any $a, b \in H$,

$$a, b^{-1} \in H$$

$$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$$

i.e., H is closed under multiplication.

Hence H forms a group and therefore a subgroup of G.

Remark: If the binary composition of the group is denoted by +, the above condition would read as $a, b \in H \Rightarrow a - b \in H$. Note also that e is always in H.

The following theorem may not prove to be very useful in as much as it confines itself to finite subsets only but nevertheless it has its importance.

Problem 3: *Let G be the group of all 2×2 non singular matrices over the reals. Find centre of G.*

Solution: If $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any element of the centre $Z(G)$ of G then it should commute with all members of G. In particular we should have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Rightarrow b = c,\ a = d$$

Also $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ gives

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$$\Rightarrow a + b = a,\ b = c = 0$$

Hence any member $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $Z(G)$ turns out to be of the type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

In other words, members of the centre $Z(G)$ are the 2×2 scalar matrices of G.

Problem 4: *Let G be a group in which*

$$(ab)^3 = a^3b^3$$

$$(ab)^5 = a^5b^5, \quad \textit{for all } a, b \in G$$

Show that G is abelian.

Solution: We first show that $b^2 \in Z(G)$ for all $b \in G$.

We know $(a^{-1}ba)^3 = a^{-1}\, b^3a$

By given condition $(a^{-1}ba)^3 = a^{-3}\,(ba)^3 = a^{-3}\, b^3a^3$

$\Rightarrow\ a^{-1}\, b^3a = a^{-3}\, b^3a^3$

$\Rightarrow\ a^2b^3 = b^3a^2$ for all $a, b \in G$

Similarly, $(a^{-1}\, ba)^5 = a^{-1}\, b^5\, a$

$(a^{-1}\, ba)^5 = a^{-5}\, b^5a^5$

$\Rightarrow\ a^{-1}\, b^5a = a^{-5}\, b^5a^5$

$\Rightarrow\ a^4b^5 = b^5a^4 \ \Rightarrow\ a^4b^3b^2 = b^5a^4$

$\Rightarrow\ (a^2)^2\, b^3b^2 = b^5a^4 \ \Rightarrow\ b^3a^4b^2 = b^5a^4$

$\Rightarrow\ a^4b^2 = b^2a^4 \ \Rightarrow\ aa^3b^2 = b^2a^4$

$\Rightarrow\ ab^2a^3 = b^2a^4$

$\Rightarrow\ ab^2 = b^2a$ for all $a, b \in G$

$\therefore\ b^2 \in Z(G)$ for all $b \in G$

Now $(ab)^4 = (ab)^5\,(ab)^{-1} = a^5b^5b^{-1}\, a^{-1}$

$= a^5b^4a^{-1} = a^5a^{-1}b^4$, as $b^2 \in Z(G) = a^4b^4$

$\therefore\ (ab)^i = a^ib^i$ for three consecutive integers $i = 3, 4, 5$

So, $ab = ba$ for all $a, b \in G$, by problem done earlier.

Hence G is abelian.

Problem 5: *Show that* $N(x^{-1}\, ax) = x^{-1}\, N(a)x$ *for all* $a, x \in G$.

Solution: Let $y \in N(x^{-1}\, ax)$

then $(x^{-1}\, ax)\, y = y\, (x^{-1}\, ax)$

$\Rightarrow\ y^{-1}\, x^{-1}\, axy = x^{-1}\, ax$

$\Rightarrow\ xy^{-1}\, x^{-1}\, a = axy^{-1}\, x^{-1}$

$\Rightarrow\ xy^{-1}\, x^{-1} \in N(a)$

$\Rightarrow\ xy^{-1}\, x^{-1} = b \in N(a)$

$y^{-1} = x^{-1}\, bx$

$\Rightarrow\ y = x^{-1}\, b^{-1}\, x,\ b^{-1} \in N(a)$ as $b \in N(a)$

$\Rightarrow\ y \in x^{-1}\, N(a)x$

$\therefore\ N(x^{-1}\, ax) \subseteq x^{-1}\, N(a)\, x$

NOTES

NOTES

Let $z \in x^{-1} N(a)x \Rightarrow z = x^{-1} cx,\ c \in N(a)$

$\therefore \quad z(x^{-1} ax) = (x^{-1} cx)\ (x^{-1} ax)$

$= x^{-1} cax$

$= x^{-1} acx \quad$ as $c \in N(a)$

$= (x^{-1} ax)\ (x^{-1} cx)$

$= (x^{-1} ax)z$

$\Rightarrow z \in N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x \subseteq N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x = N(x^{-1} ax) \quad$ for all $a, x \in G$.

It would be an easy exercise to show that intersection of two subgroups will be a subgroup. In fact, one can prove that if $\{H_i \mid i \in I\}$ be any set of subgroups of a group G then $\underset{i \in I}{\cap} H_i$ will be a subgroup of G.

Theorem 9: *Union of two subgroups is a subgroup iff one of them is contained in the other.*

Proof: Let H, K be two subgroups of a group G and suppose $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

Conversely, let H, K be two subgroups of G s.t., $H \cup K$ is also a subgroup of G. We show one of them must be contained in the other. Suppose it is not true, *i.e.*,

$H \not\subseteq K,\ K \not\subseteq H$

Then $\exists\ x \in H \quad$ s.t., $\quad x \notin K$

$\exists\ y \in K \quad$ s.t., $\quad y \notin H$

Also then $x, y \in H \cup K$ and since $H \cup K$ is a subgroup, $xy \in H \cup K$

$\Rightarrow xy \in H$ or $xy \in K$

If $xy \in H$, then as $x \in H$, $x^{-1}(xy) \in H \Rightarrow y \in H$, which is not true.

Again, if $xy \in K$, then as $y \in K$, $(xy)y^{-1} \in K \Rightarrow x \in K$ which is not true.

i.e., either way we land up with a contradiction.

Hence our supposition that $H \not\subseteq K$ and $K \not\subseteq H$ is wrong.

Thus one of the two is contained in the other.

Definition: Let H be a subgroup of a group G. For $a, b \in G$, we say a is congruent to b mod H if $ab^{-1} \in H$.

In notational form, we write $a \equiv b \bmod H$.

It is easy to prove that this relation is an equivalence relation. Corresponding to this equivalence relation, we get equivalence classes. For any $a \in G$, the equivalence class of a, we know will be given by

$$cl(a) = \{x \in G \mid x \equiv a \bmod H\}.$$

Definition: Let H be a subgroup of G and let $a \in G$ be any element. Then $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

NOTES

We show in the following theorem that any right coset of H in G is an equivalence class. To be exact we state and prove:

Theorem 10: *$Ha = \{x \in G \mid x \equiv a \bmod H\} = cl(a)$ for any $a \in G$.*

Proof: Let $x \in Ha$

Then $x = ha$ for some $h \in H$

$\Rightarrow xa^{-1} = h$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow x \equiv a \bmod H$

$\Rightarrow x \in cl(a)$

thus $Ha \subseteq cl(a)$.

Again let $x \in cl(a)$ be any element.

Then $x \equiv a \bmod H$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow xa^{-1} = h$ for some $h \in H$

$\Rightarrow x = ha \in Ha$

thus $cl(a) \subseteq Ha$

and hence $Ha = cl(a)$.

Having established that right cosets are equivalence classes, we are free to use the results that we know about equivalence classes. We can, therefore, say now that *any two right cosets are either equal or have no element in common* and also that *union of all the right cosets of H in G will equal G*.

Remark: Note that a coset is not essentially a subgroup. If G be the Quaternion group then $H = \{1, -1\}$ is a subgroup of G. Take $a = i$, then $Ha = \{i, -i\}$ which is not a subgroup of G. (it doesn't contain identity). See theorem 15 ahead.

Lemma: *There is always a $1-1$ onto mapping between any two right cosets of H in G.*

Proof: Let Ha, Hb be any two right cosets of H in G.

Define a mapping $f : Ha \to Hb$, s.t.,

$f(ha) = hb$

Then $h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$

$\Rightarrow f(h_1a) = f(h_2a)$

i.e., f is well defined.

$$f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$$

Showing f is 1–1.

That f is onto, is easily seen, as for any $hb \in Hb$, ha would be its pre image.

NOTES

The immediate utility of this lemma is seen, if the group G happens to be finite, because in that case the lemma asserts that any two right cosets of H in G have the same number of elements. Since $H = He$ is also a right coset of H in G, this leads us to state that all right cosets of H in G have the *same* number of elements as are in H (G, being, of course, finite). We are now ready to prove

Theorem 11 (Lagrange's): *If G is a finite group and H is a subgroup of G then o(H) divides o(G).*

Proof: Let $o(G) = n$.

Since corresponding to each element in G, we can define a right coset of H in G, the number of distinct right cosets of H in G is less than or equal to n.

Using the properties of equivalence classes we know

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_t$$

where t = no. of distinct right cosets of H in G.

$$\Rightarrow o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_t)$$

(reminding ourselves that two right cosets are either equal or have no element in common).

$$\Rightarrow o(G) = o(H) + o(Ha) \underbrace{+ \ldots +}_{t \text{ times}} o(H) \quad \text{using the above lemma}$$

$$\Rightarrow o(G) = t.\ o(H)$$

or that $o(H) \mid o(G)$

and we have proved a very important theorem.

But a word of caution here. Converse of Lagrange's theorem does not hold.

Remarks: (i) If G is a group of prime order, it will have only two subgroups G and $\{e\}$. See theorem 25 also.

(ii) A subset $H \neq G$ with more than half the elements of G cannot be a subgroup of G.

We have been talking about *right cosets* of H in G all this time. Are there left cosets also? The answer should be an obvious yes. After all we can similarly talk of

$$aH = \{ah \mid h \in H\}, \quad \text{for any } a \in G$$

which would be called a *left coset*. One can by defining similarly an equivalence relation ($a \equiv b \bmod H \Leftrightarrow a^{-1} b \in H$) prove all similar results for left cosets. It would indeed be an interesting 'brushing up' for the reader, by proving these results independently.

We now come to a simple but very important

Theorem 12: *Let H be a subgroup of G then*

(*i*) $Ha = H \Leftrightarrow a \in H$; $aH = H \Leftrightarrow a \in H$

(*ii*) $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $aH = bH \Leftrightarrow a^{-1} b \in H$

(*iii*) *Ha* (*or aH*) *is a subgroup of G iff* $a \in H$.

NOTES

Proof: (*i*) Let $Ha = H$

Since $e \in H$, $ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H$.

Let $a \in H$, we show $Ha = H$.

Let $x \in Ha \Rightarrow x = ha$ for some $h \in H$

Now $h \in H$, $a \in H \Rightarrow ha \in H \Rightarrow x \in H \Rightarrow Ha \subseteq H$

Again, let $y \in H$, since $a \in H$

$ya^{-1} \in H$

$\Rightarrow ya^{-1} = h$ for some $h \in H$

$\Rightarrow y = ha \in Ha$

$\Rightarrow H \subseteq Ha$

Hence $Ha = H$.

(*ii*) $Ha = Hb$

$\Leftrightarrow (Ha)b^{-1} = (Hb)b^{-1}$

$\Leftrightarrow Hab^{-1} = He$

$\Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ using (*i*)

(*iii*) If $a \in H$ then $Ha = H$ which is a subgroup. Conversely, if *Ha* is a subgroup of *G* then $e \in Ha$ and thus the right cosets *Ha* and *He* have one element *e* in common and hence $Ha = He = H \Rightarrow a \in H$ by (*i*).

Corresponding results for left cosets can be tackled similarly.

Definition: Let *G* be a group and *H*, a subgroup of *G*. Then *index* of *H* in *G* is the number of distinct right (left) cosets of *H* in *G*. It is denoted by $i_G(H)$ or $[G:H]$. (See Problem 15).

A look at the proof of Lagrange's theorem suggests that if *G* is a finite group, then $i_G(H) = \frac{o(G)}{o(H)}$.

It is, of course, possible for an infinite group *G* to have a subgroup $H \neq G$ with finite index.

Example 13: Let $< \mathbf{Z}, + >$ be the group of integers under addition.

Let $H = \{3n \mid n \in \mathbf{Z}\}$ then *H* is a subgroup of **Z**. We show *H* has only three right cosets in **Z** namely H, $H + 1$, $H + 2$.

NOTES

If $a \in \mathbf{Z}$ be any element ($\neq 0, 1, 2$) then we can write (by division algorithm).

$$a = 3n + r, \qquad 0 \leq r < 3$$

which gives

$$H + a = H + (3n + r) = (H + 3n) + r = H + r$$

where $0 \leq r < 3$

Hence H has only 3 right cosets in $\mathbf{Z}$ and thus has index 3.

Notice, $H - 1 = (H + 3) - 1 = H + (3 - 1) = H + 2$ etc.

Definition: Let H be a subgroup of a group G, we define

$C(H) = \{x \in G \mid xh = hx \text{ for all } h \in H\}$ then $C(H)$ is called *centralizer* of H in G.

Also the set

$$N(H) = \{x \in G \mid xH = Hx\}$$
$$= \{x \in G \mid xHx^{-1} = H\}$$

is called *normalizer* of H in G.

It is an easy exercise to see that both $C(H)$ and $N(H)$ are subgroups of G. See problems ahead.

Again as $x \in C(H) \Rightarrow xh = hx$ for all $h \in H$

$$\Rightarrow xH = Hx$$
$$\Rightarrow x \in N(H)$$

we notice $C(H) \subseteq N(H)$.

However, $C(H)$ need not be equal to $N(H)$ as consider the Quaternion group $G = \{\pm 1, \pm i, \pm j, \pm k\}$ and let $H = \{\pm 1, \pm i\}$.

Then $N(H) = G$ and $C(H) = \{\pm 1, \pm i\}$.

Showing that $C(H) \neq N(H)$

Problem 6: *Show that* $C(H) = G \Leftrightarrow H \subseteq Z(G)$.

Solution: Let $C(H) = G$. Let $h \in H$ be any element. Then $x \in G \Rightarrow x \in C(H)$ $\Rightarrow xh = hx \Rightarrow$ any element h in H commutes with all elements of $G \Rightarrow h \in Z(G) \Rightarrow H \subseteq Z(G)$.

Conversely, let $H \subseteq Z(G)$. Let $x \in G$. Since $H \subseteq Z(G)$ each element of H commutes with every element of G.

$$\Rightarrow xh = hx \quad \text{for all } h \in H$$
$$\Rightarrow x \in C(H) \Rightarrow G \subseteq C(H) \Rightarrow G = C(H).$$

Problem 17: *If* $G = S_3$ *and* $H = \{I, (13)\}$*, write all the left cosets of H in G.*

Solution: $(12)H = \{(12)I, (12)(13)\} = \{(12), (132)\}$

$$= (123)H \quad \text{(Show!)}$$

$(23)H = \{(23)I, (23)(13)\} = \{(23), (132)\} = (132)H$

$(13)H = H$ as $(13) \in H$

$IH = H$

are all the left cosets of H in G.

NOTES

Check Your Progress

1. What is an abelian group?
2. Give an example of general linear group.
3. Is identity element unique in a group?
4. Define subgroup.

2.6 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. If $a * b = b * a$ for all $a, b \in G$ then G is called an abelian group or a commutative group.
2. $\begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix}$
3. Yes, Identity element is unique in a group.
4. A non-empty subset H of a group G is a subgroup of G iff

   (i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H$ $a^{-1} \in H$.

2.7 SUMMARY

- A set G of elements, together with an associative binary operation, which contains an inverse for each element and an identity element is called a group.
- If $a * b = b * a$ for all $a, b \in G$ then G is called an abelian group or a commutative group.
- The set Z of integers, set Q of rational numbers and set R of real numbers form an Abelian group w.r.t. addition.
- G forms a group under a binary composition $\otimes$ and this binary composition on G is defined as $a \otimes b = c$ where c is the least +ve remainder obtained when $a \,.\, b$ is divided by n. This composition $\otimes$ is called multiplication modulo n.
- In a group G, Identity element is unique, inverse of each $a \in G$ is unique, $(a^{-1})^{-1} = a$, for all $a \in G$, where a^{-1} stands for inverse of a, $(ab)^{-1} = b^{-1} a^{-1}$ for all $a, b \in G$, $ab = ac \Rightarrow b = c$; $ba = ca$ $b = c$ for all $a, b, c \in G$

- Subgroup is a group whose members are all members of another group, both being subject to the same operations.
- If G is a finite group and H is a subgroup of G then $o(H)$ divides $o(G)$.

NOTES

2.8 KEY WORDS

- **Associativity:** The associative property states that you can add or multiply regardless of how the numbers are grouped.
- **Identity:** An element of a set which, if combined with another element by a specified binary operation, leaves that element unchanged.
- **Inverse**: An element which, when combined with a given element in an operation, produces the identity element for that operation.
- **Binary composition:** The successive application of functions to a variable, the value of the first function being the argument of the second, and so on.
- **Cosets:** A set composed of all the products obtained by multiplying each element of a subgroup in turn by one particular element of the group containing the subgroup.

2.9 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Explain closure property of a Group.
2. Give some examples of Group.
3. In a group G, show that inverse of each $a \in G$ is unique.
4. Define the Centre of a group.

Long Answer Questions

1. If $G = \{2^r \mid r = 0, \pm 1, \pm 2, ...\}$ then show that G forms a group under usual multiplication.
2. Show that a finite semi-group in which cancellation laws hold is a group.
3. Show that Centre of a group G is a subgroup of G.
4. Prove if G is a finite group and H is a subgroup of G then $o(H)$ divides $o(G)$.

2.10 FURTHER READINGS

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Dasgupta, Abhijit. 2013. *Set Theory: With an Introduction to Real Point Sets*. Berlin: Springer Science & Business Media.

NOTES

UNIT 3 A COUNTING PRINCIPLE

NOTES

Structure

3.0 INTRODUCTION

In this unit, you will learn about a counting principal in group theory, which is the study of groups. Groups are sets equipped with an operation (like multiplication, addition, or composition) that satisfies certain basic properties. As the building blocks of abstract algebra, groups are so general and fundamental that they arise in nearly every branch of mathematics and the sciences. This unit will introduce you to the concepts of normal subgroups and quotients groups. A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves the group structure.

3.1 OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of counting principle
- Define normal subgroups
- Describe quotient groups

3.2 A COUNTING PRINCIPLE

Definition: Let H and K be two subgroups of a group G. We define $HK = \{hk \mid h \in H, k \in K\}$ then HK will be a non empty subset of G (Sometimes, called the *complex* of H and K). Will it form a subgroup? The answer is provided by

Theorem 1: *HK is a subgroup of G iff $HK = KH$.*

Proof: Let HK be a subgroup of G. We show $HK = KH$

Let $x \in HK$ be any element

NOTES

Then $x^{-1} \in HK$ (as HK is a subgroup)

$\Rightarrow x^{-1} = hk$ for some $h \in H, k \in K$

$\Rightarrow x = (hk)^{-1} = k^{-1} h^{-1} \in KH$

thus $HK \subseteq KH$

Again let $y \in KH$ be any element

Then $y = kh$ for some $k \in K, h \in H$

$\Rightarrow \quad y^{-1} = h^{-1} k^{-1} \in HK$

$\Rightarrow \quad y \in HK$ (as HK is a subgroup)

$\Rightarrow \quad KH \subseteq HK$

Hence $HK = KH$.

Conversely, let $HK = KH$.

Let $a, b \in HK$ be any two elements, we show $ab^{-1} \in HK$

$a, b \in HK \Rightarrow \quad a = h_1 k_1$ for some $h_1, h_2 \in H$

$b = h_2 k_2 \qquad k_1, k_2 \in K$

Then $ab^{-1} = (h_1 k_1)\ (h_2 k_2)^{-1} = (h_1 k_1)\ (k_2^{-1} h_2^{-1})$

$= h_1 (k_1 k_2^{-1})\ h_2^{-1}$

Now $(k_1 k_2^{-1})\ h_2^{-1} \in KH = HK$

thus $(k_1 k_2^{-1})\ h_2^{-1} = hk$ for some $h \in H, k \in K$

Then $ab^{-1} = h_1 (hk) = (h_1 h) k \in HK$

Hence HK is a subgroup.

Remarks: (*i*) $HK = KH$ does not mean that each element of H commutes with every element of K. It only means that for each $h \in H, k \in K$, $hk = k_1 h_1$ for some $k_1 \in K$ and $h_1 \in H$.

(*ii*) If G has binary composition +, we define

$$H + K = \{h + k \mid h \in H, k \in K\}.$$

Theorem 2: *If H and K are finite subgroups of a group G then*

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}.$$

Proof: Let $D = H \cap K$ then D is a subgroup of K and as in the proof of Lagrange's theorem, $\exists$ a decomposition of K into disjoint right cosets of D in K and

$$K = Dk_1 \cup Dk_2 \cup \ldots \cup Dk_t$$

and also $$t = \frac{o(K)}{o(D)}$$

Again, $HK = H(\bigcup_{i=1}^{t} Dk_i)$ and since $D \subseteq H$, $HD = H$

NOTES

Thus $HK = \bigcup_{i=1}^{t} Hk_i = Hk_1 \cup Hk_2 \cup ... \cup Hk_t$

Now no two of $Hk_1, Hk_2, ..., Hk_t$ can be equal as if $Hk_i = Hk_j$ for some i, j

then $k_i k_j^{-1} \in H \Rightarrow k_i k_j^{-1} \in H \cap K \Rightarrow k_i k_j^{-1} \in D \Rightarrow Dk_i = Dk_j$

which is not true.

Hence $o(HK) = o(Hk_1) + (Hk_2) + ... + o(Hk_t)$

$$= o(H) + o(H) + ... + o(H)$$

$$= t \,.\, o(H)$$

$$= \frac{o(H) \,.\, o(K)}{o(H \cap K)}$$

which proves the result.

3.3 NORMAL SUBGROUPS

Definition: A subgroup H of a group G is called a *normal subgroup* of G if $Ha = aH$ for all $a \in G$.

A normal subgroup is also called *invariant* or *self conjugate* subgroup.

Clearly G and $\{e\}$ are normal subgroups of G and are referred to as the trivial normal subgroups. A group $G \neq \{e\}$ is called a **simple group** if the only normal subgroups of G are $\{e\}$ and G. Any group of prime order is simple.

It is easy to see that if H is a normal subgroup of G and K is a subgroup of G s.t., $H \subseteq K \subseteq G$ then H is normal in K. Again, if G is abelian, all its subgroups will be normal. We use the notation $H \trianglelefteq G$ to convey that H is normal in G.

Example 1: $H = \{1, -1\}$ is a normal subgroup of the Quaternion group G. Indeed $Ha = \{a, -a\} = aH$ for any $a \in G$.

The following two theorems give us equivalent conditions under which a subgroup of a group is normal. So one could also take any one of these as definition of a normal subgroup.

Theorem 3: *A subgroup H of a group G is normal in G iff $g^{-1}Hg = H$ for all $g \in G$.*

Proof : Let H be normal in G

then $Hg = gH$ for all $g \in G$

$\Rightarrow g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)\, H = H.$

Conversely, let $g^{-1}Hg = H$ for all $g \in G$

Then $g(g^{-1}Hg) = gH$

$\Rightarrow (gg^{-1})Hg = gH$

$\Rightarrow Hg = gH.$

Hence H is normal.

NOTES

Theorem 4: *A subgroup H of a group G is normal in G iff* $g^{-1}hg \in H$ *for all* $h \in H, g \in G$.

Proof: Let H be normal in G, then

$Ha = aH$ for all $a \in G$

Let $h \in H, g \in G$ be any elements, then

$hg \in Hg = gH$

$\Rightarrow hg = gh_1$ for some $h_1 \in H$

$\Rightarrow g^{-1}hg = h_1 \in H$

which proves the result.

Conversely, let $a \in G$ be any element,

then $a^{-1}ha \in H$ for all $h \in H$

$\Rightarrow a(a^{-1}ha) \in aH$ for all $h \in H$

$\Rightarrow ha \in aH$ for all $h \in H$

$\Rightarrow Ha \subseteq aH$

Taking $b = a^{-1}$, we note, as $b \in G$

$b^{-1}\ hb \in H\ \ h \in H$

$\Rightarrow aha^{-1} \in H$ for all $h \in H$

$\Rightarrow (aha^{-1})a \in Ha$ for all $h \in H$

$\Rightarrow ah \in Ha$ for all $h \in H$

$\Rightarrow aH \subseteq Ha.$

Hence $Ha = aH$, showing H is normal.

Remark: Evidently, it makes no difference in the argument if the above condition is read as $ghg^{-1} \in H$ for all $h \in H, g \in G$.

The next theorem also gives us an equivalent condition for a subgroup to be normal, but the importance of this theorem is much more in as much as it helps us to form what would be known as Quotient groups. The very statement of the theorem suggests the presence of a binary composition. (We would also remind the reader here that we *did* talk about the product of two subsets of a group in a remark earlier).

Theorem 5: *A subgroup H of a group G is normal subgroup of G iff product of two right cosets of H in G is again a right coset of H in G.*

NOTES

Proof: Let H be a normal subgroup of G.

Let Ha and Hb be any two right cosets of H in G.

then $(Ha)(Hb) = H(aH)b$

$= H(Ha)b$

$= HHab$

$= Hab \quad ab \in G$

Conversely, we are given that product of any two right cosets of H in G is again a right coset.

To show H is normal, let $g \in G$ be any element.

Then Hg and Hg^{-1} are two right cosets of H in G. Thus $HgHg^{-1}$ is also a right coset of H in G.

We claim $HgHg^{-1} = He$

Now $egeg^{-1} \in HgHg^{-1}$

$\Rightarrow e \in HgHg^{-1}$

Also $e \in H$

thus H and $HgHg^{-1}$ are two right cosets having one element common. Recalling the properties of equivalence classes we know that two right cosets are either equal or have no element in common. Thus, (as e is common element)

$H = HgHg^{-1}$

Now $hgh_1g^{-1} \in HgHg^{-1}$ for all $h, h_1 \in H, g \in G$

$\Rightarrow hgh_1g^{-1} \in H$ for all $h, h_1 \in H, g \in G$

$\Rightarrow h^{-1}(hgh_1g^{-1}) \in h^{-1}H$

$\Rightarrow gh_1g^{-1} \in H$ for all $h_1 \in H, g \in G$

$\Rightarrow H$ is normal in G.

Hence the result.

Let H be a subgroup of a group G. Define

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

then as seen earlier $g^{-1}Hg$ forms a subgroup of G.

Again, if we define a mapping $f: H \to g^{-1}Hg$, by

$$f(h) = g^{-1}hg$$

then f will be a 1–1 onto mapping.

In case G is finite, this would mean that both H and $g^{-1}Hg$ (for any $g \in G$) will have same number of elements.

Using this result we have thus proved that *if H be a subgroup of a finite group G s.t., there is no other subgroup of G having the same number of elements as H has, then H is normal in G.* After all, H and $g^{-1}Hg$ (for any $g \in G$) have

same number of elements would mean (by given condition) that they are equal and $H = g^{-1}Hg$ means H is normal.

Problem 1: *Prove that a non empty subset H of a group G is normal subgroup of G* $\Leftrightarrow$ *for all* $x, y \in H, g \in G, (gx)(gy)^{-1} \in H$.

Solution: Let H be normal subgroup of G.

Let $x, y \in H, g \in G$ be any elements,

then $(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \in H$

as $xy^{-1} \in H, g \in G$, H is normal in G.

Conversely, we show H is normal subgroup of G.

Let $x, y \in H$ be any elements,

then $xy^{-1} = exy^{-1}\ e = (ex)\ (ey)^{-1} \in H$ as $e \in G$

i.e., H is a subgroup of G.

Again, let $h \in H, g \in G$ be any elements

then as $(gh)(ge)^{-1} \in H$

we get $(gh)(eg^{-1}) \in H$

$\Rightarrow ghg^{-1} \in H$

$\Rightarrow H$ is normal.

Problem 2: Show that the normaliser $N(a)$ of a in a group G may not be a normal subgroup of G.

Solution: Let $G = S_3$ and $a = (23)$, then $N(a) = N((23)) = \{\sigma \in S_3 \mid \sigma(23) = (23)\sigma\} = \{I, (23)\}$

Since, $N(a)(12) = \{(12), (132)\}$

and $(12)N(a) = \{(12), (123)\}$

we find $N(a)(12) \neq (12)N(a)$ or that $N(a)$ is not normal.

Problem 3: *If N is a normal subgroup of order* 2, *of a group G then show that* $N \subseteq Z(G)$, *the centre of G.*

Solution: Let $N = \{a, e\}$.

Since $e \in Z(G)$ (centre being a subgroup contains e) all that we want to show is that $a \in Z(G)$

i.e., $ag = ga$ for all $g \in G$

or $g^{-1}ag = a$ for all $g \in G$

Let $g \in G$ be any element then as $a \in N$ and N is normal, $g^{-1}ag \in N = \{a, e\}$

$\Rightarrow g^{-1}ag = a$ or $g^{-1}ag = e$

Since $g^{-1}ag = e \Rightarrow ag = ge \Rightarrow ag = eg \Rightarrow a = e$, which is not true

we get $g^{-1}\ ag = a \ \Rightarrow a \in Z(G)$

or $N \subseteq Z(G)$.

NOTES

Problem 4: *Show that a subgroup N of G is normal iff* $xy \in N \Rightarrow yx \in N$.

Solution: Let N be normal in G and let $xy \in N$.

Since $yx = y(xy)y^{-1}$

and $xy \in N$, $y \in G$, N is normal in G we find

$$y(xy)y^{-1} \in N \Rightarrow yx \in N.$$

Conversely, let $n \in N$, $g \in G$ be any elements

then $n \in N \Rightarrow (ng)\, g^{-1} \in N$

$\Rightarrow g^{-1}(ng) \in N$ (given condition)

$\Rightarrow N$ is normal in G.

Problem 5: *Show that a subgroup H of G is normal iff* $Ha \neq Hb \Rightarrow aH \neq bH$.

Solution: Let H be normal in G and suppose $Ha \neq Hb$

then $aH \neq bH$

as $Ha = aH$, $Hb = bH$ as H is normal in G.

Conversely, let $Ha \neq Hb \Rightarrow aH \neq bH$

then $aH = bH \Rightarrow Ha = Hb$

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

Let now $g \in G$, $h \in H$ be any elements, then

$h^{-1} \in H \Rightarrow h^{-1}gg^{-1} \in H$

$\Rightarrow (h^{-1}g)\,(g^{-1}) \in H \Rightarrow (h^{-1}g)^{-1}\, g \in H$

$\Rightarrow g^{-1}hg \in H$

$\Rightarrow H$ is normal in G.

Problem 6: *Let H be a subset of a group G. Let* $N(H) = \{x \in G \mid Hx = xH\}$ *be the normalizer of H in G.* and N(H) is a subgroup of G.

(*i*) *If H is a subgroup of G then N*(*H*) *is the largest subgroup of G in which H is normal.*

(*ii*) *If H is a subgroup of G then H is normal in G iff N*(*H*) = *G.*

(*iii*) *Show by an example, the converse of* (*ii*) *fails if H is only a subset of G.*

(*iv*) *If H is a subgroup of G and K is a subgroup of N*(*H*) *then H is normal subgroup of HK.*

Solution: (*i*) We show H is normal in $N(H)$.

Since $Hh = hH$ for all $h \in H$, we find

$h \in N(H)$ for all $h \in H$.

Thus $H \leq N(H)$.

Again by definition of $N(H)$, $Hx = xH$ for all $x \in N(H)$

$\Rightarrow$ H is normal in $N(H)$.

To show that $N(H)$ is the largest subgroup of G in which H is normal, suppose K is any subgroup of G such that H is normal in K.

then $k^{-1} Hk = H$ for all $k \in K$

$\Rightarrow Hk = kH$ for all $k \in K$

$\Rightarrow k \in N(H)$ for all $k \in K$

$\Rightarrow K \subseteq N(H)$.

(*ii*) Let H be a normal subgroup of G

then $N(H) \subseteq G$ (by definition)

Let $x \in G$ be any element,

then $xH = Hx$ as H normal in G.

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

Hence $G = N(H)$.

Conversely, let $G = N(H)$, H is a subgroup of G (given)

Let $h \in H$, $g \in G$ be any elements

Then $g \in N(H)$ as $N(H) = G$

$\Rightarrow gH = Hg$

$\Rightarrow H$ is normal in G.

(*iii*) Consider $G = < a > = \{e, a, a^2, a^3\}$

then G being cyclic is abelian group.

Take $H = \{a\}$

then H is a subset and not a subgroup of G ($e \notin H$)

Also $N(H) = G$ as G is abelian.

(*iv*) Let K be a subgroup of $N(H)$

then $k \in K \Rightarrow k \in N(H) \Rightarrow Hk = kH$

i.e., $Hk = kH$ for all $k \in K$

$\Rightarrow HK = KH$

$\Rightarrow HK$ is subgroup of $N(H)$

Note, $h \in H \Rightarrow Hh = hH$ $(=H)$

$\Rightarrow H \subseteq N(H)$ Also $K \subseteq N(H)$

Again $H \subseteq HK \subseteq N(H)$

Hence H is a subgroup of HK

$\Rightarrow$ H is normal subgroup of HK

$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$.

NOTES

3.4 QUOTIENT GROUPS

NOTES

Let G be a group and N a normal subgroup of G. Let us collect all the right cosets of N in G and form a set to be denoted by $\frac{G}{N}$ or G/N. Since N is normal in G, product of any two right cosets of N will again be a right coset of N in G, *i.e.*, we have a well defined binary composition on $\frac{G}{N}$ (Prove it). We now show formally that this set $\frac{G}{N}$ forms a group under this product as its binary composition.

For $Na, Nb \in \frac{G}{N}, NaNb = Nab \in \frac{G}{N}$

If $Na, Nb, Nc \in \frac{G}{N}$ be any members, then

$Na(NbNc) = Na(Nbc) = Na(bc) = N(ab)c = NabNc = (NaNb)\ Nc.$

Again $Ne \in \frac{G}{N}$ will act as identity of $\frac{G}{N}$ and for any $Na \in \frac{G}{N}$, Na^{-1} will be the inverse of Na. Thus $\frac{G}{N}$ forms a group, called the *Quotient group* or the *factor group* of G by N.

It is easy to see that if G is abelian then so would be any of its quotient groups as

$$NaNb = Nab = Nba = NbNa.$$

Converse of this result may not hold.

Remarks: (*i*) In $\frac{G}{N}$, as N is normal, it is immaterial whether we use the word right cosets or left cosets, as $Na = aN$ for all a.

(*ii*) It would indeeed be interesting to see what $\frac{G}{\{e\}}$ and $\frac{G}{G}$ are equal to.

Are these G and $\{e\}$ respectively ? Well not really but 'almost' so. We will take it up when we come to isomorphisms.

Theorem 6: *If G is a finite group and N is a normal subgroup of G then*

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}.$$

NOTES

Proof: Since G is finite, using Lagrange's theorem

$$\frac{o(G)}{o(N)} = \text{number of distinct right cosets of } N \text{ in } G$$

$$= o\left(\frac{G}{N}\right).$$

Theorem 7: *Every quotient group of a cyclic group is cyclic.*

Proof: Let $G = < a >$ be a cyclic group.

Then G is abelian, so every subgroup of G is normal. Let H be any subgroup of G. We show $\frac{G}{H}$ is cyclic. In fact we claim $\frac{G}{H}$ is generated by Ha.

Let $Hx \in \frac{G}{H}$ be any element.

Then $x \in G = < a >$, *i.e.*, x will be some power of a

Let $x = a^m$

Then $Hx = Ha^m = Ha\ a\ .....\ a$ (m times)

$= Ha\ Ha\ .....\ Ha$ (m times)

$= (Ha)^m$

i.e., any element Hx of $\frac{G}{H}$ is a power of $Ha \Rightarrow Ha$ generates $\frac{G}{H}$

or that $\frac{G}{H}$ is cyclic.

Remarks:(*i*) The above result is proved for $m > 0$. In case $m \leq 0$, the proof follows similarly. Notice $a^m = a^{-n} = (a^{-1})^n$ where $n > 0$ and remembering that $Ha^{-1} = (Ha)^{-1}$ and so $(Ha^{-1})^n = (Ha)^{-n} = (Ha)^m$.

(*ii*) If $G = < a >$ is cyclic and $H \leq G$, then $o(G/H)$ is the least +ve integer m, s.t., $a^m \in H$.

We know if $H \leq G$, then $H = <a^m>$ where m is the least +ve integer s.t., $a^m \in H$ (see page 81).

Also, $G/H = < Ha >$. So $o(G/H) = o(Ha) = m$

as $(Ha)^m = Ha^m = H$ as $a^m \in H$ and if $(Ha)^r = H$, then $Ha^r = H \Rightarrow a^r \in H \Rightarrow m \leq r$ as m is such least.

Hence, $o(Ha) = m$ and so $o(G/H) = m$.

(*iii*) Converse of this result is not true.

NOTES

Example 2: Let G be the set of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Then it is easy to see that G will form a group under matrix multiplication. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity, $\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$ will be inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Also G is not abelian.

Let N be the subset containing members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a subgroup of G. (Prove!) Also it is normal as the product of the type

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - \frac{b}{d} \\ 0 & 1 \end{bmatrix} \in N$$

So we get the quotient group $\frac{G}{N}$. We show $\frac{G}{N}$ in abelian.

Let $Nx, Ny \in \frac{G}{N}$ be any elements, then $x, y \in G$.

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian iff $NxNy = NyNx$

$\Leftrightarrow \quad Nxy = Nyx$

$\Leftrightarrow \quad xy\,(yx)^{-1} \in N$

$\Leftrightarrow \quad xyx^{-1}\,y^{-1} \in N$

All we need check now is that the product

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}\begin{bmatrix} \frac{1}{c} & -\frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix}$$ is a matrix of the type $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$.

Thus we can have an abelian quotient group, without the 'parent' group being abelian.

NOTES

Example 3: Let $< \mathbf{Z}, + >$ be the group of integers and let $N = \{3n \mid n \in \mathbf{Z}\}$ then N is a normal subgroup of $\mathbf{Z}$.

$\frac{\mathbf{Z}}{N}$ will consist of members of the type $N + a$, $a \in \mathbf{Z}$

We show $\frac{\mathbf{Z}}{N}$ contains only three elements. Let $a \in \mathbf{Z}$ be any element, where $a \neq 0, 1, 2$ then we can write, by division algorithm,

$$a = 3q + r \quad \text{where } 0 \leq r \leq 2$$

$$\Rightarrow \quad N + a = N + (3q + r) = (N + 3q) + r = N + r \quad \text{as } 3q \in N.$$

but r can take values 0, 1, 2.

Hence $N + a$ will be one of

$$N,\ N + 1,\ N + 2$$

or that $\frac{\mathbf{Z}}{N}$ contains only these three members.

Remarks: (*i*) This example also tells us that in case of cosets, $Ha = Hb$ may not necessarily mean $a = b$. For instance, $N + 4 = N + 1$, but $4 \neq 1$ in above example.

$$[N + 4 = (N + 3) + 1 = N + 1].$$

(*ii*) This serves as an example of an infinite group which has a subgroup N having finite index in G.

(*iii*) This is also an example of a finite quotient group G/H, where the 'parent' group G is not finite. It is, however, easy to see that quotient group of a finite group is finite.

(*iv*) If $\frac{G_1}{N} = \frac{G_2}{N}$ then $G_1 = G_2$

Let $g_1 \in G_1$ be any element, then $Ng_1 \in \frac{G_1}{N} = \frac{G_2}{N}$

$\Rightarrow Ng_1 = Ng_2$ for some $g_2 \in G_2$

$\Rightarrow g_1 g_2^{-1} \in N \subseteq G_2 \Rightarrow g_1 g_2^{-1} = g$ for some $g \in G_2$

$\Rightarrow g_1 = g g_2^{-1} \in G_2 \Rightarrow G_1 \subseteq G_2$. Similarly $G_2 \subseteq G_1$. Hence $G_1 = G_2$.

Problem 4: *Find the order of the element* $< 6 > + 5$ *in the group* $\frac{\mathbf{Z}_8}{< 6 >}$.

Soluton: We have $\mathbf{Z}_8 = \{0, 1, 2, ..., 7\} \bmod 8$

and $< 6 > = \{0, 6, 12\} = H$ (say)

Then, $\frac{\mathbf{Z}_8}{< 6 >} = \frac{\mathbf{Z}_8}{H} = \{H, H+1, H+2, H+3, H+4, H+5\}$

$= \{< 6 >, < 6 > +1, < 6 > +2, < 6 > +3, < 6 > +4, < 6 > +5\}$

Now, $< 6 > + 5 \neq < 6 >$, the identity

Again $2(< 6 > + 5) = < 6 > +10 = < 6 > + 4 \neq < 6 >$

NOTES

Similarly, $3(< 6 > +5)$, $4(< 6 > +5)$, $5(< 6 > +5)$ are not $< 6 >$

whereas $6(< 6 > +5) = < 6 > +30 = < 6 > =$ identity and hence order of $< 6 > +5$ will be 6.

Problem 8: *Let N be a normal subgroup of a group G. Show that* $o(Na) | o(a)$ *for any* $a \in G$.

Soluton: Let $o(a) = n$

then n is the least +ve integer s.t., $a^n = e$.

This gives $Na^n = Ne$

$\Rightarrow$ $Na \,.\, a \ldots\ldots a = N$ (n times)

$\Rightarrow$ $Na \,.\, Na \ldots\ldots Na = N$ (n times)

$\Rightarrow$ $(Na)^n = N$, $Na \in \frac{G}{N}$ and N is identity of $\frac{G}{N}$

$\Rightarrow$ $o(Na) \mid n$ or $o(Na) \mid o(a)$.

Problem 9: *If G is a group such that* $\frac{G}{Z(G)}$ *is cyclic, where* $Z(G)$ *is centre of G then show that G is abelian.*

Solution: Let us write $Z(G) = N$. Then $\frac{G}{N}$ is cyclic. Suppose it is generated by Ng.

Let $a, b \in G$ be any two elements,

then $Na, Nb \in \frac{G}{N}$

$\Rightarrow$ $Na = (Ng)^n$, $Nb = (Ng)^m$ for some n, m

$\Rightarrow$ $Na = Ng \,.\, Ng \ldots\ldots Ng = Ng^n$

$Nb = Ng^m$

$\Rightarrow$ $ag^{-n} \in N$, $bg^{-m} \in N$

$\Rightarrow$ $ag^{-n} = x$, $bg^{-m} = y$ for some $x, y \in N$

$\Rightarrow$ $a = xg^n$, $b = yg^m$

$\Rightarrow$ $ab = (xg^n)\,(yg^m) = x(g^n y)\, g^m$

$= x(yg^n)\, g^m$ as $y \in N = Z(G)$

$= xyg^n\, g^m$

$= xyg^{n+m}$

Similarly, $ba = (yg^m)\ (xg^n) = y\ (g^m x)\ g^n = y\ (xg^m)\ g^n$

$= (yx)g^{m+n}$

$\Rightarrow \quad ab = ba$ as $xy = yx$ as $x, y \in Z(G)$

Showing that G is abelian.

NOTES

Remarks: (*i*) We are talking about $\frac{G}{Z(G)}$ assuming, therefore, that $Z(G)$ is a normal subgroup of G, a result which is easily seen to be true. See exercises.

(*ii*) One can, moving on same lines as in the above solution prove that if G/H is cyclic, where H is a subgroup of $Z(G)$ then G is abelian.

(*iii*) If G is a non abelian group then $G/Z(G)$ is not cyclic.

(*iv*) If $\frac{G}{H}$ is cyclic for some normal subgroup H of G then G may not be abelian. Take G = Quaternion group and $H = \{\pm 1, \pm i\}$ then $o(G/H) = \frac{8}{4} = 2$ a prime. So G/H is cyclic, but G is not abelian.

Problem 10: *Let G be a non-abelian group of order pq where p, q are primes then o(Z(G)) = 1.*

Solution: Since G is non-abelian, by Problem 9, $\frac{G}{Z(G)}$ is not cyclic.

Now, $o(Z(G)) \mid o(G) = pq$

$\Rightarrow o(Z(G)) = 1, p, q$ or pq

$o(Z(G)) = pq \Rightarrow Z(G) = G$

$\Rightarrow G$ is abelian which is not so.

$o(Z(G)) = p \Rightarrow o(G/Z(G)) = \frac{pq}{p} = q$. a prime, meaning $G(Z(G))$ is cyclic which is also not true.

Similarly, $o(Z(G)) = q$ cannot hold and we are left with the only possibility that $o(Z(G)) = 1$.

Problem 11: *Give an example of an infinite group in which every element is of finite order.*

Solution: (*a*) Let $< \mathbf{Q}, + >$ and $< \mathbf{Z}, + >$ be the groups of rationals and integers under addition. Then the quotient group

$$\frac{\mathbf{Q}}{\mathbf{Z}} = \left\{ \mathbf{Z} + \frac{m}{n} \,\middle|\, \frac{m}{n} \in \mathbf{Q} \right\}$$

NOTES

is an infinite group. Consider any member $\mathbf{Z}+\frac{m}{n}$ of $\frac{\mathbf{Q}}{\mathbf{Z}}$.

Since $n\left(\mathbf{Z}+\frac{m}{n}\right) = \mathbf{Z}+n\frac{m}{n} = \mathbf{Z}+m = \mathbf{Z}$ = Zero of $\frac{\mathbf{Q}}{\mathbf{Z}}$

we find $\mathbf{Z}+\frac{m}{n}$ has finite order $\leq n$. Hence we have our example.

(*b*) Consider again

$$G = \left\{ \mathbf{Z}+\frac{m}{p^n} \,\middle|\, {}_{n\geq 0}^{m},\ n \text{ are integers, } p = \text{fixed prime} \right\}$$

Then G is a subgroup of $\frac{\mathbf{Q}}{\mathbf{Z}}$.

Now $p^n\left(\mathbf{Z}+\frac{m}{p^n}\right) = \mathbf{Z}+\frac{m}{p^n}p^n = \mathbf{Z}+m = \mathbf{Z}$ = zero of G

$\Rightarrow$ order of $\mathbf{Z}+\frac{m}{p^n}$ divides p^n

$\Rightarrow$ order of $\mathbf{Z}+\frac{m}{p^n}$ is $p^r,\ r \leq n$

$\Rightarrow$ order of every element in G is finite and is of the form p^r.

Since G is inifinite, we find this would serve as an example of an infinite p-group.

Again, we can show that every subgroup $H(\neq G)$ of G is of finite order. Hence this is also an example of an infinite group in which every proper subgroup is of finite order.

Problem 12: *Show that <**Q**, +> has no proper subgroup of finite index.*

Solution: Suppose H is any proper subgroup of <**Q**, +> having finite index n.

Then, $o(\mathbf{Q}/H) = n$.

Since H is proper subgroup of **Q**, $\exists\ \frac{a}{b} \in \mathbf{Q}$ s.t., $\frac{a}{b} \notin H$

Now, if $x+H \in \frac{\mathbf{Q}}{H}$ be *any* element

then $n(x + H) = H \Rightarrow nx + H = H$

$\Rightarrow nx \in H \quad \forall\ x \in \mathbf{Q}$

Take $x = \frac{a}{nb}$, then $n\frac{a}{nb} \in H$ i.e., $\frac{a}{b} \in H$ which is not true.

Hence, such a subgroup does not exist.

Check Your Progress

1. What is a normal subgroup?
2. What is the complex of two subgroups?
3. Is every quotient group of a cyclic group is cyclic?

NOTES

3.5 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. A subgroup H of a group G is called a normal subgroup of G if $Ha = aH$ for all $a \in G$.
2. Let H and K be two subgroups of a group G and HK = {hk | h " H, k " K} then HK, a non-empty subset of G, called
3. Yes.

3.6 SUMMARY

- Let H and K be two subgroups of a group G. We define $HK = \{hk \mid h \in H, k \ K\}$ then HK will be a non-empty subset of G (Sometimes, called the *complex* of H and K)
- A subgroup H of a group G is called a normal subgroup of G if $Ha = aH$ for all $a \ G$.
- A normal subgroup is also called invariant or self-conjugate subgroup.
- H be a subgroup of a finite group G s.t., there is no other subgroup of G having the same number of elements as H has, then H is normal in G.
- A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves the group structure.
- Let H be a normal subgroup of G. Then it can be verified that the cosets of G relative to H form a group. This group is called the *quotient group* or *factor group* of G relative to H and is denoted G/H.
- Set of self-conjugate elements of G forms an abelian group Z which is called the center of G.

3.7 KEY WORDS

- **Counting principle:** If there are m ways to do one thing, and n ways to do another, then there are m*n ways of doing both.

NOTES

- **Cyclic group**: A cyclic group is a group that can be generated by a single element (the group generator).
- **Subset**: a set of which all the elements are contained in another set.
- **Subgroup**: a group whose members are all members of another group, both being subject to the same operations.

3.8 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Define self-conjugate subgroup.
2. What is a simple group and also give an example of simple group.
3. Show that a subgroup N of G is normal iff $xy \in N \Rightarrow yx \ N$.
4. Show that the normaliser $N(a)$ of a in a group G may not be a normal subgroup of G.

Long Answer Questions

1. Prove that HK is a subgroup of G iff $HK = KH$.
2. Prove that a subgroup H of a group G is normal in G iff $Hg = H$ for all $g \ G$.
3. Show that the only abelian simple groups are groups of prime order.
4. Describe quotient groups.

3.9 FURTHER READINGS

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Zassenhaus, Hans J. 2013. *The Theory of Groups*. Chelmsford: Courier Corporation.

UNIT 4 CAYLEY'S THEOREM

NOTES

Structure

4.0 INTRODUCTION

In algebra, a homomorphism is a structure-preserving map between two algebraic structures of the same type (such as two groups). A homomorphism may also be an isomorphism, an endomorphism, an automorphism, etc. In this unit, you will understand the notion of isomorphism (a type of equality) in algebraic systems. In the end, permutation groups and generalized Cayley's theorem are discussed.

4.1 OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of homomorphisms
- Understand the concept of automorphisms
- Know about permutation groups
- Discuss Cayley's theorem

4.2 HOMOMORPHISMS

In this section we introduce the reader to the idea of an isomorphism which could also be termed as an 'indirect' equality in algebraic systems. Indeed, if two systems have the same number of elements and *behave* exactly in the same manner, nothing much is lost in calling them equal, although at times the idea of equality may look little uncomfortable, especially in case of infinite sets.

Definition: Let $< G, * >$ and $< G', o >$ be two groups.

A mapping $f: G \to G'$ is called a homomorphism if

$$f(a * b) = f(a)\ o\ f(b) \quad a, b \in G$$

NOTES

As *agreed* earlier, and when there is no scope of confusion, we shall use the same symbol '.' for both binary compositions.

With that as notation we find a map

$f: G \to G'$ is a homomorphism if

$f(ab) = f(a)f(b)$

If, in addition, f happens to be one-one, onto, we say f is an *isomorphism* and in that case write $G \cong G'$.

Also clearly then

$$f(a_1 a_2 \ldots\ldots a_n) = f(a_1)f(a_2) \ldots\ldots f(a_n)$$

holds under an isomorphism (homomorphism)

An onto homomorphism is called *epimorphism.*

A one-one homomorphism is called *monomorphism.*

A homomorphism from a group G to itself is called an *endomorphism* of G.

An isomorphism from a group G to itself is called *automorphism* of G.

If $f: G \to G'$ is onto homomorphism, then G' is called *homomorphic image* of G.

Example 1: Let $< \mathbf{Z}, + >$ and $< \mathbf{E}, + >$ be the groups of integers and even integers.

Define a map $f: \mathbf{Z} \to \mathbf{E}$, s.t.,

$$f(x) = 2x \quad \text{for all } x \in \mathbf{Z}$$

then f is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

that f is 1–1 is clear by taking the steps backwards.

f is a homomorphism as

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

Also f is onto as any even integer $2x$ would have x as its pre-image.

Hence f is an isomorphism.

In fact this example shows that a subset can be isomorphic to its superset.

Example 2: *Let* $\mathbf{R}^+$ *be the group of positive real numbers under multiplication and* $\mathbf{R}$ *the group of all real numbers under addition. Then the map*

$\theta: \mathbf{R}^+ \to \mathbf{R}$ s.t.,

$\theta(x) = \log x$

is an isomorphism.

θ is clearly well defined.

$$\theta(x) = \theta(y)$$

$$\Rightarrow \quad \log x = \log y$$

$\Rightarrow \quad e^{\log x} = e^{\log y}$

$\Rightarrow \quad x = y$

shows that θ is one-one.

Since $\theta(xy) = \log xy = \log x + \log y = \theta(x) + \theta(y)$

we find θ is a homomorphism.

Finally, if $y \in \mathbf{R}$ be any member, then

Since $e^y \in \mathbf{R}^+$ and $\theta(e^y) = y$, we gather that θ is onto and hence on isomorphism. (The map $f : \mathbf{R} \to \mathbf{R}^+$, s.t., $f(a) = e^a$ can also be considered.)

NOTES

Theorem 1: *If $f : G \to G'$ is a homomorphism then*

(*i*) $f(e) = e'$

(*ii*) $f(x^{-1}) = (f(x))^{-1}$

(*iii*) $f(x^n) = [f(x)]^n$, *n an integer.*

where e, e′ are identity elements of G and G′ respectively.

Proof: (*i*) We have

$$\begin{aligned} & e \,.\, e = e \\ \Rightarrow\ & f(e \,.\, e) = f(e) \\ \Rightarrow\ & f(e) \,.\, f(e) = f(e) \\ \Rightarrow\ & f(e) \,.\, f(e) = f(e) \,.\, e' \\ \Rightarrow\ & f(e) = e' \text{ (cancellation)} \end{aligned}$$

(*ii*) Again $xx^{-1} = e = x^{-1}x$

$$\begin{aligned} \Rightarrow\ & f(xx^{-1}) = f(e) = f(x^{-1}x) \\ \Rightarrow\ & f(x)\, f(x^{-1}) = e' = f(x^{-1})\, f(x) \\ \Rightarrow\ & (f(x))^{-1} = f(x^{-1}). \end{aligned}$$

(*iii*) Let n be a +ve integer.

$$\begin{aligned} f(x^n) &= \underset{(n \text{ times})}{f(x \,.\, x \,.\,.\,.\,.\,.\,.\,.\,x)} \\ &= f(x) \,.\, f(x) \,.\,.\,.\,.\, f(x) \quad (n \text{ times}) \\ &= (f(x))^n. \end{aligned}$$

If $n = 0$, we have the result by (*i*). In case n is –ve integer, result follows by using (*ii*).

Problem 4: *Find all the homomorphisms from* $\frac{\mathbf{Z}}{4\mathbf{Z}}$ *to* $\frac{\mathbf{Z}}{6\mathbf{Z}}$.

Solution: Let $f : \frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}}$ be a homomorphism.

Then $f(4\mathbf{Z} + n) = n\, f(4\mathbf{Z} + 1)$

NOTES

So, f is completely known if $f(4\mathbf{Z} + 1)$ is known.

Now order of $(4\mathbf{Z} + 1)$ is 4 and so $o(f(4\mathbf{Z} + 1))$ divides 4

Also $o(f(4\mathbf{Z} + 1))$ divides 6 and thus $o(f(4\mathbf{Z} + 1)) = 1$ or 2

If $o(f(4\mathbf{Z} + 1)) = 1$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z} =$ zero of $\frac{\mathbf{Z}}{6\mathbf{Z}}$

Hence $f(4\mathbf{Z} + n) =$ zero

If $o(f(4\mathbf{Z} + 1)) = 2$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z} + 3$

$\Rightarrow f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$

Also $f(4\mathbf{Z} + n + 4\mathbf{Z} + m) = f(4\mathbf{Z} + n + m)$

$= 6\mathbf{Z} + 3(n + m)$

$= (6\mathbf{Z} + 3n) + (6\mathbf{Z} + 3m)$

$= f(4\mathbf{Z} + n) + f(4\mathbf{Z} + m)$

Thus there are two choices for f and it can be defined as

$$f : \frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}} \text{ s.t.,}$$

$$f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$$

Notice $4\mathbf{Z} + n = 4\mathbf{Z} + m$

$\Rightarrow n - m \in 4\mathbf{Z}$

$\Rightarrow 3(n - m) \in 12\mathbf{Z} \subseteq 6\mathbf{Z}$

$\Rightarrow 3(n - m) \in 6\mathbf{Z}$

$\Rightarrow 6\mathbf{Z} + 3n \in 6\mathbf{Z} + 3m$

i.e., f is well defined.

So there are two homomorphisms from $\frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}}$. In fact, in general, there are d homomorphisms from $\frac{\mathbf{Z}}{m\mathbf{Z}} \to \frac{\mathbf{Z}}{n\mathbf{Z}}$ where $d =$ g.c.d.(m, n)

Definition: Let $f: G \to G'$ be a homomorphism. The **Kernel** of f, (denoted by Ker f) is defined by

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

where e' is identity of G'.

Theorem 2: *If $f : G \to G'$ be a homomorphism, then Ker f is a normal subgroup of G.*

Proof: Since $f(e) = e'$, $e \in \text{Ker } f$, thus Ker $f \neq \varphi$. Again,

$x, y \in \text{Ker } f \Rightarrow f(x) = e'$

$f(y) = e'$

Now $f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)(f(y))^{-1} = e' \,.\, e'^{-1} = e'$

$\Rightarrow xy^{-1}$ Ker f

Hence it is a subgroup of G.

Again, for any $g \in G$, $x \in$ Ker f

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g)$$
$$= (f(g))^{-1} f(x)\, f(g) = (f(g))^{-1}\, e'\, f(g)$$
$$= (f(g))^{-1} f(g) = e'$$
$$\Rightarrow g^{-1}xg \in \text{Ker } f$$

or that it is a normal subgroup of G.

Theorem 3: *A homomorphism $f : G \to G'$ is one-one iff Ker $f = \{e\}$.*

Proof: Let $f : G \to G'$ be one-one.

Let $x \in$ Ker f be any element

then $f(x) = e'$ and as $f(e) = e'$

$f(x) = f(e) \Rightarrow x = e$ as f is 1-1

Hence Ker $f = \{e\}$.

Conversely, let Ker f contain only the identity element.

Let $f(x) = f(y)$

Then $f(x)\,(f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \text{Ker } f = \{e\}$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$ or that f is one-one.

Problem 2: *Show that the group <**R**, +> of real numbers cannot be isomorphic to the group R* of non zero real numbers under multiplication.*

Solution: $-1 \in R^*$ and order of -1 is 2 as $(-1)^2 = 1$. But **R** has no element of order 2. As if $x \in$ **R** is of order 2 then $2x = x + x = 0$. But this does not hold in <**R**, +> for any x except $x = 0$.

Under an isomorphism order of an element is preserved. Thus there cannot be any isomorphism between **R** and R^*.

Problem 3: *Let G be a group and $f : G \to G$ s.t., $f(x) = x^{-1}$ be a homomorphism. Show that G is abelian.*

Solution: Let $x, y \in G$ be any elements.

$$xy = (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1})$$
$$= f(y^{-1})\, f(x^{-1})$$
$$= yx, \text{ hence } G \text{ is abelian.}$$

NOTES

Theorem 4: (Fundamental theorem of group homomorphism). *If* $f: G \to G'$ *be an onto homomorphism with* $K = Ker\ f$, *then* $\frac{G}{K} \cong G'$.

NOTES

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G.

Proof: Define a map $\varphi: \frac{G}{K} \to G'$, s.t.,

$$\varphi(Ka) = f(a), \quad a \in G$$

We show φ is an isomorphism.

That φ is well defined follows by

$$\begin{aligned} & Ka = Kb \\ \Rightarrow\ & ab^{-1} \in K = \text{Ker}\, f \\ \Rightarrow\ & f(ab^{-1}) = e' \\ \Rightarrow\ & f(a)(f(b))^{-1} = e' \\ \Rightarrow\ & f(a) = f(b) \\ \Rightarrow\ & \varphi(Ka) = \varphi(Kb) \end{aligned}$$

By retracing the steps backwards, we will prove that φ is 1–1.

Again as
$$\begin{aligned} \varphi(KaKb) &= \varphi(Kab) = f(ab) = f(a)\, f(b) \\ &= \varphi(Ka)\ \varphi(Kb) \end{aligned}$$

we find φ is a homomorphism.

To check that φ is onto, let $g' \in G'$ be any element. Since $f: G \to G'$ is onto, $\exists\ g \in G$, s.t.,

$$f(g) = g'$$

Now
$$\varphi(Kg) = f(g) = g'$$

Showing thereby that Kg is the required pre-image of g' under φ.

Hence φ is an isomorphism.

Remark: The above theorem is also called *first theorem of isomorphism*. It can also be stated as:

If $f: G \to G'$ is a homomorphism with $K = \text{Ker}\, f$, then $\frac{G}{\text{Ker}\, f} \cong f(G)$.

Theorem 5: (Second theorem of Isomorphism). *Let H and K be two subgroups of a group G, where H is normal in G, then*

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

Proof: It is easy to see that $H \cap K$ will be a normal subgroup of K and as $H \subseteq HK \subseteq G$, H will be normal in HK.

Define a map $f : K \to \frac{HK}{H}$ s.t.,

$$f(k) = Hk$$

then as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

we find f is well defined.

Again $f(k_1k_2) = Hk_1k_2 = Hk_1Hk_2 = f(k_1)f(k_2)$

shows f is a homomorphism.

That f is onto is obvious and thus using Fundamental theorem, we find

$$\frac{HK}{H} \cong \frac{K}{\text{Ker } f}$$

Since $k \in \text{Ker } f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow k \in H$

$\Leftrightarrow k \in H \cap K \quad (k \in K \text{ as Ker } f \subseteq K)$

We find $\text{Ker } f = H \cap K$

and our theorem is proved.

Lemma: *If H and K are two normal subgroups of a group G such that* $H \subseteq K$, *then* $\frac{K}{H}$ *is a normal subgroup of* $\frac{G}{H}$, *and conversely.*

Proof: $\frac{K}{H}$ is a non empty subset of $\frac{G}{H}$, by definition.

For any $Hk_1, Hk_2 \in \frac{K}{H}$

$$(Hk_1)(Hk_2)^{-1} = (Hk_1)(Hk_2^{-1}) = Hk_1k_2^{-1} \in \frac{K}{H}$$

i.e., $\frac{K}{H}$ is a subgroup.

Again, for any $Hk \in \frac{K}{H}$ and $Hg \in \frac{G}{H}$, we notice,

$$(Hg)^{-1}(Hk)(Hg) = Hg^{-1}HkHg$$

$$= Hg^{-1}kg \in \frac{K}{H}$$

as $g \in G$, $k \in K$, K is normal in G gives $g^{-1}kg \in K$.

We leave the converse as an exercise for the reader.

NOTES

NOTES

Theorem 6: (Third theorem of isomorphism). *If H and K are two normal subgroups of G such that $H \subseteq K$, then*

$$\frac{G}{K} \cong \frac{G/H}{K/H}.$$

Proof: The above lemma ensures that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk of $\frac{G/H}{K/H}$.

Define a map $f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$$f(Ha) = Ka, \quad a \in G$$

f is well defined as

$$\begin{aligned} & Ha = Hb \\ \Rightarrow\ & ab^{-1} \in H \subseteq K \\ \Rightarrow\ & Ka = Kb \\ \Rightarrow\ & f(Ha) = f(Hb) \end{aligned}$$

f is a homomorphism as

$$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)\, f(Hb).$$

Ontoness of f is obvious.

Using Fundamental theorem of group homomorphism we can say

$$\frac{G}{K} \cong \frac{G/H}{\text{Ker } f}$$

We claim $\text{Ker } f = \frac{K}{H}$

A member of Ker f will be some member of $\frac{G}{H}$.

Now $Ha \in \text{Ker } f \Leftrightarrow f(Ha) = K$ (identity of G/K)

$$\begin{aligned} & \Leftrightarrow Ka = K \\ & \Leftrightarrow a \in K \\ & \Leftrightarrow Ha \in \frac{K}{H} \end{aligned}$$

Hence we find $\frac{G}{K} \cong \frac{G/H}{K/H}$

which proves our result. It is also called *Freshman's theorem*.

Remark: Since $\frac{K}{H} = \text{Ker } f$, we notice that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and hence we can talk of $\frac{G/H}{K/H}$. Thus we need not prove separately that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$.

Theorem 7: *Let $f : G \to G'$ be an onto homomorphism with Ker $f = K$. For H' a subgroup of G', define*

$$H = \{x \in G \mid f(x) \in H'\}$$

Then

(*i*) *H is a subgroup of G and $K \subseteq H$.*

(*ii*) *H' is normal subgroup of G' iff H is normal in G.*

(*iii*) *If H' is normal in G' then $\frac{G'}{H'} \cong \frac{G}{H}$.*

(*iv*) *This association gives a one-one onto mapping from the family **S'** of all subgroups of G' onto the family **S** of all subgroups of G, that contain K.*

Proof: (*i*) $H \neq \varphi$ as $f(e) = e' \in H'$ shows $e \in H$

Again, $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)(f(y))^{-1} \in H'$.

$\Rightarrow f(xy^{-1}) \in H' \Rightarrow xy^{-1} \in H$

Thus H is a subgroup.

Since $x \in \text{Ker } f = K \Rightarrow f(x) = e' \in H'$

we find $x \in H \Rightarrow K \subseteq H$.

(*ii*) Let H be normal in G.

Let $g' \in G', h' \in H'$ be any elements. Since f is onto $\exists\ g \in G, h \in G$ such that $f(g) = g', f(h) = h'$. Since $h' \in H, h \in H$

Now

$g'^{-1} h'g' = (f(g))^{-1} f(h) f(g)$

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

as $g \in G, h \in H$, H is normal in G means $g^{-1}hg \in H$

Thus H' is normal in G'.

Conversely, let H' be normal in G'.

For any elements $h \in H, g \in G$,

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

as $f(h) \in H', f(g) \in G', H'$ is normal in G'

$\Rightarrow g^{-1}hg \in H$ or that H is normal in G.

(*iii*) Define a mapping $\varphi : G \to \frac{G'}{H'}$ s.t.,

$$\varphi(g) = H' f(g)$$

then φ is well defined as $g_1 = g_2$

NOTES

NOTES

$$\Rightarrow f(g_1) = f(g_2)$$
$$\Rightarrow H' f(g_1) = H' f(g_2)$$
$$\Rightarrow \varphi(g_1) = \varphi(g_2)$$

φ will be a homomorphism as

$\varphi(g_1 g_2) = H' f(g_1 g_2) = H' f(g_1) f(g_2) \quad = H' f(g_1)\, H' f(g_2)$
$= \varphi(g_1)\varphi(g_2)$

Again, for any $H'g' \in \frac{G'}{H'}$ since $g' \in G'$ and f is onto $\exists\, g \in G$, s.t., $f(g) = g'$

or that $\varphi(g) = H' f(g) = H'g'$ showing that φ is onto.

By fundamental theorem then

$$\frac{G'}{H'} \cong \frac{G}{\text{Ker } \varphi}$$

Now $x \in \text{Ker } \varphi \Leftrightarrow \varphi(x) = H'$
$\Leftrightarrow H' f(x) = H'$
$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$

Hence $\text{Ker } \varphi = H$

(*iv*) Define a mapping $\psi : \boldsymbol{S'} \to \boldsymbol{S}$, s.t.,

$$\psi(H') = H$$

where, of course, H is $\{x \in G \mid f(x) \in H'\}$ for any H' in $\boldsymbol{S'}$ By (*i*) we know that it is subgroup of G, containing K and is thus a member of $\boldsymbol{S}$. ψ is, therefore, a well defined mapping.

Let now $\psi(H') = \psi(T')$ where $H', T' \in \boldsymbol{S'}$

then $H = T$ where

$H = \{x \in G \mid f(x) \in H'\}$

$T = \{x \in G \mid f(x) \in T'\}$

Now for any $h' \in H' \subseteq G'$, since $f : G \to G'$ is onto, we can find $h \in G$, s.t., $f(h) = h' \in H'$

But this shows $h \in H = T$
$\Rightarrow f(h) \in T'$
$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$

Similarly $T' \subseteq H'$

i.e., $H' = T'$ or that ψ is one-one.

We show now ψ is onto.

Let $H \in \boldsymbol{S}$ be any member, then H is a subgroup of G and $K \subseteq H$.

Consider $f(H) = \{f(h) \mid h \in H\}$

then $f(H) \neq \varphi$ as $e \in H \Rightarrow f(e) = e' \in f(H)$

Again, for any $f(h_1), f(h_2) \in f(H)$, $h_1, h_2 \in H$

and $(f(h_1))(f(h_2))^{-1} = f(h_1 h_2^{-1}) \in f(H)$

i.e., $f(H)$ is a subgroup of G'.

We show $f(H) = H'$ is the required pre-image of H under ψ,

i.e., we show $\psi(H') = H$,

For that we need show $H = \{x \in G \mid f(x) \in H'\}$

Let $x \in H$ then $f(x) \in f(H) = H'$

$$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$$

or that $H \subseteq \{x \in G \mid f(x) \in H'\}$

Again, if $x \in \{x \in G \mid f(x) \in H'\}$

then $f(x) \in H' = f(H)$

$\exists\ h \in H$, s.t., $f(x) = f(h)$

$$\Rightarrow f(xh^{-1}) = e'$$

$$\Rightarrow xh^{-1} \in \text{Ker } f = K$$

$$\Rightarrow x \in Kh \subseteq H \quad [K \subseteq H]$$

Thus $\{x \in G \mid f(x) \in H'\} \subseteq H$

Hence $H = \{x \in G \mid f(x) \in H'\}$

or that $\psi(H') = H$ and so ψ is onto.

which completes the proof.

Problem 4: *Let N be a normal subgroup of G, then show that any subgroup of G/N is of the type* $\frac{H}{N}$*, where H is a subgroup of G and* $N \subseteq H$.

Solution: Let $\overline{H}$ be any subgroup of G/N.

Let $f: G \to G/N$, s.t., $f(x) = Nx$ be the natural homomorphism.

Let $H = \{x \in G \mid f(x) \in \overline{H}\}$, then $H \leq G$ and $N \subseteq H$

as in above theorem.

Now $\frac{H}{N} = \{Nh \mid h \in H\} = \{f(h) \mid h \in H\} = f(H) = \overline{H}$

which proves the result.

Problem 5: *Find all the subgroups of* $\frac{\mathbf{Z}}{(12)}$*, where*

$\mathbf{Z}$ = *group of all integers under addition*

and (12) = *subgroup of* $\mathbf{Z}$ *consisting of all multiples of* 12.

NOTES

Solution: By above problem, any subgroup of $\frac{\mathbf{Z}}{(12)}$ is of the form $\frac{H}{(12)}$ where H is a subgroup of $\mathbf{Z}$ under addition and contains (12). But any subgroup of $\mathbf{Z}$ under addition is (n) = set of all multiples of n, $n \geq 0$.

$\therefore$ $H = (2), (3), (4), (6), (12)$. So subgroups of $\frac{\mathbf{Z}}{(12)}$ are

$$\frac{(2)}{(12)}, \frac{(3)}{(12)}, \frac{(4)}{(12)}, \frac{(6)}{(12)}, \frac{(12)}{(12)}$$

Note $\frac{(2)}{(12)} = \{(12), (12) + 2, (12) + 4, (12) + 6, (12) + 8, (12) + 10\}$

$\frac{(3)}{(12)} = \{(12), (12) + 3, (12) + 6, (12) + 9\}$

$\frac{(4)}{(12)} = \{(12), (12) + 4, (12) + 8\}$

$\frac{(6)}{(12)} = \{(12), (12) + 6\}$

$\frac{(12)}{(12)} = \{(12)\}$.

4.3 AUTOMORPHISMS

Example 3: Let G be a group, then the identity map $I : G \to G$, s.t., $I(x) = x$ is trivially an automorphism of G. In fact, it is sometimes called the *trivial* automorphism of G.

Example 4: Let $\mathbf{Z}$ = group of integer under addition

then $f : \mathbf{Z} \to \mathbf{Z}$, s.t.,

$f(n) = -n$

is an automorphism as $f(n) = f(m) \Rightarrow -n = -m \Rightarrow n = m \Rightarrow f$ is 1–1.

Again, since for any $n \in \mathbf{Z}$, $f(-n) = n$ we find f is onto.

Now $f(n + m) = -(n + m) = -n - m = f(n) + f(m)$

shows f is a homomorphism and hence an automorphism.

Example 5: If G be an abelian group and $f : G \to G$ be such that $f(x) = x^{-1}$ then as $f(xy) = (xy)^{-1} = y^{-1} x^{-1} = x^{-1} y^{-1} = f(x) f(y)$,

f is a homomorphism.

Again $f(x) = f(y) \Rightarrow x^{-1} = y^{-1}$

$\Rightarrow x = y \Rightarrow f$ is 1–1.

f is clearly onto and hence an automorphism.

Example 6: If G be a non-abelian group, then the above defined map $f: G \to G$ s.t., $f(x) = x^{-1}$ is not an automorphism.

NOTES

Since G is non-abelian, $\exists\, x, y \in G$ s.t., $xy \neq yx$

Now if $f(xy) = f(x)f(y)$

then $(xy)^{-1} = x^{-1}\, y^{-1}$

$\Rightarrow (xy)^{-1} = (yx)^{-1}$

$\Rightarrow xy = yx$, a contradiction.

Hence f is not an automorphism.

We notice then $f: G \to G$, s.t., $f(x) = x^{-1}$ is an automorphism iff G is abelian.

Theorem 8: *Let G be a group. Let Aut G denote the set of all automorphisms of G and A(G) be the group of all permutations of G. Then Aut G is a subgroup of A(G).*

Proof: Since $I \in$ Aut G, Aut $G \neq \varphi$

Let $T \in$ Aut G. Then T is 1–1 onto from G to G.

$\therefore$ T is a permutation of G.

$\therefore$ $T \in A(G)$. So, Aut $G \subseteq A(G)$.

Let $T_1, T_2 \in$ Aut G.

Then $(T_1\, T_2)(xy) = T_1(T_2(xy))$

$= T_1(T_2(x)T_2(y))$ as T_2 is a homomorphism

$= T_1(T_2(x))T_1(T_2(y))$ as T_1 is a homomorphism

$= (T_1T_1)(x).(T_1T_2)(y)$ for all $x, y \in G$

$\therefore$ $T_1\, T_2$ is a homomorphism from G into G.

Again, $(T_1T_2)(x) = (T_1\, T_2)(y)$

$\Rightarrow T_1(T_2(x)) = (T_1(T_2(y))$

$\Rightarrow T_2(x) = T_2(y)$ as T_1 is 1–1

$\Rightarrow x = y$ as T_2 is 1–1

$\therefore$ T_1T_2 is 1–1

Let $x \in G$. Since $T_1 : G \to G$ is onto $\exists\, y \in G$ s.t. $T_1(y) = x$.

Again as $T_2 : G \to G$ is onto, $\exists\, z \in G$ s.t. $y = T_2(z)$

$\Rightarrow T_1(T_2(z)) = x$

$\Rightarrow (T_1\, T_2)(z) = x$

$\therefore$ T_1T_2 is also onto.

So, $T_1T_2 \in$ Aut G.

NOTES

Let $T \in \text{Aut } G$. Then T is 1–1 onto $\Rightarrow$ T is invertible and

$$T^{-1} : G \to G \text{ s.t. } T^{-1}(x) = y \Leftrightarrow T(y) = x$$

as $TT^{-1} = I = T^{-1} T$

T^{-1} is 1–1 as $T^{-1}(x_1) = T^{-1}(x_2)$

$$\Rightarrow TT^{-1}(x_1) = TT^{-1}(x_2)$$

$$\Rightarrow I(x_1) = I(x_2)$$

$$\Rightarrow x_1 = x_2$$

Let $x \in G$ then $y = T(x) \in G$

$\therefore$ $T^{-1}(y) = T^{-1}(T(x)) = (T^{-1}T)\, x = x$

$\therefore$ T^{-1} is onto.

Let $T^{-1}(xy) = z$ then $T(z) = xy$

Let $T^{-1}(x) = x_1,\ T^{-1}(y) = y_1$

Then $x = T(x_1),\quad y = T(y_1)$

$$\Rightarrow T(z) = xy = T(x_1)\, T(y_1) = T(x_1 y_1)$$

as T is a homomorphism.

$\therefore$ $z = x_1 y_1$ as T is $1 - 1$

So $T^{-1}(xy) = z = x_1 y_1 = T^{-1}(x)\, T^{-1}(y)$ for all $x, y \in G$

$\Rightarrow$ T^{-1} is a homomorphism.

Thus $T^{-1} \in \text{Aut } G$

Hence, Aut G is a subgroup of $A(G)$.

(Thus Aut G forms a group).

Inner Automorphisms

Let $g \in G$. Define $T_g : G \to G$ s.t.

$$T_g(x) = gxg^{-1} \quad \text{for all } x \in G$$

Then T_g is 1–1 as

$$T_g(x) = T_g(y)$$

$$\Rightarrow gxg^{-1} = gyg^{-1}$$

$$\Rightarrow x = y.$$

Let $x \in G$. Then $g^{-1} xg \in G$.

and $T_g(g^{-1} xg) = g(g^{-1} xg)\, g^{-1} = x$

$\therefore$ T_g is onto

Also $T_g(xy) = g(xy)\, g^{-1}$

$$= (gxg^{-1})\, (gyg^{-1})$$

$= T_g(x)\ T_g(y)$ for all $x, y, \in G$

Hence T_g is automorphism of G and it is called an *inner automorphism* of G.

Theorem 9: *The set I(G) of all inner automorphisms of G is a subgroup of Aut G.*

NOTES

Proof: $T_e \in I(G)$ where e = identity of G.

$\therefore \quad I(G) \neq \varphi$

Let $T_{g_1}, T_{g_2} \in I(G)$

Then $T_{g_1} T_{g_2}(x) = T_{g_1}(g_2 x g_2^{-1}) = g_1 g_2\ x\ g_2^{-1}\ g_1^{-1}$

$= (g_1 g_2)\ x\ (g_1 g_2)^{-1}$

$= T_{g_1 g_2}(x)$ for all $x \in G$

$\therefore \quad T_{g_1} T_{g_2} = T_{g_1 g_2} \in I(G)$

Let $T_g \in I(G)$

Then $T_g\ T_{g-1} = T_e = I$ (as $T_e(x) = exe^{-1} = x$ for all $x \in G$)

and $T_{g-1}\ T_g = I$

$\therefore \quad T_{g-1} = (T_g)^{-1} \Rightarrow (T_g)^{-1} \in I(G)$

$\therefore$ $I(G)$ is a subgroup of Aut G.

In fact, $I(G)$ is normal in Aut G.

A question arises, when is $T_{g_1} = T_{g_2}$?

Suppose $T_{g_1} = T_{g_2}$

then $T_{g_1}(x) = T_{g_2}(x)$ for all $x \in G$

$\Leftrightarrow \quad g_1\ x\ g_1^{-1} = g_2\ x\ g_2^{-1}$ for all $x \in G$

$\Leftrightarrow \quad g_2^{-1}\ g_1\ x = x\ g_2^{-1}\ g_1$ for all $x \in G$

$\Leftrightarrow \quad g_2^{-1}\ g_1 \in Z(G)$

$\Leftrightarrow \quad g_1 Z(G) = g_2 Z(G)$

$\therefore \quad T_{g_1} = T_{g_2} \Leftrightarrow g_1 Z(G) = g_2 Z(G)$

Problem 6: *For any integer $a > 1$, $n > 0$ show that*

$n \mid \varphi(a^n - 1)$

Solution: Let $G = < b >$ s.t. $o(G) = o(b) = a^n - 1$

Define $T : G \to G$ s.t.,

$T(x) = x^a$

Since $(a\ ,\ a^n - 1) = 1,\ T \in$ Aut G

NOTES

Also $T^2(x) = T(T(x))$

$= T(x^a) = (x^a)^a = x^{a^2}$

In general, $T^r(x) = x^{a^r}$

$\therefore \quad T^n(x) = x^{a^n} = x$ for all $x \in G$

(as $x^{o(G)} = e \Rightarrow x^{a^n - 1} = e \Rightarrow x^{a^n} = x$)

$\therefore \quad T^n = 1$

If $T^m = 1$, then $T^m(b) = b$

$\Rightarrow b^{a^m} = b \Rightarrow b^{a^m - 1} = e$

$\Rightarrow o(b) \mid (a^m - 1)$

$\Rightarrow a^n - 1 \mid (a^m - 1) \Rightarrow a^n - 1 \leq (a^m - 1)$

$\Rightarrow a^n \leq a^m \Rightarrow n \leq m$

$\therefore \quad o(T) = n$

Also $o(\text{Aut } G) = \varphi(a^n - 1)$,

$T \in \text{Aut } G \Rightarrow o(T) \mid o(\text{Aut } G)$

$\Rightarrow n \mid \varphi(a^n - 1)$.

Characteristic Subgroups

A subgroup H of G is called a *characteristic subgroup* of G if

$T(H) \subseteq H$ for all $T \in \text{Aut } G$.

Example 7: Let G be a cyclic group of order 4

$G = \{e, a, a^2, a^3\}$

Then Aut $G = \{I, T\}$, where $T(x) = x^3$ for all $x \in G$

Let $H = \{e, a^2\} \leq G$

$\therefore \quad I(H) = \{I(e), I(a^2)\} = H$

$T(H) = \{T(e), T(a^2)\} = \{e, a^6 = a^2\} = H$

$\therefore$ H is a characteristic subgroup of G.

4.4 PERMUTATION GROUPS

Theorem (Cayley's) 10: *Every group G is isomorphic to a permutation group.*

Proof: Let G be the given group and $A(G)$ be the group of all permutations of the set G.

For any $a \in G$, define a map $f_a : G \to G$, s.t.,

NOTES

$$f_a(x) = ax$$

then as $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

f_a is well defined.

Again, $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ (cancellation in group G)

$\Rightarrow f_a$ is 1–1.

Also, for any $y \in G$, since $f_a(a^{-1}y) = a(a^{-1}y) = y$, we find $a^{-1}y$ is pre-image of y or that f_a is onto and hence a permutation on G.

Thus $f_a \in A(G)$.

Let K be the set of all such permutations. We show K is a subgroup of $A(G)$. $K \neq \varphi$ as $f_e \in K$.

Let $f_a, f_b \in K$ be any members

then since $f_b \; o \; f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x)) = f_b(b^{-1}x) = b(b^{-1}x)$

$= ex = f_e(x)$ for all x

we find $f_{b^{-1}} = (f_b)^{-1}$ (Note $f_e = I$, identity of $A(G)$).

Also as $(f_a \; o \; f_b)\, x = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$ for all x

we find $f_{ab} = f_a \; o \; f_b$

Now $f_a \; o \; (f_b)^{-1} = f_a \; o \; f_{b^{-1}} = f_{ab^{-1}} \in K$

Showing that K is a subgroup of $A(G)$.

Define now a mapping $\varphi : G \to K$, s.t.,

$$\varphi(a) = f_a$$

then φ is well defined, 1-1 map as

$a = b$

$\Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x) \quad \forall \; x$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \varphi(a) = \varphi(b)$

φ is obviously onto, and since

$$\varphi(ab) = f_{ab} = f_a \; o \; f_b = \varphi(a)\; \varphi(b)$$

φ is a homomorphism and hence an isomorphism which proves our assertion. Note K being a subgroup of a permutation group is a permutation group.

Remark: In particular, if G is a finite group of order n then G is isomorphic to a subgroup of S_n.

NOTES

Problem 7: *Using Cayley's theorem, find the permutation group K isomorphic to the group G = {2, 4, 6, 8} under multiplication modulo 10.* (*Here 6 is the identity of G and G = <2>*).

Solution: The set K as defined in the Cayley's theorem above is given by $K = \{f_a \mid a \in G\}$, where f_a is defined by $f_a(x) = ax$. Thus here a = 2, 4, 8, 6 and

$$f_2(2) = 4, \quad f_2(4) = 8, \quad f_2(8) = 6, \quad f_2(6) = 2$$
$$f_4(2) = 8, \quad f_4(4) = 6, \quad f_4(8) = 2, \quad f_4(6) = 4$$
$$f_8(2) = 6, \quad f_8(4) = 2, \quad f_8(8) = 4, \quad f_8(6) = 8$$
$$f_6(2) = 2, \quad f_6(4) = 4, \quad f_6(8) = 8, \quad f_6(6) = 6$$

Thus $f_6 = I$ and $K = \{f_2, f_4, f_8, f_6 = I\}$

If we identify f_2 with the permutation (1234), we notice the others are (13)(24), (1432) and thus K is {(1234), (13)(24), (1432), I} and this is the required premutation group isomorphic to G.

In fact the isomorphism can be viewed as $\theta: G \to K$, s.t.,

$$\theta(2) = (1234),\ \theta(4) = (13)(24),\ \theta(8) = (1432),\ \theta(6) = I$$

Theorem 11: *Order of any permutation f in S_n is equal to the l.c.m. of the orders of the disjoint cycles of f.*

Proof: Let $f = f_1 f_2 \ldots f_n$

be the representation of f as product of disjoint cycles $f_1, f_2, \ldots, f_n$

Let $o(f_i) = r_i \quad i = 1, 2, \ldots, n$

then $f_i^{r_i} = I$ (identity of S_n)

Let $r = \text{l.c.m.}(r_1, r_2, \ldots, r_n)$

Now $f^r = (f_1 f_2 \ldots f_n)^r = f_1^r f_2^r \ldots f_n^r$ as f_i are disjoint and so commutative.

Since $r_i \mid r$ for all i, we have $r = r_i k_i, \quad i = 1, 2, \ldots, n$

Thus $f^r = f_1^{r_1 k_1} f_2^{r_2 k_2} \ldots f_n^{r_n k_n} = I \,.\, I \ldots I = I$

Suppose now $f^t = I$

$$\Rightarrow (f_1 f_2 \ldots f_n)^t = I$$
$$\Rightarrow f_1^t f_2^t \ldots f_n^t = I$$
$$\Rightarrow f_1^t = f_2^t = \ldots = f_n^t = I$$

as $f_1, f_2, \ldots, f_n$ are disjoint. (Note if some $f_i^t \neq I$ then L.H.S. cannot be I).

$$\Rightarrow r_i \mid t \quad \text{for all } i$$
$$\Rightarrow r \mid t$$

Hence $r = o(f)$.

Example 8: Order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 1 & 3 \end{pmatrix} = (1245)(36)$$

is l.c.m.(4, 2) = 4 as $o(1245) = 4$ and $o(36) = 2$.

NOTES

Problem 8: *Give an example of two subgroups H, K which are not normal, but HK is a subgroup.*

Solution: Let $H = \{I, (12)\}$

$K = \{I, (123), (132)\}$

be two subgroups of S_4 (that these are subgroups can be verified).

Here $HK = \{I, (12), (123), (132), (12)(123), (12)(132)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

$KH = \{I, (123), (132), (12), (123)(12), (132)(12)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

Thus $HK = KH \Rightarrow HK$ is a subgroup.

Now $H(123) = \{(123), (12)(123)\} = \{(123), (23)\}$

$(123)H = \{(123), (13)\}$

or that $H(123) \neq (123)H$

i.e., $Ha \neq aH$ for some $a \in S_4$

$\Rightarrow H$ is not normal in S_4.

Similarly one can check that $K(14) \neq (14)K$

or that K is not normal in S_4.

Problem 9: *Show that* $Z(S_n) = \{I\}$, $(n \geq 3)$.

Solution: Let $f \in Z(S_n)$ be such that $f \neq I$

then $\exists$ a s.t., $f(a) = b$ where $b \neq a$

Let $c \neq a, b$ be any element (note $n \geq 3$)

Let g be the mapping where $g(a) = a$

$g(b) = c$

$g(c) = b$

then $g \in S_n$

Now $(fg)a = f(g(a)) = f(a) = b$

$(gf)a = g(f(a)) = g(b) = c$

$\Rightarrow fg \neq gf$ *i.e.*, $f \notin Z(S_n)$

Thus if $f \neq I$ then it cannot belong to $Z(S_n)$ or that $Z(S_n) = \{I\}$.

Cor.: S_n is non abelian $\forall$ $n \geq 3$. Note G is abelian iff $G = Z(G)$.

4.5 CAYLEY'S THEOREM

NOTES

Theorem 12: (Generalised Cayley's theorem): *Let H be a subgroup of G and* $\mathcal{L} = \{aH \mid a \in G\}$ *then* $\exists$ *a homomorphism* $\theta : G \to A(\mathcal{L})$ *s.t., Ker* θ *is the largest normal subgroup of G contained in H.*

Proof: Define $\theta : G \to A(\mathcal{L})$ s.t.,

$$\theta(g) = f_g$$

where $f_g : \mathcal{L} \to \mathcal{L}$ s.t.

$$f_g(aH) = gaH$$

To show that θ is well defined, we need prove that $f_g \in A(\mathcal{L})$

Now $f_g(aH) = f_g(bH)$

$\Rightarrow gaH = gbH$

$\Rightarrow aH = bH \quad \Rightarrow f_g$ is 1-1

Again for any $aH \in \mathcal{L}$,

$f_g(g^{-1}aH) = aH$, showing that

f_g is onto and thus $f_g \in A(\mathcal{L})$

We have $\theta(gh) = f_{gh}$, $\theta(g)\theta(h) = f_g f_h$

and since $f_{gh}(aH) = ghaH$

$f_g f_h(aH) = f_g(f_h(aH)) = f_g(haH) = ghaH$

we find $f_{gh} = f_g f_h$

or that θ is a homomorphism.

Since Kernel of a homomorphism is normal subgroup, we have Ker θ, a normal subgroup of G.

Again, if $g \in$ Ker θ then

$\theta(g) = I =$ Identity of $A(\mathcal{L})$

$\Rightarrow f_g = I$

$\Rightarrow f_g(aH) = aH \quad \forall\ aH \in \mathcal{L}$

In particular,

$f_g(eH) = eH \Rightarrow geH = eH \quad \Rightarrow gH = H$

$\Rightarrow g \in H$

$\Rightarrow$ Ker $\theta \subseteq H$

Let now K be any normal subgroup of G, contained in H. Let $k \in K$ be any element. We want to show that $k \in$ Ker θ or that $\theta(k) = I$.

or that $f_k = I$

or that $f_k(aH) = aH \quad \forall\ aH$

Now $f_k(aH) = kaH = a(a^{-1}ka)\ H = ahH = aH$

[Note $a^{-1}ka \in K \subseteq H$]

Hence $K \subseteq$ Ker θ which proves the theorem.

NOTES

Remarks: (*i*) If we wish to work with right cosets, θ can be defined by $\theta(g) = f_g$ where $f_g(Ha) = Hag^{-1}$.

(*ii*) If $H = \{e\}$, the above theorem is the Cayley's theorem, as then Ker $\theta = \{e\}$ $\Rightarrow$ θ is 1–1.

Cor. (Index theorem): If $H \neq G$ is a subgroup of a finite group G, s.t., $o(G)$ does not divide $i_G(H)!$ then G has a non trivial normal subgroup. (*i.e.*, G is not simple).

Proof: By above theorem, we find Ker θ is a normal subgroup of G.

Since Ker $\theta \subseteq H \neq G$, Ker $\theta \neq G$

If Ker $\theta = \{e\}$, then θ is 1-1 and thus $\theta : G \to A(\mathcal{L})$ is 1-1 homomorphism *i.e.*, G is isomorphic to a subgroup T of $A(\mathcal{L})$.

$$\Rightarrow\ o(G) = o(T)$$

But $o(T) \mid o(A(\mathcal{L})) \Rightarrow o(G) \mid o(A(\mathcal{L})) = i_G(H)!$ a contradiction and so Ker $\theta \neq \{e\}$ and is the required non trival normal subgroup.

Problem 10: *Let H be a subgroup of a finite group G such that o*(*H*) *and* $(i_G(H)-1)!$ *are coprime then show that H is normal in G.*

Solution: Let $S = \{aH \mid a \in G\}$ = Set of left cosets of H in G.

Define $\theta : G \to A(S)$ s.t.,

$\theta(g) = T_g$

where $T_g : S \to S$ s.t., $T_g(aH) = gaH$

Then as seen in generalised Cayley's theorem, θ is a homomorphism and Ker $\theta \subseteq H$.

Also then $\dfrac{G}{\text{Ker}\theta} \cong T$ where $T \leq A(S)$

$\Rightarrow o(G/\text{Ker}\ \theta) = o(T)$ where $o(T) \mid o(A(S)) = \underline{\lfloor i_G(H)}$

Let $i_G(H) = \dfrac{o(G)}{o(H)} = n$

then $o(T) \mid \underline{\lfloor n}$ and thus $\dfrac{o(G)}{o(\text{Ker}\theta)} \mid \underline{\lfloor n}$

Again Ker $\theta \leq H \Rightarrow o(\text{Ker}\ \theta) \mid o(H)$

$\Rightarrow o(H) = m.o(\text{Ker}\ \theta)$ for some m

$\Rightarrow \dfrac{o(G)}{n} = m.o(\text{Ker}\ \theta)$

$$\Rightarrow nm = \frac{o(G)}{o(\text{Ker}\,\theta)}$$

NOTES

or that $nm \mid \underline{n} \Rightarrow nm \mid n.\underline{n-1} \Rightarrow m \mid \underline{n-1}$

Also $m \mid o(H)$ and as they are coprime, $m = 1$ or that $H = \text{Ker}\ \theta$ i.e., $H \trianglelefteq G$.

Check Your Progress

1. What is epimorphism?
2. What is automorphism?
3. What is a characteristic group?

4.6 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. An onto homomorphism is called epimorphism.
2. An isomorphism from a group G to itself is called automorphism of *G*.
3. A subgroup H of G is called a characteristic subgroup of G if $T(H) \subseteq H$ for all $T \in \text{Aut}\ G$.

4.7 SUMMARY

- Let $< G, * >$ and $< G', o >$ be two groups. A mapping $f : G \to G'$ is called a homomorphism if $f(a * b) = f(a)\ o\ f(b)\ \ a, b \in G$
- An onto homomorphism is called epimorphism.
- A one-one homomorphism is called monomorphism.
- A homomorphism from a group *G* to itself is called an endomorphism of *G*.
- An isomorphism from a group *G* to itself is called automorphism of *G*.
- If *f*: *G* *G'* is onto homomorphism, then *G*' is called homomorphic image of *G*.
- Let *G* be a group, then the identity map *I* : *G* *G*, s.t., *I (x)* = *x* is trivially an automorphism of *G*. In fact, it is sometimes called the trivial automorphism of *G*.
- The set *I(G)* of all inner automorphisms of *G* is a subgroup of Aut *G*.
- A subgroup *H* of *G* is called a characteristic subgroup of *G* if *T(H)* H for all T Aut G.
- Every group G is isomorphic to a permutation group.

4.8 KEY WORDS

- **Isomorphism:** A one-to-one correspondence (mapping) between two sets that preserves binary relationships between elements of the sets.
- **Kernel:** The kernel of a homomorphism measures the degree to which the homomorphism fails to be injective.
- **Permutation group:** A group G whose elements are permutations of a given set M and whose group operation is the composition of permutations in G (which are thought of as bijective functions from the set M to itself).

NOTES

4.9 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Define homomorphisms with help of an example.
2. Prove the following theorem: a homomorphism $f: G \to G'$ is one-one iff Ker $f = \{e\}$.
3. Give an example of automorphisms.
4. What are characteristics subgroups?

Long Answer Questions

1. The set $I(G)$ of all inner automorphisms of G is a subgroup of Aut G.
2. Show that order of any permutation f in S_n is equal to the *l.c.m.* of the orders of the disjoint cycles of f.
3. Show that $Z(S_n) = \{I\}$, $(n \geq 3)$.
4. Prove generalised Cayley's theorem.

4.10 FURTHER READINGS

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Eie, Minking, Shou-Te Chang. 2010. *A Course on Abstract Algebra*. Singapore: World Scientific.

Adhikari, Mahima, Avishek Adhikari. 2013. *Basic Modern Algebra with Applications*. Berlin: Springer Science & Business Media.

NOTES

BLOCK - II

SYLOW'S THEOREM AND RING THEORY

UNIT 5 ANOTHER COUNTING PRINCIPLE

Structure

5.0 INTRODUCTION

In mathematics, you sometimes come across with a concept known as the "counting principle". This is concerned with the total number of combination under given conditions. When you deal with the happening of two or more activities or events, it is often required to know quickly the number of total possible activities or events. It can be done by a mathematical device called counting principle.

In this unit, you will learn an equivalence relation on a finite set, measure the size of the equivalence classes under this relation and then equate the number of elements in the set to the sum of orders of these equivalence classes. With this approach, this unit discusses some important results about finite groups.

5.1 OBJECTIVES

After going through this unit, you will be able to:

- Discuss another counting principal for group theory
- Know about its applications
- Solve related problems

5.2 ANOTHER COUNTING PRINCIPLE

NOTES

Definition: Let G be a group, $a, b \in G$. Define a relation $\sim$ on G as follows:

$$a \sim b \Leftrightarrow \exists\ c \in G \text{ s.t. } a = c^{-1} bc$$

It is not difficult to see that $\sim$ is an equivalence relation on G. If $a \sim b$ *we say* a *is conjugate* to b (or a, b *are conjugates and relation* $\sim$ *is called conjugate relation on* G).

Let $cl(a)$ denote the equivalence class of a in G then $cl(a)$ is called *conjugate class or conjugacy class* of a in G. Since $\sim$ is an equivalence relation on G, it divides G into disjoint equivalence classes.

$$\therefore \qquad G = \bigcup_{a \in G} cl(a), \text{ where}$$

$$\begin{aligned} cl(a) &= \{x \in G \mid x \sim a\} \\ &= \{x \in G \mid x = y^{-1} ay,\ y \in G\} \\ &= \{y^{-1} ay \mid y \in G\} \\ &= \text{set of all conjugates of } a \text{ in } G. \end{aligned}$$

Remarks: (*i*) $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$

Suppose $cl(a) = \{a\}$. Then $y^{-1}ay = a$ for all $y \in G$

$\therefore \quad ya = ay$ for all $y \in G$

$\therefore \quad a \in Z(G)$

Conversely, let $a \in Z(G)$. Let $x \in cl(a)$ be any element, then $x = y^{-1}ay$ for some $y \in G$

$$\Rightarrow x = ay^{-1} y \text{ (as } a \in Z(G)$$

$$\Rightarrow x = a \Rightarrow cl(a) = \{a\}.$$

(*ii*) G is abelian $\Leftrightarrow cl(a) = \{a\}$ for all $a \in G$

G is abelian $\Leftrightarrow G = Z(G)$

$\Leftrightarrow a \in Z(G)$ for all $a \in G$

$\Leftrightarrow cl(a) = \{a\}$ for all $a \in G$.

We shall denote by $k(G)$ or k, the number of conjugate classes in G. It follows by remark (*ii*) that $o(G) = k \Leftrightarrow G$ is abelian.

Normalizer or Centralizer of an element $a \in G$ was defined to be the set $N(a) = \{x \in G \mid xa = ax \text{ for all } x \in G\}$. Also $N(a) \leq G$. It can be shown that $N(a) = G \Leftrightarrow a \in Z(G)$

$$N(a) = G \Leftrightarrow g \in N(a) \text{ for all } g \in G$$

$$\Leftrightarrow ga = ag \text{ for all } g \in G$$

$$\Leftrightarrow a \in Z(G).$$

NOTES

So, by remark (*i*) it follows that

$$N(a) = G \Leftrightarrow cl(a) = \{a\}.$$

Problem 1: *Suppose $a \in G$ has only two conjugates in G then show that N(a) is a normal subgroup of G.*

Solution: Let $a, g^{-1}ag$ be two conjugates of a in G. We show

$$G = N(a) \cup N(a)g$$

Let $x \in G$. Consider $x^{-1}ax$. Then $x^{-1}ax = a$ or $g^{-1}ag$.

If $x^{-1}ax = a$, then $xa = ax \Rightarrow x \in N(a)$

If $x^{-1}ax = g^{-1}ag$, then $xg^{-1}a = axg^{-1}$

$$\Rightarrow xg^{-1} \in N(a)$$

$$\Rightarrow x \in N(a)g$$

$$\therefore \quad G = N(a) \cup N(a)g$$

and thus index of $N(a)$ in G is 2, showing thereby that $N(a)$ is a normal subgroup of G.

Problem 2: *Let G be a finite group and x, y be conjugate elements of G. Show that the number of distinct elements $g \in G$ s.t. $g^{-1}xg = y$ is $o(N(x))$.*

Solution: Let $g = g_1, g_2 \ldots, g_n$ be distinct elements of G s.t., $g_i^{-1}xg_i = y$

Let $S = \{g = g_1, g_2 \ldots, g_n\}$

We show that $S = N(x)g$

Suppose $s \in S$ then $s = g_i$ for some i, $1 \le i \le n$

If $s = g_1 = g$, then $s = g = eg \in N(x)\, g$

If $s \neq g_1$, then $s = g_i$, $i \neq 1$

and $g^{-1} xg = g_i^{-1} xg_i$

$$\Rightarrow g_i g^{-1} x = xg_i g^{-1}$$

$$\Rightarrow g_i g^{-1} \in N(x)$$

$$\Rightarrow g_i \in N(x)$$

$$\Rightarrow s \in N(x)g$$

or that $S \subseteq N(x)g$

Again $z \in N(x)g \quad \Rightarrow z = hg, \quad h \in N(x)$

$$\Rightarrow z^{-1} xz = g^{-1} h^{-1} xhg$$

$$\Rightarrow z^{-1} xz = g^{-1} xg \quad \text{as } xh = hx$$

$$\Rightarrow z^{-1} xg = y$$

$$\Rightarrow z = g_i \quad \text{for some } i$$

$$\Rightarrow z \in S$$

$$\Rightarrow N(x)g \subseteq S$$

Hence $S = N(x)g$

and thus $o(S) = o(N(x)g) = o(N(x))$

(**Note:** As $gg_i^{-1} x = xgg_i^{-1}$ for all $i = 1,..., n$

$gg_i^{-1} \in N(x)$ for all i

$\Rightarrow N(x)g = N(x)g_i$ for all i)

NOTES

Problem 3: *Suppose X is a conjugate class of non trivial elements of G. Let $T \in Aut\ G$. Show that $T(X) = \{T(x) \mid x \in X\}$ is a conjugate class of elements of G.*

Solution: Let $X = cl(a), \quad a \neq e$

We show that $T(X) = cl(Ta)$

Let $y \in T(X) \Rightarrow y = Tx, \quad x \in X = cl(a)$

$= T(g^{-1} ag), \quad g \in G$

$= T(g)^{-1} T(a) T(g) \in cl(T(a))$

$\therefore \quad T(X) \subseteq cl(Ta)$

Again $z \in cl(Ta) \Rightarrow z = h^{-1} T(a) h, \quad h \in G$

$= (Th_1)^{-1} Ta\ Th$

(as T is onto $\Rightarrow h = Th_1, \quad h_1 \in G$)

$= Th_1^{-1} Ta\ Th$

$= T(h^{-1} ah)$

$\in T(cl(a)) = T(X)$

$T(X) = cl(Ta)$

Hence $T(X)$ is a conjugate class of G.

5.3 APPLICATION AND RELATED PROBLEMS

The following theorem helps us to determine the order of conjugate class of an element.

Theorem 1: *Let G be a finite group, $a \in G$.*

Then $$o(cl(a)) = \frac{o(G)}{o(N(a))}$$

where cl(a) is the conjugate class of a.

Proof: Since $N(a) \leq G$, G can be written as union of disjoint right cosets of $N(a)$ in G.

Let $$G = \bigcup_{i=1}^{t} N(a)x_i \quad [t \leq n = o(G)]$$

NOTES

Then $o(G) = t \cdot o(N(a))$ ...(1)

Let $S = \{x_1^{-1} ax_1, ..., x_t^{-1} ax_t\}$

Suppose $x_i^{-1} ax_i = x_j^{-1} ax_j$ for $i \neq j$

Then $x_i x_j^{-1} a = a x_i x_j^{-1}$

$\Rightarrow x_i x_j^{-1} \in N(a)$

$\Rightarrow N(a)x_i = N(a)x_j$, a contradiction

$\therefore$ all elements in S are distinct i.e., $o(S) = t$

We show that $S = cl(a)$

Let $s \in S$ then $s = x_i^{-1} a x_i$, for some i, $1 \leq i \leq t$

$\Rightarrow s$ is conjugate of a

$\Rightarrow s \in cl(a) \Rightarrow S \subseteq cl(a)$

Again $x \in cl(a) \Rightarrow x = g^{-1} ag$, $g \in G$

$g \in G \Rightarrow g \in N(a)x_i$ for some i, $1 \leq i \leq t$

$\Rightarrow g = yx_i$, $y \in N(a)$

Thus $x = x_i^{-1} y^{-1} a y x_i$

$= x_i^{-1} ax_i$ as $ya = ay$

$\Rightarrow x \in S$

$\therefore$ $cl(a) \subseteq S \Rightarrow S = cl(a)$

and so $o(cl(a)) = o(S) = t$

and hence from (1) we get $o(cl(a)) = \dfrac{o(G)}{o(N(a))}$.

Remark: Since $G = \underset{a \in G}{\cup} (cl(a))$

$$o(G) = \sum_{a \in G} o(cl(a))$$

$$= \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$= o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

(By remark (i) earlier $o(cl(a)) = 1 \Leftrightarrow a \in Z(G)$).

$\therefore$ $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$

i.e., $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \dfrac{o(G)}{o(N(a))}$

This equation is called ***class equation*** of G.

NOTES

Problem 4: *Let G be a finite group and $x \in G$ then show that*

$$o(N(x)) \geq o\left(\frac{G}{G'}\right).$$

Solution: We show that $cl(x) \subseteq G'x$

Let $y \in cl(x) \Rightarrow y = g^{-1}xg, \quad g \in G$

$= (g^{-1}xg)(x^{-1}x)$

$= (g^{-1}xg^{-1}x^{-1})x$

$\in G'x$

$\therefore \quad cl(x) \subseteq G'(x)$

$\therefore \quad o(cl(x)) \leq o(G'x)$

$\therefore \quad \frac{o(G)}{o(N(x))} \leq o(G'x) = o(G')$

$\therefore \quad \frac{o(G)}{o(G')} \leq o(N(x)).$

Problem 5: *If index of Z(G) in G is n then show that any conjugate class has at most n elements.*

Solution: We have

$$n = \frac{o(G)}{o(Z(G))} \text{ and } o(cl(a)) = \frac{o(G)}{o(N(a))}$$

Since $Z(G) \subseteq N(a)$ always

$o(Z(G)) | o(N(a)) \Rightarrow o(N(a)) = k.o(Z(G))$

i.e., $o(Cl(a)) = \frac{o(G)}{o(N(a))} = \frac{n.o(Z(G))}{k.o(Z(G))} = \frac{n}{k}$

Thus, maximum value of $o(cl(a))$ is when $k = 1$, proving the result.

Problem 6: *Let G be group of order p^n, p = prime, n = + ve integer. Show that $o(Z(G)) > 1$.*

Solution: If $G = Z(G)$, $o(Z(G)) = o(G) > 1$.

If $G \neq Z(G)$, then $\exists$ some $a \in G$, s.t., $a \notin Z(G)$.

Then $N(a) < G$ [as $a \notin Z(G) \Rightarrow at \neq ta$ for some $t \in G$, i.e., $t \notin N(a)$, $t \in G$].

$\therefore \quad o(N(a)) = p^m, \quad m < n$

i.e., $\frac{o(G)}{o(N(a))} = p^{n-m}, \quad n - m > 0$

i.e. $o(cl(a)) = p^{n-m} =$ multiple of p

$\therefore \quad \sum_{a \notin Z(G)} o(cl(a)) = \text{multiple of } p = kp, \text{ (say)}$

By class equation of G

NOTES

$$p^n = o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$\Rightarrow \; o(Z(G)) = p^n - kp = p(p^{n-1} - k)$$

$$\Rightarrow \; p \mid o(Z(G)) \Rightarrow o(Z(G) > 1.$$

Remark: It follows from above problem that if G is a finite non-abelian simple group then $o(G)$ is divisible by at least two distinct primes. Since G is simple, it has no non-trivial normal subgroup. Now $Z(G)$ is a normal subgroup of G. $Z(G) = G \Rightarrow G$ is abelian, which is not so. Thus $Z(G) = \{e\}$, which means $o(G)$ cannot be of the type p^n, i.e., it is not divisible by only one prime.

Problem 7: *A group of order p^2 (p = prime) is abelian.*

Solution: Suppose $o(G) = p^2$ and G is non-abelian.

Then $Z(G) \neq G$. So $\exists\, a \in G$, s.t., $a \notin Z(G)$ and as in previous problem, $N(a) \subsetneq G$.

Again, $Z(G) \subseteq N(a)$ always but as $a \notin Z(G)$, $Z(G) \subsetneq N(a)$

Now $o(Z(G) \mid o(G) = p^2 \Rightarrow o(Z(G)) = 1, p \text{ or } p^2$

But $o(Z(G)) > 1$ by problem 6

and $o(Z(G)) = p^2 \Rightarrow Z(G) = G$ which is not true

Hence $o(Z(G)) = p$

Again, $o(N(a)) \mid o(G) = p^2$ gives $o(N(a)) = 1, p \text{ or } p^2$

Since $N(a) \neq G, \quad o(N(a)) \neq p^2$

Also $Z(G) \subsetneq N(a) \Rightarrow o(N(a)) > 1$

$\therefore \quad o(N(a)) = p$

But that means $Z(G) = N(a)$, a contradiction

Hence G is abelian.

Note: If $o(Z(G)) = p$, then $o\left(\frac{G}{Z(G)}\right) = \frac{p^2}{p} = p,$ a prime $\Rightarrow \frac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian.

A question arises whether group of order p^3(p = prime) is abelian? The answer is no as the Quaternion group is non-abelian and has order 2^3. Infact, there exist non-abelian groups of order p^3 for all primes p.

For example

NOTES

Let $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \begin{array}{l} a, b\ c \text{ are arbitrary} \\ \text{elements of a field } F \end{array} \right\}$

Then G is a non-abelian group of order p^3 if F is a field of order p. It is called the *Heisenberg group* over F. In general, order of the Heisenberg group over F is $(o(F))^3$.

Problem 8: *Let G be a non abelian group of order p^3. Determine $o(Z(G))$ and k = number of conjugate classes of G.*

Solution: Since G is non-abelian, $\exists\ a \in G$, s.t., $Z(G) \subsetneqq N(a) \subsetneqq G$ as in previous problems.

Now $o(Z(G)) \mid o(G) = p^3 \Rightarrow o(Z(G)) = 1, p, p^2$ or p^3

Similarly, $o(N(a)) = 1, p, p^2$ or p^3

$o(Z(G)) \neq 1$. By problem 16

$o(Z(G)) \neq p^3$ as $Z(G) \neq G$

so $o(Z(G)) = p$ or p^2

Similarly, $o(N(a)) = p$ or p^2 and as $Z(G) \subsetneqq N(a)$

We find $o(Z(G)) = p$ and $o(N(a)) = p^2$

Let now k be the total number of conjugate classes. Since

$$G = \bigcup_{a \in G} cl(a)$$

$$o(G) = \sum_{a \in G} o(cl(a)) = \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

i.e., $$p^3 = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

As number of conjugate classes when $a \in Z(G)$ is $o(Z(G)) = p$

$[a \in Z(G) \Leftrightarrow cl(a) = \{a\}$, i.e., $o(cl(a)) = 1]$

So remaining classes are $k - p$, each will have order given by

$$o(cl(a)) = \frac{o(G)}{o(N(a))} = \frac{p^3}{p^2} = p$$

Hence $p^3 = p + (k - p)p \Rightarrow k = p^2 + p - 1$.

Problem 9 : *Let G be a non-abelian group of order p^3, where p is a prime. Show that Z(G) = G′.*

Solution: Now $o(Z(G)) = p$. So $o\left(\frac{G}{Z(G)}\right) = p^2 \Rightarrow \frac{G}{Z(G)}$

NOTES

is abelian $\Rightarrow G' \subseteq Z(G) \Rightarrow G' = \{e\}$ or $Z(G)$. Since G is non-abelian, $G' = Z(G)$

In particular, $D'_8 = Z(D_8) = \{e, a^2\}$

and $G' = Z(G) = \{1, -1\}$,

where G is the quaternion group of order 8.

Problem 10: *Find all the conjugate classes of the quaternion group.*

Solution: We have the quaternion group

$$G = \{\pm 1, \pm i, \pm j, \pm k\}$$

Let us determine the conjugate class of i.

Now, in general, we know that

$< a > \subseteq N(a)$ in any group

$[x \in < a > \Rightarrow x = a^m$ and as $a.a^m = a^m.a$, we find $a^m \in N(a)]$

Thus $< i > \subseteq N(i)$ or $\{i, i^2, i^3, i^4 = 1\} \subseteq N(i)$

and, therefore, $< i > \subseteq N(i) \leq G$ gives

$4 | o(N(i)) | 8$

Again, since $j \notin N(i)$ as $ji \neq ij$

and $j \in G$,

$N(i) \subsetneq G$

Hence $o(N(i)) = 4$ or that $< i > = N(i)$

Since $o(cl(a)) = \dfrac{o(G)}{o(N(a))}$

$$o(cl(i)) = \frac{8}{4} = 2$$

$\Rightarrow cl(i) = \{i, -i\}$ as $i \in cl(i)$ always and as $-i = kik^{-1}, -i \in cl(i)$

$[kik^{-1} = ki(-k) = -(k(ik)) = -(-kki) = k^2 i = -i]$

Similarly other conjugate classes will be $\{\pm j\}$, $\{\pm k\}$, $\{1\}$ $\{-1\}$

Notice as $1, -1 \in Z(G)$ $o(cl(1)) = 1$, $o(cl(-1)) = 1$

as $o(cl(a)) = 1 \Leftrightarrow a \in Z(G)$

We can verify the class equation here

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$8 = 2 + (2 + 2 + 2)$$

Problem 11: *Let G be a group and $e \neq a \in G$ s.t., $o(a)$ = finite. Suppose. G has only two conjugate classes. Then show that G is a finite group of order* 2.

NOTES

Solution: Let $e \neq b \in G$. Since G has only 2 conjugate classes, namely $\{e\}$ and $cl(a)$. $b \in cl(a) \therefore b = g^{-1} ag$ for some $g \in G$.

$\therefore$ $o(b) = o(a)$ for all $b \neq e$ in G

Suppose $o(a) = mn$, $m > 1$, $n > 1$

Then $o(a^m) = n$

Since order of all non identity elements in G is same, $o(a^m) = mn$

$\therefore$ $n = mn \Rightarrow m = 1$; a contradiction

$\therefore$ $o(a) = p$ = prime.

$\therefore$ $o(b) = p$ for all $e \neq b \in G$

Suppose $p \neq 2$

then $a^2 \neq e \Rightarrow a^2 \in cl(a)$

$\therefore$ $a^2 = g^{-1} ag$ for some $g \in G$

$\therefore$ $(a^2)^2 = (g^{-1} ag)^2$

$= g^{-1} a^2 g$

$= g^{-1} (g^{-1} ag) g$

$= g^{-2} ag^2$

$\therefore$ $a^{2^2} = g^{-2} ag^2$

In this way, we get $a^{2^p} = g^{-p} ag^p$

Since $o(g) = o(a) = p$

$a^{2^p} = eae = a$

$\Rightarrow a^{2^p - 1} = e \Rightarrow o(a) = p \mid 2^p - 1$

By Fermat's Theorem, $p \mid 2^p - 2$

$\therefore$ $p \mid (2^p - 1) - (2^p - 2) = 1$, a contradiction

$\therefore$ $p = 2$

$\Rightarrow o(a) = 2$. So $o(b) = 2$ for all $e \neq b \in G$

$\Rightarrow G$ is abelian.

So, every conjugate class in G is of length one. Since G has only 2 classes, order of G is 2.

(**Note:** $\exists$ infinite groups in which no non-trivial element has finite order and group has only 2 conjugate classes. Therefore, it is necessary to assume that $\exists$ $e \neq a \in G$ s.t. $o(a)$ = finite, in the above problem).

Problem 12: *Prove that a group of order* 15 *is abelian. Hence, show that it is cyclic.*

NOTES

Solution: Suppose G is a group of order 15. Suppose it is non-abelian. Then $Z(G) \neq G$

$\therefore$ $o(Z(G)) = 1, 3$ or 5 as $o(Z(G)) \mid o(G) = 15$

If $o(Z(G)) = 3$ or 5, then $o\left(\frac{G}{Z}\right) = 5$ or 3 = prime

$\Rightarrow$ $\frac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian, a contradiction.

$\therefore$ $o(Z(G)) = 1$

Thus there is only one conjugate class of length one. All other classes are of length 3 or 5 as order of class divides $o(G) = 15$. If all other classes are of length 3, then by class equation,

$o(G) = 15 = 1 + 3k$, which is not true.

Therefore, there exists one class C of length 5 and this is the only class of length 5 (by class equation).

Let $x \in C$. Then $C = cl(x)$ and

$$5 = o(C) = o(cl(x)) = \frac{o(G)}{o(N(x))} \Rightarrow o(N(x)) = 3$$

Since $x \neq e$ and $x \in N(x)$, $o(x) \mid o(N(x)) = 3 \Rightarrow o(x) = 3$.

Conversely, let $o(x) = 3$. Since $o(x) \mid o(N(x))$, $o(N(x)) = 3k$ where $k = 1$ or 5 as $o(N(x)) \mid o(G) = 15$.

If $k = 5$, then $o(N(x)) = 15 = o(G) \Rightarrow N(x) = G$.

$\Rightarrow$ $x \in Z(G) \Rightarrow x = e$ as $Z(G) = \{e\}$, a contradiction

$\therefore$ $k = 1 \Rightarrow o(N(x)) = 3$

$$\Rightarrow o(cl(x)) = \frac{o(G)}{o(N(x))} = \frac{15}{3} = 5$$

$\Rightarrow$ $cl(x) = C$

as C is the only class of length 5. Since $x \in cl(x)$ we find $x \in C$.

So, the number of elements of order 3 is 5, a contradiction as number of elements of order p (p = prime) is multiple of $p - 1$ (in this case, number of elements of order 3 will be a multiple of 2)

$\therefore$ G must be abelian.

Let $e \neq x \in G$. Since $o(x) \mid o(G) = 15$, $o(x) = 3$ or 5. If all non-identity elements in G are of order 3, let $o(x) = 3$, $o(y) = 3$, $H = < x >$, $K = < y >$ then $o(H) = 3 = o(K)$. Since G is abelian, H is normal in G, K is normal in $G \Rightarrow HK \leq G$ $\Rightarrow$ $o(HK) \mid o(G) = 15$.

But $o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = \frac{3 \times 3}{1} = 9$ and $9 \nmid 15$

we get a contradiction

$\therefore$ $\exists\, a \in G$ s.t. $o(a) = 5$. By the same argument as above $\exists\, b \in G$, s.t. $o(b) = 3$. Since $ab = ba$, $o(a)$ and $o(b)$ are relatively prime.

$$o(ab) = o(a)\, o(b)$$
$$= 3 \times 5 = 15$$
$$= o(G)$$

$\therefore$ G is cyclic group of order 15.

(**Note :** We shall prove the above result again with the help of Sylow's Theorems in the next chapter).

Definition: Let $H \leq G$. Let $g \in G$. Then $g^{-1} Hg$ is called conjugate of H in G. The set $\{g^{-1} Hg \mid g \in G\} = cl(H)$ is called *conjugate class* of H in G. As before, we can determine the order of this conjugate class.

Theorem 2: *Let $H \leq G$, G = finite group.*

Then $o(cl(H)) = \frac{o(G)}{o(N(H))}$.

Proof: Since $N(H) \leq G$

$$G = \bigcup_{i=1}^{t} N(H)x_i$$

where $N(H)\, x_i \cap N(H)\, x_j = \varphi$ for some $i \neq j$

Let $S = \{x_1^{-1} Hx_1, \ldots, x_t^{-1} Hx_t\}$

We show that $S = cl(H)$

Let $g^{-1} Hg \in cl(H)$, $g \in G$

$g \in G \Rightarrow g \in N(H)x_i$ for some i

$\Rightarrow g = yx_i$, $y \in N(H)$

$\Rightarrow g^{-1} Hg = x_i^{-1} y^{-1} Hyx_i$

$= x_i^{-1} Hx_i$ as $y \in N(H) \Rightarrow y^{-1} Hy = H$

$\Rightarrow g^{-1} Hg \in S$

$\therefore$ $cl(H) \subseteq S$

Clearly, $S \subseteq cl(H)$

$\therefore$ $S = cl(H)$.

Also $x_i^{-1} Hx_i = x_j^{-1} Hx_j$

$\Rightarrow x_i\, x_j^{-1} H = Hx_i\, x_j^{-1}$

NOTES

NOTES

$$\Rightarrow x_i x_j^{-1} \in N(H)$$
$$\Rightarrow N(H)x_i = N(H)x_j$$
$$\Rightarrow i = j$$

$\therefore$ $o(S) = t$

$$\Rightarrow o(cl(H)) = t = \frac{o(G)}{o(N(H))}.$$

Problem 13: Let $H \neq G$ *be a subgroup of a finite group G. Show that G cannot be expressed as union of conjugates of H.*

Solution: The number of conjugates of H in G is given by $\frac{o(G)}{o(N(H))}$

So $$o(\cup x^{-1}Hx) \leq \frac{o(G)}{o(N(H))}(o(H)-1)+1$$

$$\leq \frac{o(G)}{o(H)}(o(H)-1)+1 \text{ as } H \leq N(H)$$

$$= o(G) - \frac{o(G)}{o(H)} + 1$$

$$\leq o(G) - 2 + 1 \qquad as \frac{o(G)}{o(H)} \geq 2$$

$$= o(G) - 1 < o(G)$$

Thus, G cannot be written as union of conjugates of H.

Check Your Progress

1. What is conjugate class?
2. What relation divides a group G into disjoint equivalence classes?
3. What is a normalizer of an element of a group G?

5.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. Let *cl(a)* denote the equivalence class of *a* in *G* then *cl(a)* is called conjugate class.
2. Conjugate relation.
3. Normalizer of an element $a \in G$ is defined as $N(a) = \{ x \in G \mid xa$ for all $x \in G\}$.

5.5 SUMMARY

- Let G be a group, $a, b \in G$. Then a conjugate relation $\sim$ on G is defined as $a \sim b \Leftrightarrow \exists\ c \in G$ s.t. $a = c^{-1}\ bc$.
- Conjugate relation is equivalent on G.
- Let $cl(a)$ denote the equivalence class of a in G then $cl(a)$ is called conjugate class.
- Normalizer of an element $a \ G$ is defined as $N(a) = \{ x \in G \mid xa$ for all $x \in G\}$. Also $N(a) \leq G$, *then* $N(a) = G \Leftrightarrow a \in Z(G)$.

NOTES

5.6 KEY WORDS

- **Conjugate:** A mathematical value or entity having a reciprocal relation with another.
- **Equivalence relation:** A relation $\sim$ on a set is called an equivalence relation if it's reflexive, symmetric and transitive.
- **Finite group:** A finite group is a mathematical group with a finite number of elements.

5.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Define conjugate relation.
2. Show that of if $a \in Z(G)$ and $x \in cl(a)$ be any element, then $x = y^{-1}ay$ for some $y \in G$.
3. If $a \in G$ and $N(a) \leq G$, *then show that* $N(a) = G \Leftrightarrow a \in Z(G)$.
4. What is conjugate class?

Long Answer Questions

1. Prove that a group of order p^2 (p = prime) is abelian.
2. Find all the conjugate classes of the quaternion group.
3. Drive the class equation of G.
4. If $H \neq G$ be a subgroup of a finite group G, then show that G cannot be expressed as union of conjugates of H.

5.8 FURTHER READINGS

NOTES

Herstein, I.N. 2006. *TOPICS IN ALGEBRA, 2ND ED*. New Jersey: John Wiley & Sons.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

UNIT 6 SYLOW'S THEOREM

NOTES

Structure

6.0 INTRODUCTION

This unit discusses about p-groups, Sylow's three theorems and their applications. In the field of finite group theory, the Sylow theorems are a collection of theorems named after the Norwegian mathematician Ludwig Sylow. They provide a detailed information about the number of subgroups of fixed order that a given finite group contains. These theorems are a fundamental part of finite group theory and have very important applications in the classification of finite simple groups. The ideas developed are so useful that the plenty can be known about the nature of a group by knowing only its order. Direct products of groups with its applications are taken up at the end of the unit.

6.1 OBJECTIVES

After going through this unit, you will be able to:

- State Sylow's Theorem and learn its applications
- Learn the Direct Products of groups and its applications
- Solve related problems

6.2 SYLOW'S THEOREM

Definition: A p-group is a group in which every element has order p^r where p = prime. Here p is same for all elements and r may vary.

The group $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ and the Quaternion group are examples of finite p-groups. Here $p = 2$.

S_3 is not a p-group.

NOTES

Theorem 1: *Let G be a finite group. Then G is a p-group if and only if* $o(G) = p^n$.

Proof: Suppose G is a p-group. Let q be a prime dividing $o(G)$. By Cauchy's theorem $\exists\ x \in G$ s.t. $o(x) = q$. But $o(x) = p^r$ as G is a p-group.

$\therefore\ q = p^r \Rightarrow q = p$. So, p is the only prime dividing $o(G)$. Thus $o(G) = p^n$.

Conversely, let $o(G) = p^n$ (p = prime).

Let $x \in G$. Then $o(x) \mid o(G) = p^n \Rightarrow o(x) = p^r$.

$\therefore$ every element of G has order which is some power of p. So, G is a p-group.

Remarks:

(*i*) Any finite p-group has non-trivial centre.

(*ii*) A p-group may or may not be abelian.

Problem 1: *Let G be a finite group such that for every pair a, b of non-identity elements of G there exists T ∈ Aut G such that T(a) = b. Show that G is abelian.*

Solution: Let $e \neq a, b \in G$. By hypothesis $T(a) = b$ for some $T \in$ Aut G. So $o(T(a)) = o(a) \Rightarrow o(a) = o(b)$.

$\Rightarrow$ every non-identity element of G has same order n. every non-identity element of G has order prime $p \Rightarrow G$ is a p-group.

$\Rightarrow\ Z(G) \neq \{e\} \Rightarrow e \neq a \in Z(G)$. Let x be any element of G. Then $\exists\ T \in$ Aut G such that $T(a) = x$. Since $T(Z(G)) \subseteq Z(G) \Rightarrow x = T(a) \in Z(G) \Rightarrow G \subseteq Z(G)$.

$\Rightarrow\ G = Z(G) \Rightarrow G$ is abelian.

Problem 2: *Let G be a finite cyclic p-group. Show that if H and K be any two subgroups of G then either* $H \subseteq K$ *or* $K \subseteq H$.

Solution: Let $G = < a >$, then $o(G) = o(a) = p^n$ for some prime p.

Let H be a subgroup of G, then H is cyclic.

Let $H = < a^m >$.

Let d = g.c.d. (m, p^n)

Then $d = mx + p^n y$ for some integers x and y

Now $a^d = a^{mx+p^n y} = a^{mx} \cdot a^{p^n y} = (a^m)^x \in H$ [as $o(a) = p^n$]

Thus $< a^d > \subseteq H$

Again as $d \mid m, \quad m = dq$

So $a^m = (a^d)^q \in < a^d >$

or that $H = < a^m > \subseteq < a^d >$

and hence $H = < a^d >$ where $d \mid p^n$

and so $H = \langle a^{p^i} \rangle$

Let K be another subgroup of G, then $K = \langle a^{p^k} \rangle$. Suppose $i \geq k$ and let $i = k + t$

where $t \geq 0$ is an integer

Now $a^{p^i} = a^{p^{k+t}} = (a^{p^k})^{p^t} \in K$

which implies $H = \langle a^{p^i} \rangle \subseteq K$

If $k \geq i$, then $K \subseteq H$

which proves the result.

Problem 3: *If G is a finite non abelian p-group then show that* $p^2 \mid o(\text{Aut } G)$

Solution: Since G is a p-group. $o(Z(G)) > 1$

Suppose $o(G) = p^n$ and let $o(Z(G)) = p^m$

Since G is non abelian, $o(Z(G)) < o(G)$, thus $m < n$ and also $m \geq 1$.

Thus $o\left(\frac{G}{Z(G)}\right) = p^{n-m}, \quad n - m \geq 1$

If $n - m = 1$ then $o\left(\frac{G}{Z(G)}\right) = p \Rightarrow \frac{G}{Z(G)}$ is cyclic.

$\Rightarrow G$ is abelian

which is not true. Hence $n - m \geq 2$

Again $\frac{G}{Z(G)} \cong I(G) \Rightarrow o\left(\frac{G}{Z(G)}\right) = o(I(G))$

$\Rightarrow p^2$ divides $o(I(G))$

and as $I(G) \leq \text{Aut } G$ we find $p^2 \mid o(\text{Aut } G)$.

We now prove the converse of Lagrange's Theorem for finite abelian groups.

Theorem 2: *Let G be an abelian group of order n. Then for every divisor m of n, G has a subgroup of order m.*

Proof: We prove the result by induction on n. When $n = 1$, $G = \{e\}$ and so result is clearly true for $n = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $o(G) = n$, $m \mid n$, $m > 1$. Let p be a prime dividing m. So, $p \mid n = o(G)$. By Cauchy's Theorem $\exists\ x \in G$ s.t. $o(x) = p$. Let $K = < x >$.

Then $o(K) = o(x) = p$. Since G is abelian, K is normal in G.

Now $o\left(\frac{G}{K}\right) = \frac{n}{p} < n$. Also $\frac{G}{K}$ is abelian. Let $m = pm_1$.

NOTES

NOTES

Now $m = pm_1 \mid o(G) = o\left(\frac{G}{K}\right) o(K)$

$\Rightarrow m_1 \mid o\left(\frac{G}{K}\right)$

By induction hypothesis $\exists$ subgroup $\frac{H}{K}$ of $\frac{G}{K}$ s.t. $o\left(\frac{H}{K}\right) = m_1$. $H \leq G$.

$\therefore \quad o(H) = o(K)m_1 = pm_1 = m$

So, result is true in this case also. Hence by induction, theorem is proved.

Cor. : Converse of Lagrange's theorem holds in finite cyclic groups.

Remark: In case of finite cyclic groups we notice its not only that converse of Lagrange's theorem holds but for each divisor of $o(G)$ there exists a unique subgroup. This is, however, not essentially true in finite abelian groups. For instance, in $K_4 = \{e, a, b, c\}$ there are three subgroups of order 2.

Sylow *p*-subgroups

Let p be a prime s.t. p^n divides order of a group G and p^{n+1} does not divide it. Then a subgroup H of G s.t. $o(H) = p^n$ is called a Sylow p-subgroup of G or p-Sylow subgroup of G.

We now discuss three theorems due to Sylow called Sylow's theorems. First theorem shows the existence of a Sylow p-subgroup of G for every prime p dividing $o(G)$ while second theorem shows that any two Sylow p-subgroups of G are conjugate. The third theorem gives the number of Sylow p-subgroups of G.

Our next theorem is a partial converse to Lagrange's theorem.

Theorem 3 (Sylow's First Theorem): *Let p be a prime and m, a +ve integer s.t. p^m divides o(G). Then $\exists$ a subgroup H of G s.t. $o(H) = p^m$.*

Proof: We prove the theorem by induction on $o(G)$. Result is vacuously true when $o(G) = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $p^m \mid o(G)$. If K is a subgroup of G s.t. $K \neq G$ and $p^m \mid o(K)$, then by induction $\exists\ H \leq K$ s.t., $o(H) = p^m$. $H \leq K \Rightarrow H \leq G$. So result holds in this case. Assume p^m does not divide order of any proper subgroup of G. Consider class equation of G.

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$a \notin Z(G) \Rightarrow N(a) \neq G \Rightarrow p^m \nmid o(N(a))$$

But $\quad p^m \mid o(G) \Rightarrow p^m \mid \frac{o(G)}{o(N(a))}$. $o(N(a))$

NOTES

$\Rightarrow \quad p \mid \dfrac{o(G)}{o(N(a))}$ for all $a \notin Z(G)$) as $p^m \nmid o(N(a))$

$\Rightarrow \quad p \mid \sum_{a \notin Z(G)} \dfrac{o(G)}{o(N(a))}$

$\Rightarrow \quad p \mid o(G) - \sum_{a \notin Z(G)} \dfrac{o(G)}{o(N(a))} = o(Z(G))$

$\Rightarrow \exists\ x \in Z(G)$ s.t. $o(x) = p$

Let $K = \langle x \rangle \subseteq Z(G) \quad \Rightarrow K$ is normal in G.

Now $o(G/K) < o(G)$ and $p^m \mid o(G) = o(G/K).\ o(K)$, $p^m \nmid o(K)$ and thus $p^{m-1} \mid p^m \mid o(G/K)$. (Notice in case $m = 1$, the result follows by Cauchy's theorem).

By induction hypothesis $\exists$ a subgroup $\dfrac{H}{K}$ of $\dfrac{G}{K}$ s.t. $o\left(\dfrac{H}{K}\right) = p^{m-1}$.

$\therefore \qquad o(H) = p^m,\ \dfrac{H}{K} \leq \dfrac{G}{K} \Rightarrow H \leq G$

Thus result is true in this case also.

Hence by induction the theorem follows.

Remark: Suppose G is a group of order $2^3.3^2.5$ then Sylow's First theorem says that G has at least one subgroup each of order 2, 2^2, 2^3, 3, 3^2, 5. But the theorem does not say anything about the group G having a subgroup of order 6, 10, 15 or any other divisor of $o(G)$ that has two or more distinct prime factors.

In view of theorems 2 and 3 above we observe that converse of Lagrange's theorem holds for all finite abelian groups and all finite groups of prime-power order.

Cor.: If p is a prime s.t. $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$, then a $\exists$ Sylow p-subgroup of G.

Proof: Take $m = n$ and use the above theorem.

Thus if $o(G) = 2^3.3^2.5$, any subgroup of order 8 will be a Sylow 2-subgroup and any subgroup of order 9 will be a sylow 3-subgroup of G and so on.

Remark: Sometimes the statement of this corollary is taken as Sylow's first theorem. In fact, another (more general) version of the theorem would be

If G a finite group of order $n = p^k q$ ($k \geq 1$), where p is a prime and q, a +ve integer, (p, q relatively prime) then for each i, $1 \leq i \leq k$, G has a subgroup of order p^i.

NOTES

Double Cosets

Definition: Let $H, K \leq G$. Let $a, b \in G$. Define a relation '$\sim$' on G as follows:

$$a \sim b \Leftrightarrow \exists\ h \in H,\ k \in K \text{ s.t. } a = hbk$$

It can be easily shown that '$\sim$' is an equivalence relation on G. So, it divides G into disjoint union of equivalence classes. Equivalence class of $a \in G$ is given by

$$\begin{aligned} cl(a) &= \{x \in G \mid a \sim x\} \\ &= \{hak \mid h \in H,\ k \in K\} \\ &= HaK, \text{ called double coset of } H \text{ and } K \text{ in } G. \end{aligned}$$

$$G = \bigcup_a cl(a) = \bigcup_a Hak$$

Define $f : HaK \to HaKa^{-1}$ s.t.,

$f(hak) = haka^{-1}$ for all $h \in H,\ k \in K$

Clearly, f is well defined as $hak = h'ak'$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

f is 1–1 as $f(hak) = f(h'ak')$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

$$\Rightarrow hak = h'ak'$$

Let $haka^{-1} \in HaKa^{-1} \Rightarrow hak \in Hak$ and

$f(hak) = haka^{-1}$

$\therefore$ f is both 1–1 and onto.

Thus, $o(Hak) = o(HaKa^{-1})$, (if H, K are finite)

$$= \frac{o(H)\, o(aKa^{-1})}{o(H \cap aKa^{-1})} = \frac{o(H)\, o(K)}{o(H \cap aKa^{-1})}$$

If G is a finite group, then

$$o(G) = \sum_a o(HaK) = \sum_a \frac{o(H)o(K)}{o(H \cap aKa^{-1})}$$

We are now ready to prove Sylow's second theorem.

Theorem 4 (Sylow's Second theorem): *Any two Sylow p-subgroups of a finite group G are conjugate in G.*

Proof: Let P, Q be Sylow p-subgroups of G. Let $o(P) = p^n = o(Q)$ where $p^{n+1} \nmid o(G)$. Suppose P and Q are not conjugate in G.

i.e., $P \neq gQg^{-1}$ for any $g \in G$

By the discussion done above

$$o(PxQ) = \frac{o(P)\,o(Q)}{o(P \cap xQx^{-1})}$$

Since, $P \cap xQx^{-1} \leq P$

$o(P \cap xQx^{-1}) = p^m$, $m \leq n$

If $m = n$, then $P \cap xQx^{-1} = P$

$\Rightarrow P \subseteq xQx^{-1}$

$\Rightarrow P = xQx^{-1}$ as $o(xQx^{-1}) = o(Q) = o(P)$

which is a contradiction.

$\therefore$ $m < n$ and thus $o(PxQ) = p^{2n-m}$, $m < n$ for all $x \in G$

$\Rightarrow o(PxQ) = p^{n+1}\,(p^{n-m+1})$ = multiple of p^{n+1}

Thus $o(G) = \sum_x o(PxQ)$ = multiple of p^{n+1}

p^{n+1} | R.H.S. $\Rightarrow p^{n+1} \mid o(G)$, a contradiction

$\therefore$ $P = gQg^{-1}$ for some $g \in G$.

Before we prove Sylow's third theorem, we prove

Lemma: *Let P be a Sylow p-subgroup of G. Then the number of Sylow p-subgroups of G is equal to* $\frac{o(G)}{o(N(P))}$.

Proof: We know that

$$o(cl(P)) = \frac{o(G)}{o(N(P))}$$

Since $cl(P) = \{Q \mid Q \leq G,\ Q = gPg^{-1},\ g \in G\}$

= set of all Sylow p-subgroups of G,

the number of Sylow p-subgroups of G is $\frac{o(G)}{o(N(P))}$.

Theorem 5 (Sylow's Third Theorem): *The number of Sylow p-subgroups of G is of the form* $1 + kp$ *where* $(1 + kp) \mid o(G)$, *k being a non-negative integer.*

Proof: Let P be a Sylow p-subgroup of G.

Let $o(P) = p^n$. Now $G = \bigcup_x PxP$

$$= \bigcup_{x \in N(P)} PxP \cup \bigcup_{x \notin N(P)} PxP$$

$x \in N(P) \Rightarrow Px = xP \quad \Rightarrow PPx = PxP$

$\Rightarrow Px = PxP$

NOTES

$$\therefore \quad \underset{x\in N(P)}{\cup} PxP = \underset{x\in N(P)}{\cup} Px = N(P)$$

as $P \le N(P)$ and union of disjoint right cosets equals the set

$$x \notin N(P) \quad \Rightarrow Px \neq xP \Rightarrow xPx^{-1} \neq P$$

$$\Rightarrow o(P \cap xPx^{-1}) = p^m,\ m < n$$

(as in Sylow's second theorem)

$$\Rightarrow o(PxP) = P^{2n-m}, \quad m < n$$

$$\therefore \quad o(G) = o(N(P)) + \sum_{x\notin N(P)} o(PxP)$$

$$= o(N(P)) + \sum_{x\notin N(P)} p^{2n-m}$$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \sum \frac{p^{2n-m}}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))}, \quad t = \text{integer}$$

Since L.H.S. = integer, $p^{n+1}\ \dfrac{t}{o(N(P))} = r = \text{integer}$

$$\therefore \quad p^{n+1}t = r.o(N(P))$$

Again as $P \le N(P)$

$o(P) \mid o(N(P))$

$\Rightarrow p^n \mid o(N(P))$

$\Rightarrow o(N(P)) = p^n u$

$P^{n+1}t = r\ o(N(P))$

$\Rightarrow pt = r.u$

$\Rightarrow p \mid ru$

If $p \mid u$ then $p^{n+1} \mid o(N(P)) \mid o(G) \Rightarrow p^{n+1} \mid o(G)$, a contradiction.

$\therefore\ p \mid r \Rightarrow \dfrac{r}{p} = \text{integer} \Rightarrow \dfrac{t}{u} = \text{integer } k = \dfrac{r}{p}.$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))} = 1 + p\frac{t}{u} = 1 + kp$$

By above lemma, $\dfrac{o(G)}{o(N(P))}$ = number of Sylow p-subgroups of G.

$\therefore$ The number of Sylow p-subgroups is of the form $1 + kp = \dfrac{o(G)}{o(N(P))}$

$\Rightarrow (1 + kp) \mid o(G)$.

This proves the theorem.

Note: If $o(G) = p^n q$, $(p, q) = 1$ then the number of Sylow p-subgroups is

$$1 + kp, \text{ where } (1 + kp) \mid p^n q$$

$$\Rightarrow (1 + kp) \mid q \text{ as } (1 + kp, p^n) = 1$$

NOTES

Cor.: If P is the only Sylow p-subgroups of G, then P is normal in G and conversely.

Proof: By Sylow's third theorem

$$\frac{o(G)}{o(N(P))} = 1 \Rightarrow o(G) = o(N(P))$$

Since $N(P) \leq G$

$N(P) = G$

$\Rightarrow P$ is normal in G.

Conversely, if Sylow p-subgroup P is normal in G, then

$$N(P) = G \quad \Rightarrow o(N(P)) = o(G)$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1$$

$\Rightarrow$ The number of Sylow p-subgroups of G is 1

$\Rightarrow P$ is the only Sylow p-subgroup of G.

Lemma: *Let P be a Sylow p-subgroup of G. Let* $x \in N(P)$ *s.t.* $o(x) = p^i$. *Then* $x \in P$.

Proof: Let $o(P) = p^n, \quad p^{n+1} \nmid o(G)$

Now $(Px)^{p^i} = Px^{p^i} = Pe = P$

[P is normal in $N(P)$ and $x \in N(P)$]

$\Rightarrow o(Px) \mid p^i$

$\Rightarrow o(Px) = p^j, j \geq o$

Let $j > 0$. $\bar{K} = < Px > \leq \frac{N(P)}{P}$ s.t. $o(\bar{K}) = p^j$

Since $(\bar{K}) \leq \frac{N(P)}{P}$, $\bar{K} = \frac{K}{P}$ where $K \leq N(P)$

$$p^j = o(\bar{K}) = \frac{o(K)}{o(P)} = \frac{o(K)}{p^n}$$

$\Rightarrow o(K) = p^{n+j}, \ j > 0$

But $o(K) \mid o(N(P)) \mid o(G)$

$\Rightarrow p^{n+j} \mid o(G), \ j > 0$, a contradiction

$\therefore\ j = 0 \qquad o(Px) = p^j = 1$

$\Rightarrow\ Px = P \Rightarrow x \in P.$

Theorem 6: *Every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

NOTES

Proof: Let $H \leq G$ s.t. $o(H) = p^m$ i.e. H is a p-subgroup of G.

Let S = set of all Sylow p-subgroups of G.

Then $o(S) = 1 + kp$

Define a relation $\sim$ on S as follows:

For $P_1, P_2 \in S$, let $P_1 \sim P_2 \Leftrightarrow \exists\ x \in H$ s.t. $P_1 = xP_2x^{-1}$. It can be shown that $\sim$ is an equivalence relation on S. For $P \in S$ equivalence class of P in S is given by $cl(P) = \{xPx^{-1} \mid x \in H\}$.

If $N_H(P) = \{x \in H \mid xP = Px\}$ then $N_H(P) \leq H$.

Thus $$o(cl(P)) = \frac{o(H)}{o(N_H(P))}\ p^s,\ s \geq 0.$$

Suppose H is not contained in any Sylow p-subgroup of G. Then $H \not\subseteq P$.

$\therefore\ \exists$ some $x \in H$ s.t. $x \notin P$

If $xPx^{-1} = P$, then $x \in N(P)$ and $o(x) = p^i$ [as $x \in H$, $o(x) \mid o(H)$]

$\Rightarrow\ x \in P$ by above lemma, which is not true

Hence $xPx^{-1} \neq P,\ x \in H$

$\Rightarrow\ P, xPx^{-1}$ are distinct members of $cl(P) \Rightarrow o(cl(P)) > 1$

$\therefore\ o(cl(P)) = p^s, s > 0 \quad \Rightarrow o(cl(P))$ = multiple of p

This is true for all $P \in S$

Since $S = \cup\ cl(P)$

$$o(S) = \sum o(cl(P)) = \text{a multiple of } p$$

$\Rightarrow\ 1 + kp$ = a multiple of p, a contradiction.

Hence H is contained in some Sylow p-subgroup of G.

Problem 4: *Show that the number of Sylow p-subgroups of S_p, where p is a prime, is (p – 2)!*

Solution: Now $o(S_p) = p!$

The order of Sylow p-subgroup is p as p^2 does not divide $p!$

Let $f = (1\ 2\ 3\ \ldots\ p)$. Then $0(f) = p$ and $0(\langle f \rangle) = p$. Any cycle of length p in S_p generates a group of order p. The number of cycles of length p is $(p - 1)!$

Since any element other than identity in a group of order p is of order p and generates the same group of order p.

The number of Sylow p-subgroups of S_p is $\frac{(p-1)!}{p-1} = (p-2)!$

For example, in S_5, <(1 2 3 4 5)>, <(2 1 3 4 5)>, <(2 3 1 4 5)>, <(2 3 4 1 5)>, <(2 3 5 4 1)>, <(1 3 2 4 5)> are 6 Sylow 5-subgroups of order 5 in S_5.

NOTES

Problem 5: *Show that all Sylow p-subgroups of G are isomorphic.*

Solution: Let P and Q be two Sylow p-subgroups of G. Then $Q = x^{-1} Px$ for some $x \in G$.

Define $\theta : P \to Q$ s.t.,

$$\theta(p) = x^{-1}px, \quad p \in P.$$

Then θ is an isomorphism. So $P \cong Q$.

Problem 6: *Let* $o(G) = 30$. *Show that*

(*i*) *Either Sylow* 3*-subgroup or Sylow* 5*-subgroup is normal in G.*

(*ii*) *G has a normal subgroup of order* 15.

(*iii*) *Both Sylow* 3*-subgroup and Sylow* 5*-subgroup are normal in G.*

Solution: $o(G) = 30 = 2 \times 3 \times 5$

The number of Sylow 3-subgroups is $1 + 3k$ and $(1 + 3k) \mid 10 \Rightarrow k = 0$ or 3

If $k = 0$, then Sylow 3-subgroup is normal.

Let $k \neq 0$, then $k = 3$. This gives 10 Sylow 3-subgroups H_i each of order 3 and so we have 20 elements of order 3. [Notice (for $i \neq j$) $o(H_i \cap H_j) \mid o(H_i) = 3 \Rightarrow o(H_i \cap H_j) = 1$ only and so these 20 elements are different. Each H_i has one element e of order 1 and other two of order 3. $a \in H_i \Rightarrow o(a) \mid o(H_i) = 3 \Rightarrow o(a) = 1, 3$].

The number of Sylow 5-subgroups is $1 + 5k'$ and $(1 + 5k') \mid 6 \Rightarrow k' = 0$ or 1.

If $k' = 0$. Then Sylow 5-subgroup is normal.

Let $k' \neq 0$. Then $k' = 1$. This gives 6 Sylow 5 subgroups each of order 5 and we get 24 elements of order 5. But we have already counted 20 elements of order 3. Thus we have more than 44 elements in G, a contradiction. So,. either $k = 0$ or $k' = 0$.

i.e., either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

Which proves (*i*).

Let H be a Sylow 3-subgroup of order 3 and K, a Sylow 5-subgroup of order 5.

By (*i*), either H is normal in G or K is normal in G.

In any case, $HK \leq G$, $o(HK) = 15$ as $o(H \cap K)$ divides $o(H) = 3$ and $o(K) = 5 \Rightarrow o(H \cap K) = 1$. Since index of HK in G is 2, HK is normal in G. This proves (*ii*).

NOTES

Suppose, H is normal in G, K is not normal in G. By (i) G has 6 Sylow 5-subgroups and so 24 elements of order 5. But $o(HK) = 15 \Rightarrow HK$ is cyclic (*See problem* 13 *ahead*) $\Rightarrow HK$ has $\varphi(15) = 8$ elements of order 15. Thus G has $24 + 8 = 32$ elements, a contradiction.

$\therefore$ K is normal in G.

If H is not normal in G, they by (i), G has 10 Sylow 3-subgroups and so 20 elements of order 3. From above HK has 8 elements of order 15 and K has 4 elements of order 5. This gives $20 + 8 + 4 = 32$ elements in G, a contradiction.

$\therefore$ H is normal in G. So both H and K are normal in G.

This proves (*iii*).

Problem 7: *Let $o(G) = pq$, where p, q are distinct primes, $p < q$, $p \nmid q - 1$. Show that G is cyclic.*

Solution: The number of Sylow p-subgroups is $1 + kp$ and $(1 + kp) \mid q \Rightarrow 1 + kp = 1$ or q, $1 + kp = 1 \Rightarrow$ Sylow p-subgroup is unique $\Rightarrow$ Sylow p-subgroup H is normal in G.

$1 + kp = q \Rightarrow kp = q - 1 \Rightarrow p \mid q - 1$, a contradiction.

Thus $1 + kp \neq q$ and so Sylow p-subgroup is normal.

The number of Sylow q-subgroups is $1 + k'q$ and $(1 + k'q) \mid p \Rightarrow 1 + k'q = 1$ or p

If $1 + k'q = p$, then $k'q = p - 1 \Rightarrow q \mid p - 1 \Rightarrow q \leq p - 1 < p$, a contradiction. $1 + k'q = 1 \Rightarrow$ Sylow q-subgroup K is normal in G.

$o(H) = p$, $o(K) = q$, $H \cap K = \{e\}$, H is normal is G, K is normal in G.

$[x \in H \cap K \Rightarrow o(x) \mid o(H),\ o(x) \mid o(K) \Rightarrow o(x) = 1]$

Thus $hk = kh$ for all $h \in H$, $k \in K$

Let $H = \langle a \rangle$, $K = \langle b \rangle$ (Groups of prime order are cyclic)

$o(a) = o(H) = p$, $o(b) = o(K) = q$

Now $ab = ba$, $(o(a), o(b)) = (p, q) = 1$

$o(ab) = a(a)\ o(b) = pq = o(G)$

$\Rightarrow$ G is cyclic.

Problem 8: (Wilson's Theorem): *Using Sylow's theorems show that* $(p - 1)! \equiv -1 (mod\ p)$ *for any prime p.*

Solution: Consider S_p, then order of S_p is $p(p - 1)(p - 2) \ldots 2.1$

The number of Sylow p-subgroups of order p in S_p are of the form $1 + kp$, where k is a non -ve integer. Since each Sylow p-subgroup is of order p, we get $(p - 1)$ elements of order p. Again, any two groups of order p have only identity in common and thus the number of elements of order p in S_p is $(1 + kp)(p - 1)$. Also any element of order p in S_p is a cycle of length p and the number of cycles of length p in S_p is $(p - 1)!$

So $(1 + kp)(p - 1) = (p - 1)!$

i.e., $(p - 1)! \equiv -1 (\text{mod } p)$.

Problem 9: *Let p be a prime dividing* $o(G)$ *and* $(ab)^p = a^p b^p$ *for all* $a, b \in G$. *Show that*

(*i*) *Sylow p-subgroup P is normal in G.*

(*ii*) $\exists$ *a normal subgroup N of G s.t.*

$P \cap N = \{e\}$ *and* $G = PN$

(*iii*) *G has non-trivial centre.*

Solution: Let $p^n \mid o(G), p^{n+1} \nmid o(G)$

Let $H = \{x \in G \mid x^{p^n} = e\}$

$H \neq \varphi$ as $e^{p^n} = e \Rightarrow e \in H$

Let $x, y \in H \Rightarrow (xy^{-1})^{p^n} = x^{p^n} (y^{-1})^{p^n} = e.e = e$

$\Rightarrow xy^{-1} \in H$

$H \leq G$

Let q be a prime dividing $o(H)$.

Then $x \in H$ s.t. $o(x) = q$

But $x \in H \Rightarrow o(x) \mid p^n \Rightarrow q \mid p^n \Rightarrow q = p$

$\therefore$ H is a p-group. $o(H) = p^m$, $m \leq n$.

Let P be a Sylow p-subgroup of G.

Then $o(P) = p^n$. Let $x \in P \Rightarrow x^{p^n} = e$

$\Rightarrow x \in H \Rightarrow P \subseteq H \Rightarrow o(P) \mid o(H) \Rightarrow p^n \mid p^m \Rightarrow n \leq m \ \therefore \ m = n$

So, $o(H) = p^n = o(P)$

$\Rightarrow H = P$.

Thus H is the only Sylow p-subgroup of G and so is normal in G.

This proves (*i*)

Define $\theta : G \to G$ s.t.

$\theta(x) = x^{p^n}$

Then θ is a homomorphism.

$\Rightarrow \dfrac{G}{\text{Ker } \theta} \cong ImG$ is normal in G $[\theta(G) = ImG]$

Since $x \in \text{Ker } \theta \Leftrightarrow \theta(x) = e$

$\Leftrightarrow x^{p^n} = e$

NOTES

NOTES

$\Leftrightarrow x \in H = P$

$P = \text{Ker } \theta$

Let $N = ImG$ which is normal in G.

(as $\theta(x) \in N$, $g \in G \Rightarrow g^{-1}\theta(x)g = g^{-1}x^{p^n} g$

$= (g^{-1}xg)^{p^n} = \theta(g^{-1}xg) \in N$)

Let $x \in P \cap N \Rightarrow x \in P, x \in N$

$\Rightarrow x^{p^n} = e, \; x = \theta(y) = y^{p^n}$

$\Rightarrow y^{p^{2n}} = e \Rightarrow o(y) = p^r, r \leq n$

as $p^{n+1} \nmid o(G)$

we get $y^{p^r} = e, \; r \leq n$

$\Rightarrow y^{p^n} = (y^{p^r})^{p^{n-r}} = e \Rightarrow x = e$

$\Rightarrow P \cap N = \{e\}$

Also $\frac{G}{P} \cong N \Rightarrow \frac{o(G)}{o(P)} = o(N)$

$\Rightarrow o(G) = o(P).\, o(N)$

But $o(PN) = o(P)\, o(N)$

$\Rightarrow o(G) = o(PN)$

$\Rightarrow PN = G$

This proves (*ii*).

Let $z \in Z(P), z \neq e$. Let $g \in G$.

Since $G = PN$, $g = xy, x \in P, y \in N$

Also P is normal in G, N is normal in G, $P \cap N = \{e\}$

$\Rightarrow x'y' = y'x'$ for all $x' \in P, y' \in N$

Now $zg = z(xy) = (zx)y$

$= (xz)y$ as $z \in Z(P)$

$= x(zy) = x(yz)$ as $z \in P, y \in N$

$= (xy)z = gz$ for all $g \in G$

$\therefore \quad z \in Z(G)$

$\therefore \quad Z(G) \neq \{e\}$

which proves (*iii*).

NOTES

Problem 10: *Show that there is no simple group of order* 144.

Proof: Let G be a group of order $144 = 2^4 \times 3^2$, and suppose G is simple.

The number of Sylow 3-subgroups of G is $1 + 3k$ and $(1 + 3k) \mid 16 \Rightarrow k =$ 0, 1, 5. If $k = 0$, then Sylow 3-subgroup is unique and normal, which is not possible.

If $k = 1$, then $\exists$ 4 Sylow 3-subgroups of G and if P is any one of these then as $\frac{o(G)}{o(N(P))} = 4 =$ number of Sylow 3-subgroups, we find $N(P)$ is a subgroup of G with index 4 which is not possible in view of problem 20 above.

If $k = 5$, then $\exists$ 16 Sylow 3-subgroups each of order 9 in G. Let H_1, H_2, be any Sylow 3-subgroups. Since $H_1 \cap H_2 \leq H_1$, $o(H_1 \cap H_2) \mid 9 \Rightarrow o(H_1 \cap H_2) = 1$, 3 or 9. If $o(H_1 \cap H_2) = 9$, then $o(H_1 \cap H_2) = o(H_1) = o(H_2), \Rightarrow H_1 = H_1 \cap H_2 = H_2$, a contradiction. If $o(H_1 \cap H_2) = 3$, then $H_1 \cap H_2$ is normal in H_1 and H_2. Since $N(H_1 \cap H_2)$ is the largest subgroup of G in which $H_1 \cap H_2$ is normal.

$$H_1 \subseteq N(H_1 \cap H_2), \quad H_2 \subseteq N(H_1 \cap H_2)$$
$$\Rightarrow H_1H_2 \subseteq N(H_1 \cap H_2) \subseteq G$$

Again as $$o(H_1H_2) = \frac{o(H_1)\, o(H_2)}{o(H_1 \cap H_2)} = 27,$$

$o(N(H_1 \cap H_2)) \geq 27$ and divides $o(G) = 144$

$\therefore \quad o(N(H_1 \cap H_2)) = 36, 48, 72$ or 144

But then $[G : N(H_1 \cap H_2)] = 4, 3, 2$ or 1 which is not possible by problem 20.

$\therefore \quad o(H_1 \cap H_2) = 1$

i.e., any two Sylow 3-subgroups of G intersect trivially. This gives 128 elements of order 3^i ($i = 1$ or 2). Since Sylow 2-subgroup is of order 16 and not normal, there are at least 16 elements of order 2^i ($i = 1, 2, 3$ or 4) and one identity element. So, we get 145 elements in G, a contradiction.

Showing that G is a simple group.

Problem 11: *Let p be a prime dividing* $o(G)$. *Show that*

(*i*) *If K is normal in G and P is a Sylow p-subgroup of G, then* $P \cap K$ *is a Sylow p-subgroup of G.*

(*ii*) $\frac{PK}{K}$ is a *Sylow p-subgroup of* $\frac{G}{K}$

(*iii*) *Every Sylow p-subgroup of* $\frac{G}{K}$ *is of the form* $\frac{PK}{K}$ *where P is a Sylow p-subgroup of G.*

NOTES

Solution: (*i*) Suppose $P \cap K$ is not a Sylow p-subgroup of K. Then $\exists$ Sylow p-subgroup Q of K s.t., $P \cap K \subset Q \subseteq R$ where R = Sylow p-subgroup of G.

Since P and R are Sylow p-subgroups of G,

$P = xRx^{-1}$ for some $x \in G$

$xQx^{-1} \subseteq x(K \cap R)x^{-1}$

$\subseteq (xKx^{-1}) \cap (xRx^{-1})$

$= K \cap P$ as K is normal in G

$\subset Q$

But $o(xQx^{-1}) = o(Q) \Rightarrow xQx^{-1} = Q$, a contradiction.

$\therefore$ $P \cap K$ is a Sylow p-subgroup of K.

(*ii*) Let $p^m \mid o(K)$, $p^{m+1} \nmid o(K)$

Then $o(P \cap K) = p^m$ by (*i*)

But $o\left(\frac{PK}{K}\right) = \frac{o(P)\,o(K)}{o(P \cap K)\,o(K)} = \frac{o(P)}{o(P \cap K)} = \frac{p^n}{p^m} = p^{n-m}$

Now $p^n \mid o(G)$, $p^m \mid o(K) \Rightarrow p^{n-m} \mid o\left(\frac{G}{K}\right)$

Also $p^{n-m+1} \nmid o(G/K)$

$\therefore$ $\frac{PK}{K}$ is a Sylow p-subgroup of $\frac{G}{K}$.

(*iii*) Let $\frac{H}{K}$ be a Sylow p-subgroup of $\frac{G}{K}$

Let $p^n \mid o(G)$, $p^{n+1} \nmid o(G)$

$p^m \mid o(K)$, $p^{m+1} \nmid o(K)$

Let $o(K) = p^m v$, $(p, v) = 1$

$o(G) = p^n u$, $(p, u) = 1$

$\therefore$ $p^{n-m} \mid o(G/K)$, $p^{n-m+1} \nmid o\left(\frac{G}{K}\right)$

$\Rightarrow$ order of Sylow p-subgroup of $\frac{G}{K}$ is p^{n-m}

$\Rightarrow$ $o\left(\frac{H}{K}\right) = p^{n-m}$

$\Rightarrow$ $o(H) = o(K)\, p^{n-m} = p^n v$, $(p, v) = 1$

Let P be a Sylow p-subgroup of H then P is also a Sylow p-subgroup of G.

Clearly, $PK \subseteq H$ as $P \subseteq H$, $K \subseteq H$

and $o(PK) = \dfrac{o(P)\, o(K)}{o(P \cap K)} = \dfrac{p^n p^m v}{p^m}$

(as by (i) $P \cap K$ is Sylow p-subgroup of K)

$\therefore\ o(PK) = p^n v,\ (p, v) = 1$

$= o(H)$

$\therefore\ H = PK$

$\Rightarrow\ \dfrac{H}{K} = \dfrac{PK}{K}$ where P = Sylow p-subgroup of G

This proves (iii).

Problem 12: *If H is normal in G and P is a Sylow p-subgroup of H then $G = N_G(P)\, H$.*

Solution: Let $x \in G$. Then $x^{-1} Px$ is a Sylow p-subgroup of H as H is normal in G and $P \subseteq H$.

Thus, $x^{-1} Px = y^{-1} py$ for some $y \in H$

$\Rightarrow\ yx^{-1} Pxy^{-1} = P$

$\Rightarrow\ yx^{-1} \in N(P)$

$\Rightarrow\ x = (xy^{-1})\, y \in N_G(P)H.$

$\Rightarrow\ G = N_G(P)H.$

Sylow Groups in Sp^k

We now give a method of constructing Sylow p-groups inductively in the symmetric groups Sp^k.

Suppose p = prime s.t. $p^r \mid n!$ and $p^{r+1} \nmid n!$. Then $r = \sum_{j=1}^{\infty} \left[\dfrac{n}{p^j} \right]$, where $[x]$ represents greatest integer not greater than x. (This result can be found in any book on Number theory).

In particular, if $n = p^k$, then $r = p^{k-1} + p^{k-2} + \ldots + 1$ we denote r by $n(k)$ to mean the highest power of p dividing $p^k!$.

When $k = 1$, then clearly $p \mid o(S_p) = p!$ and $p^2 \nmid p!$

(as $p^2 \mid p! \quad \Rightarrow\ p \mid (p-1) \ldots 2.1$

$\Rightarrow\ p \mid (p - r),\ 1 \le r \le p - 1$

$\Rightarrow\ p \le p - r$, a contradiction)

NOTES

$\therefore$ order of Sylow p-subgroup in S_p is p and group generated by $(1\ 2...p)$ is a Sylow p-subgroup. So, We have constructed Sylow p-subgroup when $k = 1$. Assume that we have constructed it for $k - 1$. Consider Sp^k.

Divide the set of p^k letters $1, 2,...p^k$ into p sets each consisting of p^{k-1} letters as follows

$$\{1,\ 2,...\ p^{k-1}\},\ \{p^{k-1} + 1,...,\ 2p^{k-1}\},...$$
$$...\{(p-1)\}\ p^{k-1} + 1,...,\ p^{k-1}\ p = p^k\}$$

Let

$\sigma = (1p^{k-1} + 1...(p-1)\ p^{k-1} + 1)\ (2p^{k-1} + 2\ ...(p-1)\ p^{k-1} + 2)...(p^{k-1}\ 2p^{k-1}\ ...\ p^k)$

= product of p^{k-1} disjoint cycles each of length p.

Note, first cycle in σ consists of first letter from each set, second cycle has second letter from each set and so on.

Clearly $\sigma^p = I$ as disjoint cycles commute.

Let $A = \{\tau \in Sp^k \mid \tau\ (i) = i \text{ for all } i > p^{k-1}\}$

$\therefore$ $I \in A$ i.e., $A \neq \phi$

Let $\tau, \tau' \in A \Rightarrow \tau\ \tau'\ (i) = i$ for all $i > p^{k-1}$

$\Rightarrow\ \tau\tau' \in A \leq Sp^k$

But $\tau \in A \Rightarrow \tau$ is permutation on p^{k-1} letters, and so $A \cong Sp^{k-1}$.

By induction hypothesis Sp^{k-1} has Sylow p-subgroup. Thus A has Sylow p-subgroup P_1. $o(P_1) = p^{n\,(k-1)} = 1 + ... + P^{k-2}$.

Let $P_2 = \sigma\ P_1\ \sigma^{-1}$, $P_3 = \sigma^2\ P_1\ \sigma^{-2}$,... $P_p = \sigma^{p-1}\ P_1\ \sigma^{-(p-1)}$.

Each $P_i \leq Sp^k$ s.t. $P_i \cong P_1$ (where $x \in P_1$ is mapped into $\sigma^i x \sigma^{-i}$).

$\therefore$ $o(P_i) = o(P_1) = p^{n(k-1)}$. Also σ takes letters of first set into second set, letters from second set into third set and so on. So, $\tau \in A \Rightarrow \sigma T \sigma^{-1}$ consists of letters from second set as $T \in A$ means $\tau(i) = i$ for all $i > p^{k-1}$. Similarly $\sigma^2\tau\sigma^{-2}$ will consist of letters from third set on. Therefore, $P_1, P_2,..., P_{p-1}$ will have disjoint permutations and so commute with each other. Hence $T = P_1\ P_2...P_p \leq Sp^k$.

Also
$$\begin{aligned} o(T) &= o(P_1)\ o(P_2)\ ...o(P_p) \\ &= o(P_1)\ o(P_1)\ ...o(P_1)\ (p \text{ times}) \\ &= p^{\,p(n(k-1))} = p^{1+n(k-1)} \end{aligned}$$

Let
$$\begin{aligned} P &= \{\sigma^j t \mid t \in T,\ 0 \leq j \leq p-1\} \\ &= <\sigma>\ T \end{aligned}$$

Since
$$\begin{aligned} \sigma T \sigma^{-1} &= \sigma(P_1...P_P)\sigma^{-1} \\ &= (\sigma\ P_1\sigma^{-1})\ (\sigma\ P_2\sigma^{-1})\ ...\ (\sigma\ P_p\sigma^{-1}) \end{aligned}$$

NOTES

$= P_2P_3...P_pP_1 = P_1P_2...P_p = T$

$\Rightarrow \sigma T = T\sigma$

$\Rightarrow <\sigma> T = T <\sigma>$

$\therefore P \leq Sp^k$

Also $<\sigma> \cap T = \{I\}$ as s takes first set into second set while T takes first set into first set,

$$\therefore \quad o(P) = o(<\sigma>)\, o(T)$$
$$= pp^{pn}\,(k-1)$$
$$= p^{p(n\,(k-1))+1}$$
$$= P^{p(1+p+...+p^{k-2})+1}$$
$$= P^{1+p+...+p^{k-1}} = p^{n(k)}$$

So, P is required Sylow p-subgroup of G.

Problem 13: *Find a Sylow* 3*-subgroup of* S_9.

Solution: We urge the reader to first go through the discussion on the previous two pages. Let $P_1 = \{I, (123), (132)\}$ be a Sylow 3-subgroup of S_3.

Divide the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ into 3 sets as follows

$\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}$

Let $\sigma = (147)(258)(369)$

Then $\sigma^3 = I$

Let $P_2 = \sigma\, P_1\sigma^{-1} = \{I, (456), (465)\}$

$P_3 = \sigma^2\, P_2\, \sigma^{-2} = \{I, (789), (798)\}$

Let $T = P_1 P_2 P_3$, $o(T) = 3^3$

Let $P = <\sigma> T$

Then $o(P) = 3^4$

Also $n(2) = 1 + 3 = 4$

$\Rightarrow P$ is a Sylow 3-subgroup of S_9.

Problem 14: *Let G be the group of* $n \times n$ *invertible matrices over the integers modulo p. p a prime. Find a p-Sylow subgroup of G.*

Solution: Let A be an $n \times n$ matrix in G. Since A is invertible, rows of A are linearly independent over the field F of integers modulo p. Since first row of A is linearly independent, it is non zero. It can be chosen in $(p^n - 1)$ ways. Second row should not be α ($\alpha \in F$) times the first row. So, second row can be chosen in $(p^n - p)$ ways. Third row should not be α times first row + β times second row ($\alpha, \beta \in F$). So, third row can be chosen in $(p^n - p^2)$ ways as α, β can be chosen in p^2 ways. In this way, last nth row can be chosen in $p^n - p^{n-1}$ ways.

$$\therefore \quad o(G) = (p^n - 1)\,(p^n - p)\,...\,(p^n - p^{n-1})$$

$$= p^{1+2+\ldots+(n-1)} ((p^n - 1)(p^{n-1} - 1) \ldots (p - 1))$$

$$= p^{\frac{n(n-1)}{2}} ((p^n - 1) \ldots (p - 1))$$

NOTES

Since $(p, (p^i - 1)) = 1$, order of Sylow p-subgroup of G is $p^{\frac{n(n-1)}{2}}$

Let $P = \left\{ \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & \ldots & \end{bmatrix} \{| \text{ entries above diagonal from } F\} \right\}$

$P \neq \varphi$ as $I \in P$

Also

$$A, B \in P \Rightarrow A = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}$$

$$\Rightarrow AB = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \end{bmatrix} \in P$$

$\therefore \quad P \leq G$

Let $A \in P$. The first row in A can be chosen in p^{n-1} ways, second row in p^{n-2} ways and in this way $(n-1)$th row in p ways and last row is fixed.

So, $o(P) = p^{n-1} p^{n-2} \ldots p^1$

$$= p^{1+\ldots+(n-1)} = p^{\frac{n(n-1)}{2}}$$

$\therefore$ P is Sylow p-subgroup of G.

6.3 DIRECT PRODUCTS

The reader is well acquainted with the idea of product of two sets as a set of ordered pairs. We explore the possibility of getting a new group through the product of two groups. Let G_1, G_2 be any two groups.

NOTES

Let $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$.

What better way could there be than to define multiplication on G by $(g_1, g_2)\ (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$. That G forms a group under this as its composition should not be a difficult task for the reader. Indeed (e_1, e_2) will be identity of G where e_1, e_2 are identities of G_1 and G_2 respectively. Also $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

We call $G = G_1 \times G_2$ *direct product or external direct product* (EDP) of $G_1,\ G_2$.

Again if G_1, G_2 are abelian then so would be $G_1 \times G_2$.

In a similar way, we can define external direct product $G_1 \times G_2 \times ... \times G_n$ of arbitrary groups $G_1, G_2..., G_n$ as

$$G_1 \times ... \times G_n = \{(g_1,..., g_n) \mid g_i \in G_i\}$$

where compostion is component wise multiplication.

If compositions of the groups are denoted by + we also sometimes use the notation

$G_1 \oplus G_2 \oplus ... \oplus G_n$ to denote the external direct product.

Let $G = G_1 \times ... \times G_n$ = direct product of $G_1,..., G_n$.

Define $H_1 = \{g_1, e_2,..., e_n\} \mid g_1 \in G_1, e_i$ = identity of $G_i\}$

$H_2 = \{(e_1, g_2, e_3..., e_n) \mid g_2 \in G_2\}$.

.....

$H_n = \{(e_1, e_2, e_3..., g_n) \mid g_n \in G_n\}$

We show that H_1 is normal in G.

$H_1 \neq \varphi$ as $(e_1, e_2,..., e_n) \in H_1$

Let $(g_1, e_2,..., e_n)\ (g'_1, e_2,..., e_n) \in H_1$

Then $(g_1, e_2,..., e_n)\ (g'_1, e_2,..., e_n)^{-1}$

$= (g_1, e_2,..., e_n)\ (g_1^{-1}, e_2,...e_n)$

$= (g_1 g_1^{-1}, e_2,...e_n) \in H_1$

Thus $H_1 \leq G$

Let $g = (g_1.....g_n) \in G$

$x = (x_1, e_2,..., e_n) \in H_1$

Then $gxg^{-1} = (g_1,..., g_n)\ (x_1, e_2..., e_n)\ (g_1^{-1},..., g_n^{-1})$

$= (g_1 x_1 g_1^{-1}, e_2,...e_n) \in H_1$

$\therefore$ H_1 is normal in G.

Similarly, each H_i is normal in G for all $i = 1,..., n$.

Let $g = (g_1,..., g_n) \in G$

NOTES

Then $g = (g_1, e_2,..., e_n)\ (e_1, g_2, e_3...e_n)...(e_1, e_2 ,..., e_{n-1}, g_n) \in H_1 H_2...H_n$

Suppose $g = h_1 h_2...h_n = h'_1 h'_2,...,h'_n,\ h_i, h'_i \in H_i$

Then $(g_1, e_2,..., e_n) ... (e_1,... e_{n-1}, g_n) = (g'_1,..., e_n)...(e_1,...e_{n-1}, g'_n)$

$\Rightarrow (g_1,..., g_n) = (g'_1...g'_n)$

$\Rightarrow g_i = g'_i$ for all $i = 1,..., n$

$\Rightarrow h_i = h'_i$ for all $i = 1,..., n$

So, $g \in G$ can be written uniquely as product of elements from $H_1,..., H_n$.

We summarise this through the following definition.

Let $H_1 ,..., H_n$ be normal subgroups of G. G is said to be an internal direct product (IDP) of $H_1,..., H_n$ if $G = H_1H_2... H_n$ and each $g \in G$ can be written uniquely as product of elements from $H_1,..., H_n$.

Example 1: (*a*) Consider the groups $\mathbf{Z}_2 = \{0, 1\}$, $\mathbf{Z}_3 = \{0, 1, 2\}$ under addition modulo. Here $\mathbf{Z}_2 \times \mathbf{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0) (1, 1), (1, 2)\}$ will form a group under element wise multiplication (addition). In fact it is a cyclic group generated by (1, 1).

Indeed, $2(1, 1) = (1, 1) + (1, 1) = (1 \oplus_2 1, 1 \oplus_3 1) = (0, 2)$,

$3(1, 1) = (1, 1) + (1, 1) + (1, 1) = (1, 0)$ etc.

We further note that since two cyclic groups of same order are isomorphic, we must have $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.

On the other hand one can show that $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not isomorphic to $\mathbf{Z}_4$. In fact $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic (whereas $\mathbf{Z}_4$ is). If $\mathbf{Z}_2 \times \mathbf{Z}_2$ is cyclic then it has a generator whose order should be same as $o(\mathbf{Z}_2 \times \mathbf{Z}_2) = 4$. But no element of $\mathbf{Z}_2 \times \mathbf{Z}_2$ has order 4. Notice, $2(1, 1) = (0, 0)$ i.e., order of $(1, 1)$ is less then or equal to 2 etc. Hence no element can be generator of $\mathbf{Z}_2 \times \mathbf{Z}_2$. One can show that $\mathbf{Z}_n \times \mathbf{Z}_m \cong \mathbf{Z}_{nm}$ iff n and m are relatively prime.

(*b*) Let us now consider $\mathbf{Z} \times \mathbf{Z}$. We know $\mathbf{Z}$ is cyclic, generated by 1. Would $\mathbf{Z} \times \mathbf{Z}$ be cyclic? Suppose it is and let (a, b) be a generator of $\mathbf{Z} \times \mathbf{Z}$.

Since $(1, 1) \in \mathbf{Z} \times \mathbf{Z}$, $\exists$ an integer m s.t., $(1, 1) = m\ (a, b)$

$\Rightarrow ma = 1, mb = 1, \quad m, a, b$ integers

giving the possibilities $a = \pm 1, b = \pm 1$. Now $(1, 2) \in \mathbf{Z} \times \mathbf{Z}$ but for no integer t, we can have $(1, 2) = t(a, b) \quad (a = \pm 1, b = \pm 1)$

Hence $\mathbf{Z} \times \mathbf{Z}$ is not cyclic.

Theorem 7: *Let H_1, H_2 be normal in G. Then G is an IDP of H_1 and H_2 if and only if*

(*i*) $G = H_1H_2$

(*ii*) $H_1 \cap H_2 = \{e\}$.

NOTES

Proof: Suppose G is an IDP of H_1 and H_2. Let $g \in G$.

Then $g = h_1h_2,\ h_1 \in H_1, h_2 \in H_2$.

Then $G \subseteq H_1H_2$. But $H_1H_2 \subseteq G$

$\Rightarrow$ $G = H_1H_2$

Let $g \in H_1 \cap H_2 \Rightarrow g \in H_1, g \in H_2$

$\therefore$ $g = ge = eg$ is written in 2 ways as product of elements from H_1 and H_2.

$\therefore$ $g = e \Rightarrow H_1 \cap H_2 = \{e\}$.

Conversely, let $G = H_1H_2$ and $H_1 \cap H_2 = \{e\}$

Let $g \in G \Rightarrow g \in H_1H_2 \Rightarrow g = h_1h_2,\ h_1 \in H_1, h_2 \in H_2$

Let $g = h_1h_2 = h'_1h'_2,\quad h_1, h'_1 \in H_1, h_2, h'_2 \in H_2$

$\Rightarrow h_1^{-1} h'_1 = h_2h_2^{-1} \in H_1 \cap H_2 = \{e\}$

$\Rightarrow h_1 = h'_1, h_2 = h'_2$

$\therefore$ G is an IDP of H_1 and H_2.

Example 2: Let $G = < a >$ be of order 6. Let $H = \{e, a^2, a^4\}, K = \{e, a^3\}$ then H and K are normal (G is abelian) subgroups of G. $H \cap K = \{e\}$.

$$HK = \{e, ea^3, a^2e, a^2a^3, a^4e, a^4a^3\}$$
$$= \{e, a^2, a^3, a^4, a^5, a\} = G$$

Hence G is IDP of H and K

Theorem 8: *Let $H_1, H_2,..., H_n$ be normal in G. Then G is an IDP of $H_1, H_2,..., H_n$ if and only if*

(*i*) $G = H_1H_2... H_n$

(*ii*) $H_i \cap H_1H_2... H_{i-1} H_{i+1}...H_n = \{e\}$

for all $i = 1,... n$

Proof: Suppose G is an IDP of $H_1,..., H_n$. Then (*i*) follows from the definition of IDP

Let $g \in H_i \cap H_1... H_{i-1} H_{i+1} ... H_n$

Then $g = h_i,\ h_i \in H_i$ and $g = h_1h_2...h_{i-1} h_{i+1}... h_n, h_j \in H_j$

$\Rightarrow g = ee ... h_i ... e$

$g = h_1h_2 ... h_{i-1} e h_{i+1} ... h_n$

Since this representation of g should be unique we get $e = h_1, e = h_2,..., h_i = e,...$

or that $g = e$, which proves the result.

Conversely, let $g \in G$ then $g \in H_1... H_n \Rightarrow g = h_1... h_n, h_i \in H_i$

We show this representation is unique.

Let $g = h'_1 ..... h'_n,\ h'_i \in H_i$

$\therefore$ $h_1 ..... h_n = h'_1 ..... h'_n$

NOTES

By (*ii*) $H_i \cap H_j = \{e\}$ for all $i \neq j$ because if $x \in H_i \cap H_j$

Then $x \in H_i$, $x \in H_j$. $(j \neq i)$

$$x \in H_j \Rightarrow x \in H_1 \ldots H_j \ldots H_{i-1}\, H_{i+1} \ldots H_n$$

as $x = e \ldots x \ldots e.\ e \ldots e$

$$\Rightarrow x \in H_i \cap H_1 \ldots H_{i-1}\, H_{i+1} \ldots H_n = \{e\}$$

Also H_i is normal in G, H_j is normal in G for all i, j, thus $h_i h_j = h_j h_i$ for all $i \neq j$

$$\therefore \quad h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow h_n = (h_1^{-1} h'_1)\,(h_2^{-1} h'_2) \ldots\ldots\ldots (h_{n-1}^{-1} h'_{n-1})\, h'_n$$

$$\therefore\ h_n\, h_n^{'-1} = (h_1^{-1} h'_1) \ldots\ldots\ldots (h_{n-1}^{-1} h'_{n-1}) \in H_1 \ldots\ldots\ldots H_{n-1} \cap H_n = \{e\}$$

$$\therefore \quad h_n = h'_n$$

Similarly $h_{n-1} = h'_{n-1}, \ldots\ldots, h_1 = h'_1$

Hence G is an IDP of $H_1, \ldots\ldots, H_n$.

Remark: If G is an IDP of $H_1, H_2, \ldots\ldots, H_n$ then $H_i \cap H_j = \{e\}$, $i \neq j$.

We now show that IDP of subgroups of G is isomorphic to their external direct product (EDP).

Theorem 9: *Let G be a group and suppose G is IDP of $H_1, \ldots, H_n$. Let T be EDP of $H_1, \ldots, H_n$. Then G and T are isomorphic.*

Proof: Define $\theta : T \to G$, s.t.,

$$\theta(h_1, \ldots\ldots\ldots, h_n) = h_1 \ldots\ldots\ldots h_n, \quad h_i \in H_i$$

θ is well defined as $(h_1, \ldots, h_n) = (h'_1, \ldots, h'_n)$

$$\Rightarrow h_i = h'_1 \text{ for all } i$$

$$\Rightarrow h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow \theta(h_1, \ldots\ldots\ldots, h_n) = \theta(h'_1, \ldots\ldots\ldots, h'_n)$$

θ is homomorphism as

$$\theta(h_1, \ldots\ldots\ldots, h_n)\,(h'_1, \ldots\ldots\ldots, h'_n)$$

$$= \theta(h_1 h'_1, \ldots\ldots\ldots, h_n h'_n)$$

$$= (h_1 h'_1) \ldots\ldots\ldots (h_n h'_n)$$

$$= (h_1, \ldots, h_n)\,(h'_1, \ldots, h'_n)$$

as $h_i h_j = h_j h_i$

$h'_i h'_j = h'_j h'_i$ for all $i \neq j$

$$= \theta(h_1, \ldots, h_n)\ \theta(h'_1, \ldots, h'_n)$$

θ is 1 – 1 as $\theta(h_1, \ldots, h_n) = \theta(h'_1, \ldots, h'_n)$

$$\Rightarrow h_1 \ldots\ldots\ldots h_n = h'_1 \ldots\ldots\ldots h'_n$$

$$\Rightarrow h_i = h'_i \text{ for all } i \text{ by definition of IDP}$$

$\Rightarrow (h_1,... h_n) = (h'_1,..., h'_n)$

θ is onto as $g \in G \Rightarrow g = h_1... h_n,\ h_i \in H_i$

$= \theta(h_1,..., h_n),\ (h_1,..., h_n) \in T$

$\therefore$ θ is an isomorphism.

Hence $G \cong T$.

NOTES

Problem 14: *Let A, B be finite cyclic groups of order m and n respectively. Prove that A × B is cyclic if and only if m and n are relatively prime.*

Solution: Let $A = < a >, B = < b >$

$o(A) = o(a) = m,\ o(B) = o(b) = n$

Suppose $A \times B$ is cyclic.

Let $A \times B = < (x, y) >, \quad x \in A, y \in B$

$o(A \times B) = mn = o(x, y)$

Let g.c.d. of m and n be d.

$\therefore$ $\frac{m}{d}$ and $\frac{n}{d}$ are relatively prime integers.

Consider $(x, y)^{\frac{mn}{d}} = \left(x^{\frac{mn}{d}}, y^{\frac{mn}{d}} \right)$

$= \left((x^m)^{\frac{n}{d}}, (y^n)^{\frac{m}{d}} \right)$

$= \left(e_1^{\frac{n}{d}}, e_2^{\frac{m}{d}} \right)$, e_1 = identity of A

e_2 = identity of B

$= (e_1, e_2)$

$=$ identity of $A \times B$

$\therefore$ $o(x, y) \left| \frac{mn}{d} \right.$

$\Rightarrow mn \left| \frac{mn}{d} \right.$

$\Rightarrow d.\frac{mn}{d} \left| \frac{mn}{d} \right.$

$\Rightarrow d \mid 1 \Rightarrow d = 1.$

$\therefore$ m and n are relatively prime.

Conversely, let m and n be relatively prime. We show $A \times B$ is cyclic, generated by (a, b). For that we prove $o(a, b) = mn = o(A \times B)$.

NOTES

Consider $(a, b)^{mn} = (a^{mn}, b^{mn})$

$= ((a^m)^n, (b^n)^m)$

$= (e_1, e_2)$ = identity of $A \times B$

Let $(a, b)^r = (e_1, e_2)$

$\Rightarrow (a^r, b^r) = (e_1, e_2)$

$\Rightarrow a^r = e_1, b^r = e_2$

$\Rightarrow o(a) = m \mid r, o(b) = n \mid r$

$\Rightarrow mn \mid r$ as m, n are relatively prime.

$\Rightarrow mn \leq r$

$\therefore$ $o(a, b) = mn = o(A \times B)$

Hence $A \times B = < (a, b) >$ = cyclic group generated by (a, b).

Remark: One could generalise the above result and say If $G_1, G_2, ..., G_n$ be finite cyclic groups of order $m_1, m_2, ..., m_n$ then $G_1 \times G_2 \times ... \times G_n$ is cyclic if and only if m_i, m_j are relatively prime $(i \neq j)$.

Problem 15: *Let $o(G) = p^2q^2$, p, q are distinct primes such that $q \nmid p^2 - 1$, $p \nmid q^2 - 1$. Then G is abelian.*

Solution: The number of Sylow p-subgroups of G is $1 + kp$ such that $1 + kp | q^2$. So, $1 + kp = 1$, q or q^2. If $1 + kp = q^2$, then $p | q^2 - 1$, a contradiction.

If $1 + kp = q$, then $p | q - 1 \Rightarrow p \leq q - 1 < q$, a contradiction.

So, there is only one Sylow p-subgroup H of G such that $H \trianglelefteq G$. Similarly, there is only one Sylow q-subgroup K of G such that $K \trianglelefteq G$. Then $G = H \times K$. Since H and K are abelian, so is G.

Problem 16: *If every Sylow subgroup of a group G is normal and abelian, then show that G is abelian.*

Solution: Let $\wp$ be the group generated by all Sylow subgroups of G. Then $\wp \leq G$. If P, Q are Sylow subgroups of different orders, then P and Q are normal and $P \cap Q = \{e\}$.

$\Rightarrow$ $xy = yx$ for all $x \in P$ and $y \in Q$. Also, $xy = yx \; \forall \; x, y \in P$.

Thus $\wp$ is abelian.

Let P be any Sylow subgroup of G, then $P \in \wp \Rightarrow o(P) \mid o(\wp) \; \forall$ Sylow subgroups P of G.

$\Rightarrow$ $o(G) \mid o(\wp) \Rightarrow \wp = G$ or that G is abelian.

Problem 17: *Show that if G is a group of order* 45, *it is IDP of its Sylow subgroups.*

Solution: $o(G) = 45 = 3^2 \times 5$.

Number of Sylow 5-subgroups is $(1 + 5k)$ s.t., $(1 + 5k) \mid 9$ which gives $k = 0$

i.e., ∃ a unique normal Sylow 5-subgroup H of G where $o(H) = 5$.

Similarly, ∃ *a* unique normal Sylow 3-subgroup K of order 9.

Since $o(H \cap K) \mid 9, 5$, we find $o(H \cap K) = 1 \Rightarrow H \cap K = \{e\}$

NOTES

Also $o(HK) = \frac{5 \times 9}{1} = 45 = o(G) \Rightarrow G = HK$

Hence G is IDP of its sylow subgroups H & K.

Problem 18: *If H, K are normal subgroups of G, show that* $\frac{G}{H \cap K}$ *is isomorphic to a subgroup of* $\frac{G}{H} \times \frac{G}{K}$.

Solution: Define $\theta: G \to \frac{G}{H} \times \frac{G}{K}$ s.t.,

$$\theta(x) = (Hx, Kx) \quad \text{for all } x \in G$$

θ is well defined as $x = y \Rightarrow Hx = Hy, Kx = Ky \Rightarrow (Hx, Kx) = (Hy, Ky)$.

θ is a homomorphism as

$$\begin{aligned}\theta(xy) &= (Hxy, Kxy)\\ &= (HxHy, KxKy)\\ &= (Hx, Kx)\ (Hy, Ky)\\ &= \theta(x)\ \theta(y) \quad \text{for all } x, y \in G\end{aligned}$$

$$\begin{aligned}\text{Ker } \theta &= \{x \in G \mid \theta(x) = \text{identity of } \frac{G}{H} \times \frac{G}{K}\}\\ &= \{x \in G \mid (Hx, Kx) = (H, K)\}\\ &= \{x \in G \mid Hx = H, Kx = K\}\\ &= \{x \in G \mid x \in H, x \in K\}\\ &= \{x \in G \mid x \in H \cap K\}\\ &= H \cap K.\end{aligned}$$

$\therefore \ \frac{G}{\text{Ker } \theta} = \frac{G}{H \cap K}$ is isomorphic to $\theta(G)$

(Note θ is onto map from G to $\theta(G)$)

Also, $\theta(G)$ is a subgroup of $\frac{G}{H} \times \frac{G}{K}$.

$\therefore \ \frac{G}{H \cap K}$ is isomorphic to a subgroup of $\frac{G}{H} \times \frac{G}{K}$.

NOTES

Check Your Progress

1. What is a p-group?
2. Give an example of finite p-group.
3. What is Sylow's second Theorem?

6.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. A *p*-group is a group in which every element has order p^r where *p* = prime. Here *p* is same for all elements and *r* may vary
2. Group K^4 = {I, (12) (34), (13) (24), (14) (23)}
3. Any two Sylow *p*-subgroups of a finite group *G* are conjugate in *G*.

6.5 SUMMARY

- A *p*-group is a group in which every element has order p^r where *p* = prime. Here *p* is same for all elements and *r* may vary.
- Any finite *p*-group has non-trivial Centre.
- A *p*-group may or may not be abelian.
- Let *p* be a prime s.t. p^n divides order of a group *G* and p^{n+1} does not divide it. Then a subgroup *H* of *G* s.t. *o(H)* = is called a Sylow *p*-subgroup of *G* or *p*-Sylow subgroup of *G*.
- Let $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_1 \in G_2\}$, then $G = G_1 \times G_2$ called direct product or external direct product (EDP) of G_1, G_2.

6.6 KEY WORDS

- **Prime:** A prime number is a whole number greater than 1 whose only factors are 1 and itself.
- **Cyclic group:** A cyclic group or monogenous group is a group that is generated by a single element.
- **Normal subgroup:** A normal subgroup is a subgroup that is invariant under conjugation by members of the group of which it is a part.

6.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

NOTES

Short Answer Questions

1. Define Sylow *p*-subgroup.
2. Find a Sylow 3-subgroup of S_n.
3. Show that if *G* is a group of order 45, it is IDP of its Sylow subgroups.
4. Show that all Sylow *p*-subgroups of *G* are isomorphic.

Long Answer Questions

1. If *G* is a finite group, then show that *G* is a *p*-group if and only if $o(G) = p^n$.
2. State and prove Sylow's First Theorem.
3. Prove that every *p*-subgroup of a finite group *G* is contained in some Sylow *p*-subgroup of *G*.
4. If every Sylow subgroup of a group *G* is normal and abelian, then show that *G* is abelian.

6.8 FURTHER READINGS

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Zassenhaus, Hans J. 2013. *The Theory of Groups*. Chelmsford: Courier Corporation.

UNIT 7 FINITE ABELIAN GROUPS

NOTES

Structure

7.0 INTRODUCTION

The concept of an abelian group is one of the first concepts encountered in undergraduate abstract algebra, from which many other basic concepts, such as modules and vector spaces, are developed. The term Abelian group comes from Niels Henrick Abel, a mathematician who worked with groups even before the formal theory was laid down. This unit discusses about finite abelian groups and the fundamental theorem on finite abelian groups. In the end you will also see some problems based on proven theorems.

7.1 OBJECTIVES

After going through this unit, you will be able to:

- Understand finite abelian groups
- Learn some theorems on finite groups
- Solve problems based on abelian groups

7.2 FINITE ABELIAN GROUPS AND SUPPLEMENTARY PROBLEMS

Having studied direct products, one would like to know whether groups can be written as direct product of some 'simple looking' groups, Luckily, such a class of groups exists, namely finite abelian groups. The main purpose of this section is to prove that all important theorem called fundamental theorem on finite abelian groups which states that a finite abelian group is a direct product of cyclic groups of prime power order and the representation is unique except for the order in which the factors are arranged. This paves the way for us to spell out the method that gives the number of non-isomorphic finite abelian groups of a given order.

NOTES

We first show that a finite abelian group can be written as a direct product of p-groups.

Theorem 1: *A finite abelian group is a direct product of its Sylow p-subgroups.*

Proof: Let G be a finite abelian group of order n. Let $n = p_1^{\alpha 1} \ldots p_r^{\alpha r}$ $p_i's$ being distinct primes.

Let $S_1,\ldots S_r$ be distinct Sylow p_i-subgroups respectively. $o(S_i) = p_i^{\alpha i}$ for all $i = 1,\ldots, r$

We show that $G = S_1 \times \ldots \times S_r$

Since G is abelian, each S_i is a normal subgroup of G.

Let $m = p_2^{\alpha 2} \ldots p_r^{\alpha r}$

and $T = \{x \in G \mid x^m = e\}$ Then $(p_1^{\alpha 1}, m) = 1$

and T is a subgroup of G as G is abelian.

Now $x \in S_1 \cap T \Rightarrow o(x) \mid o(S_1) = p_1^{\alpha 1}$

and $o(x) \mid m$

So, $o(x) \mid (p_1^{\alpha 1}, m) = 1$

$\Rightarrow o(x) = 1$

$\Rightarrow x = e$

$\therefore$ $S_1 \cap T = \{e\}$

As $(p_1^{\alpha 1}, m) = 1$, $\exists$ integers u, v such that

$up_1^{\alpha 1} + vm = 1$

Let $x \in G$. Then $x = x^1$

$= x^{up1^{\alpha 1} + vm}$

$= x^{vm} \cdot x^{up1^{\alpha 1}}$

$\in S_1$. T (as $(x^{vm})^{p1^{\alpha 1}} = (x^{p1^{\alpha 1}m})^v = x^{vn} = (x^n)^v = e$

$\Rightarrow o(x^{vm}) \mid p_1^{\alpha 1}$

$\Rightarrow o(x^{vm}) = p_1^{\beta 1}$

$\Rightarrow < x^{vm} >$ is a p_1 group

$\Rightarrow < x^{vm} > \subseteq S_1$

$\Rightarrow x^{vm} \in S_1$

Also $(x^{up1^{\alpha 1}})^m = x^{un} = e$

$\Rightarrow x^{up1^{\alpha 1}} \in T$)

$\therefore$ $G = S_1T$. Also as seen earlier $S_1 \cap T = \{e\}$

Since G is abelian, S_1 and T are normal subgroups of G, and thus G is IDP of S_1 and T

NOTES

$\therefore$ $G = S_1 \times T$ (because of the isomorphism)

Also, $o(G) = o(S_1 T)$

$= o(S_1)\, o(T)$

$\Rightarrow n = p_1^{\alpha_1}\, o(T)$

$\Rightarrow o(T) = p_2^{\alpha_2} \ldots p_r^{\alpha_r} = m$

As above, we can show that

$T = S_2 \times U$, where U is a subgroup of T such that $o(U) = p_3^{\alpha_3} \ldots p_r^{\alpha_r}$. In this way, we shall have

$$G = S_1 \times S_2 \ldots S_r$$

which proves the theorem.

Remark: Since a Sylow p-subgroup is a group of prime power order, we have established that *A finite abelian group is a direct product of groups of prime power order.*

Having *broken G* into product of groups of prime power order, we concentrate now on results pertaining to abelian groups of prime power order rather than on G itself.

Theorem 2: *Let G be an abelian group of prime power order p^n and let $a \in G$ have maximal order amongst all elements in G. Then G is IDP of A and K, where A is the cyclic subgroup generated by a and $K \leq G$. Hence G can be expressed as $G = A \times K$.*

Proof: Let $o(G) = p^n$, p a prime.

We use induction on n. If $n = 1$ then $o(G) = p$, a prime and thus G is a cyclic group of order p and if $G = < a >$ then a is an element of maximal order p in G and also then $G = < a > \times \{e\}$ and so the result holds for $n = 1$.

Let the result be true for abelian groups of order p^k, where $k < n$.

Let $a \in G$ be an element of maximal order and suppose $o(a) = p^m$.

In case $G = < a >$, then $G = < a > \times \{e\}$ and there is nothing to prove.

So assume, $G \neq < a >$. Thus $\exists$ elements in G which are not in $< a > = A$. Out of these elements let b be an element of minimal order.

Now $$o(b^p) = \frac{o(b)}{\text{g.c.d.}(o(b), p)} = \frac{o(b)}{p} < o(b).$$

Note as $o(b) | o(G) = p^n$, $o(b)$ is of the type p^i for some i.

So $o(b^p) < o(b) \Rightarrow b^p \in A$ as b is of minimal order s.t., $b \notin A$.

Now $b^p \in A = <a> \Rightarrow b^p = a^i$ for some i

If $x \in G$ be any element then as

$o(x) | o(G) = p^n$, $o(x) = p^t$ for some t

and so $x^{p^t} = e$

Again as $o(a) = p^m$ is maximal order of an element in G, $p^t \leq p^m$ i.e., $p^t \mid p^m$ and so $x^{p^m} = e \quad \forall\ x \in G$

$\Rightarrow b^{p^m} = e$

NOTES

Thus $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$

$\Rightarrow o(a^i) \leq p^{m-1}$

$\Rightarrow a^i$ cannot be a generator of $A = < a >$ as $o(A) = o(a) = p^m$ and $o(a^i) < p^m$

$\Rightarrow (p^m, i) \neq 1$

So p^m and i have common factors

$\Rightarrow p \mid i$ or that $i = pj$

$\Rightarrow b^p = a^i = a^{pj}$

Let $c = a^{-j}b$ then if $c \in A$, then $a^{-j}b \in A$

$\Rightarrow a^{-j}b = a_1$ for some $a_1 \in A$.

$\Rightarrow b = a^j a_1 \in A$, which is not true. Hence $c \notin A$

Again $c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e,\ c \neq e$

$\Rightarrow o(c) = p$

i.e., $\exists$ an element $c \in G$ s.t., $c \notin A$ and $o(c) = p$.

So $o(b)$ should also be p as b has minimal order

Let $B = < b >$, then $o(B) = o(b) = p$

Also, $A \cap B \leq B \Rightarrow o(A \cap B) | o(B) = p$

$\Rightarrow o(A \cap B) = 1$ or p.

If $o(A \cap B) = p$, then $o(A \cap B) = o(B)$

$\Rightarrow A \cap B = B \Rightarrow B \subseteq A$

which is not possible as $b \notin A$

Hence, $o(A \cap B) = 1$ or that $A \cap B = \{e\}$

Let $\bar{G} = G/B$.

Since $a \in G$, $Ba \in G/B = \bar{G}$

Let $Ba = \bar{a} \in \bar{G}$

Now $(\bar{a})^{o(a)} = (Ba)^{o(a)} = Ba \cdot Ba \cdots Ba = Ba^{o(a)} = Be = B =$ Identity of $\bar{G}$

$\therefore \quad o(\bar{a}) \mid o(a) \qquad (1)$

Again, $Ba^{o(\bar{a})} = (Ba)^{o(\bar{a})} = (Ba)^{o(Ba)} = B =$ Identity of $\bar{G}$

$\Rightarrow a^{o(a)} \in B$

Also, $a^{o(\bar{a})} \in A \Rightarrow a^{o(\bar{a})} \in A \cap B = \{e\}$

$\Rightarrow a^{o(\bar{a})} = e \Rightarrow o(a) \mid o(\bar{a}) \Rightarrow o(a) = o(\bar{a})$ from (1)

NOTES

Now $\bar{a}$ will be an element of maximal order in $\bar{G}$ as if $c^{-} \in \bar{G}$ is an element with more order than $o(\bar{a})$ then

as $o(\bar{c}) \mid o(c)$ as in (1), we get

$o(\bar{c}) \leq o(c) \Rightarrow o(c) \geq o(\bar{c}) > o(\bar{a}) = o(a)$

contradicting the fact that a is of maximal order.

Now $o(\bar{G}) < o(G)$ and so using induction we can say $\bar{G}$ is an IDP of $< \bar{a} >$ and $\bar{T}$ for some subgroup $\bar{T}$ of $\bar{G}$ and

$$\bar{G} = < \bar{a} > \bar{T}, \quad < \bar{a} > \cap \bar{T} = \{\bar{e}\}$$

$\bar{T}$ is a subgroup of $\bar{G} = G/B \Rightarrow \bar{T} = \frac{K}{B}$ for some $K \leq G$

We show G is IDP of A and K

Let $x \in A \cap K$ then $x \in A$ and $x \in K$

$\Rightarrow x = a^i$ for some i

and $x \in K \Rightarrow a^i \in K \Rightarrow Ba^i \in \bar{T}$

$\Rightarrow (Ba)^i \in \bar{T}$

$\Rightarrow (\bar{a})^i \in \bar{T}$

$\Rightarrow (\bar{a})^i \in < \bar{a} > \cap \bar{T} = \{\bar{e}\}$

$\Rightarrow (\bar{a})^i = \bar{e} \Rightarrow Ba^i = Be \Rightarrow a^i \in B$

$\therefore$ $a^i \in A \cap B = \{e\} \Rightarrow a^i = e$

$\therefore$ $x = a^i = e \Rightarrow A \cap K = \{e\}$

Now let $x \in G$ then $\bar{x} = Bx \in \bar{G} = < \bar{a} > \cdot \bar{T}$

$\Rightarrow \bar{x} = (\bar{a})^j \bar{y}, \quad \bar{y} \in \bar{T} = {}^{K}\!/_{B}$

$\Rightarrow Bx = (Ba)^j By = Ba^j y \qquad (\bar{y} = By)$

$\Rightarrow xy^{-1}a^{-j} \in B \subseteq K$

$\Rightarrow xy^{-1}a^{-j} = k$ for some $k \in K$

$\Rightarrow x = ka^j y = a^j z$ for some $z \in K$

or that $x \in < a >. K \Rightarrow G \subseteq AK$

i.e., $G = AK$, $A \cap K = \{e\}$

So G is an IDP of A and K and can be expressed as $A \times K$.

We are now ready to prove the fundamental theorem on finite abelian groups.

Theorem 3: (The Fundamental Theorem on Finite Abelian Groups). *A finite abelian group is direct product of cyclic groups of prime power order*. (representation being unique).

NOTES

Proof: Let G be a finite abelian group. We prove the result by induction on $o(G)$. If $o(G) = 1$, then result is trivially true. Assume that the result is true for all abelian groups of order $< o(G)$.

Let $o(G) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, p_is are distinct primes.

By theorem 1, $G = S_1 \times \ldots \times S_r$, where S_i is the Sylow p_i-subgroup of order $p_i^{\alpha_i}$ ($i = 1, 2, \ldots, r$). i.e., a subgroup of prime power order.

By theorem 2, $S_i = A_i \times K_i$, where each A_i is a cyclic group.

$$\Rightarrow G = (A_1 \times K_1) \times \ldots \times (A_r \times K_r)$$
$$= (A_1 \times \ldots \times A_r) \times (K_1 \times \ldots \times K_r)$$

Now $o(K_1 \times \ldots \times K_r) < o(G)$ and $K_1 \times K_2 \ldots \times K_r$ is an abelian group. By induction hypothesis $K_1 \times \ldots \times K_r = T_1 \times \ldots \times T_s$, where each T_i is a cyclic subgroup of G of prime power order.

$$\therefore \quad G = A_1 \times \ldots \times A_r \times T_1 \times \ldots \times T_s$$
$$= \text{direct product of cyclic subgroups of prime power orders.}$$

$\therefore$ result is true in this case as well.

By induction result is true for all finite abelian groups G.

Note: By theorem 2, S_i is IDP of A_i and K_i

i.e., $S_i = A_i K_i$, $A_i \cap K_i = \{e\}$

$$\therefore \quad o(S_i) = \frac{o(A_i)o(K_i)}{o(A_i \cap K_i)} = o(A_i)o(K_i)$$

But $o(S_i) = p_i^{\alpha_i}$ = prime power and thus $o(A_i)$ and $o(K_i)$ being its divisors are also prime powers.

Summing up, we notice that any finite abelian group is product of $S_1, S_2, \ldots, S_n$ where each S_i is a group of prime power order and each S_i is then a product of cyclic groups of prime power order. To tackle the uniqueness issue, we notice that each S_i is unique as if $x \in S_i$ then $o(x) \mid o(S_i) = p_i^{\alpha_i} \Rightarrow o(x) = p_i^{\beta i}$ and thus $x \notin S_j$ for any $j \neq i$.

We wind up the whole process by proving

Theorem 4: *Let G be a finite abelian group of order p^n, p a prime. Suppose $G = A_1 \times \ldots \times A_k$ where each A_i is a cyclic group of order p^{n_i} with $n_1 \geq n_2 \geq \ldots \geq n_k > 0$. Then the integers $n_1, \ldots, n_k$ are uniquely determined,* (*called invariants of G*).

NOTES

In other words, if G is a finite abelian group of prime power order p^n and

$$G = A_1 \times A_2 \times \ldots \times A_k$$
$$G = B_1 \times B_2 \times \ldots \times B_l$$

where A_i and B_j are non trivial cyclic subgroups with

$$o(A_1) \geq o(A_2) \geq \ldots \geq o(A_k) > 0$$
$$o(B_1) \geq o(B_2) \geq \ldots \geq o(B_l) > 0$$

then $k = l$ and $o(A_i) = o(B_i)\ \forall i$.

Proof: Suppose $G = A_1 \times \ldots \times A_k$

and $G = B_1 \times \ldots \times B_l$

where A_i and $B_j s$ are cyclic groups s.t. $o(A_i) = p^{n_i}$, $o(B_j) = p^{h_j}$,

$n_1 \geq n_2 \geq \ldots \geq n_k > 0$, $h_1 \geq h_2 \geq \ldots \geq h_l > 0$

Our aim is to show that $k = l$ and $n_i = h_i$ for all i. Let $g \in G$. Then $g = a_1 a_2 \ldots a_k$, $a_i \in A_i$

Since $n_1 \geq n_i$ for all $i = 1,\ldots, k$

$p^{n_i} \mid p^{n1}$ for all $i = 1,\ldots, k$

$\therefore$ $p^{n1} = p^{n_i} p^{u_i}$ for all $i = 1,\ldots, k$

So, $g^{p^{n1}} = a_1^{p^{n1}} a_2^{p^{n1}} \ldots a_k^{p^{n1}}$

$= a_1^{p^{n1}} a_2^{p^{n2} p^{u2}} \cdots a_k^{p^{nk} p^{uk}}$

$= e$ as $(a_i)^{p^{ni}} = a_i^{o(Ai)} = e$ for all i

$\therefore$ $o(g) \mid p^{n1}$ for all $g \in G$

$\Rightarrow o(g) \leq p^{n1}$ for all $g \in G$

Also A_1 is a cyclic group of order $p^{n1} \Rightarrow \exists$ an element of order p^{n1}.

So p^{n1} is the maximal order of elements in G. Similarly, by taking

$G = B_1 \times \ldots \times B_l$, we get p^{h1} to be the maximal order of elements in G.

$\therefore$ $p^{n1} = p^{h1} \Rightarrow n_1 = h_1$

Suppose we have proved that $n_1 = h_1$, $n_2 = h_2,\ldots, n_{t-1} = h_{t-1}$. Suppose $n_t \neq h_t$. Let $n_t > h_t = m$. Define $C = \{x^{p^m} \mid x \in G\}$. Since G is abelian, C is subgroup of G.

Let $A_1 = \langle a_1 \rangle,\ldots, A_k = \langle a_k \rangle$, $o(a_i) = o(A_i) = p^{n_i}$

$B_1 = \langle b_1 \rangle,\ldots, B_k = \langle b_k \rangle$, $o(b_j) = o(B_j) = p^{h_j}$

We claim that

$$C = \langle b_1^{p^m} \rangle \times \ldots \times \langle b_{t-1}^{p^m} \rangle$$

Let $x^{p^m} \in C$, $x \in G$

Now $x \in G \Rightarrow x = x_1 \ldots x_{t-1}\, x_t \ldots x_l$, $x_j \in B_j$

$x_j \in B_j \Rightarrow x_j = b_j^{r_j}$

$\therefore \quad x^{p^m} = x^{p^m}{}_1 \ldots x^{p^m}{}_l$

$= b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m} \; b_t^{r_t p^m} \ldots b_l^{r_1 p^m},$

Now for all $j \geq t$, $o(B_j) = p^{h_j} \mid p^{h_t} = p^m$

$\Rightarrow p^m = p^{h_j} p^{v_j}$

$= e$ for all $j \geq t$

$\Rightarrow b_j^{p^m} = b_j^{p^{h_j} p^{v_j}} = e$ for all $j \geq t$

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m}$

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} \ldots b_{t-1}^{r_{t-1} p^m}$

$\in < b_1^{p^m} > \ldots < b_{t-1}^{p^m} >$

$\therefore \quad C \subseteq < b_1^{p^m} > \ldots < b_{t-1}^{p^m} >$

But $b_j^{p^m} \in C \Rightarrow < b_j^{p^m} > \subseteq C$

$\therefore \quad C = < b_1^{p^m} > \ldots < b_{t-1}^{p^m} >$

Also $x \in < b_1^{p^m} > \cap < b_2^{p^m} > \ldots < b_{t-1}^{p^m} >$

$\Rightarrow x \in B_1, x \in B_2 \ldots B_{t-1}$

$\Rightarrow x \in B_1, x \in B_2 \ldots B_{t-1} \; B_t \ldots B_l$

$\Rightarrow x = e.$

Similarly for other intersections.

$\therefore \quad C = < b_1^{p^m} > \times \ldots\ldots \times < b_{t-1}^{p^m} >$

Thus $o(C) = o(b_1^{p^m}) \ldots\ldots o(b_{t-1}^{p^m})$

$$= \frac{o(b_1)}{(p^m, o(b_1))} \ldots \frac{o(b_{t-1})}{(p^m, o(b_{t-1}))}$$

$$= \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m}$$

Now $G = A_1 \times \ldots\ldots \times A_k = < a_1 > \times \ldots\ldots \times < a_k >$ and $C \leq G$

$\Rightarrow C = < a_1^{p^m} > \times \ldots\ldots \times < a_k^{p^m} >$

$$\Rightarrow o(C) = \frac{o(a_1)}{(p^m, o(a_1))} \ldots\ldots \frac{o(a_k)}{(p^m, o(a_k))}$$

$$= \frac{p^{n_1}}{(p^m, p^{n_1})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

Since $n_1 = h_1, \ldots, n_{t-1} = h_{t-1}$

$$o(C) = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

NOTES

So, $\frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$

NOTES

$$\Rightarrow \quad 1 = \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\geq \frac{p^{n_t}}{(p^m, p^{n_t})}, \text{ as } \frac{p^{n_j}}{(p^m, p^{n_j})} \geq 1$$

$$> 1 \text{ as } n_t > m \quad \Rightarrow (p^m, p^n t) = p^m$$

$$\Rightarrow \frac{p^{n_t}}{(p^m, p^{n_t})} = \frac{p^{n_t}}{p^m} = p^{n_t - m} > 1$$

a contradiction.

$\therefore$ $n_i = h_i$ for all i

So, $o(G) = o(A_1) \ldots\ldots o(A_k) = o(B_1) \ldots\ldots o(B_l)$

$\Rightarrow$ $p^{n1} \ldots\ldots\ldots p^{nk} = p^{h1} \ldots\ldots\ldots p^{ht}$

If $k > l$, $p^{n1} \ldots\ldots\ldots p^{nt}\, p^{nt+1} \ldots\ldots\ldots p^{nk} = p^{h1} \ldots\ldots\ldots p^{ht}$.

$\Rightarrow$ $p^{nl+1} \ldots\ldots\ldots p^{nk} = 1$ as $n_i = h_i$ for all i

which is not true.

$\therefore$ k is not greater then l. Similarly l is not greater than k.

$\therefore$ $k = l$.

Problem 1: *Let G be the finite abelian group of order mp^n where $p \nmid m$. Then show that G is IDP of H and K where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$ and also that $o(H) = p^n$.*

Solution: It can be easily checked that H and K are subgroups of G.

We show $G = HK$, $HK = \{e\}$

Now as $p \nmid m$, g.c.d. $(p^n, m) = 1$ and thus there exist integers s, t such that

$$1 = sm + tp^n$$

If $x \in G$ be any element then

$$x = x^{sm+tp^n} = x^{sm} \cdot x^{tp^n}$$

Now $\left(x^{sm}\right)^{p^n} = \left(x^{p^n m}\right)^s = e^s = e \qquad (a^{o(G)} = e)$

$$\Rightarrow x^{sm} \in H$$

Again $\left(x^{tp^n}\right)^m = \left(x^{p^n m}\right)^t = e^t = e \Rightarrow x^{tp^n} \in K$

So $x \in HK \Rightarrow G \subseteq HK \Rightarrow G = HK$

NOTES

Let now $x \in H \cap K \Rightarrow x \in H$ and $x \in K$

$\Rightarrow x^{p^n} = e$ and $x^m = e$

$\Rightarrow o(x) \mid p^n$ and $o(x) \mid m$

$\Rightarrow o(x) = 1$ as $(p^n, m) = 1$

$\Rightarrow x = e$ or that $H \cap K = \{e\}$

Since G is abelian, H, K are normal subgroups and hence G is IDP of H and K.

Again, $$p^n m = o(G) = o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)} = o(H) \cdot o(K)$$

If, $p|o(K)$, then by Cauchy's theorem $\exists\, k \in K$ s.t., $o(k) = p$. Also $k \in K \Rightarrow k^m = e$ (by definition of K) and so $p \mid m$, which is not true. Thus $p \nmid o(K)$ or that $o(K)$ is not a multiple of p and hence $o(H) = p^n$.

A beautiful application of theorem 4 is

Theorem 5: *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*

Proof: Suppose G, G' are finite abelian groups of order p^n. Let G and G' be isomorphic and θ be an isomorphism from G onto G'.

Let $G = A_1 \times \ldots \times A_k$, $A_i = \langle a_i \rangle$, $o(A_i) = p^{n_i}$

Since θ is an isomorphism, $\theta(A_i)$ is normal subgroups of G' for all $i = 1,\ldots, k$.

$\therefore\ \theta(A_1) \ldots\ldots \theta(A_k)$ is a subgroup of G

Also $g' \in G' \Rightarrow \exists\, g \in G$ s.t. $\theta(g) = g$

$g \in G \Rightarrow g = x_1 \ldots\ldots x_k,\ x_i \in A_i$

$\Rightarrow g' = \theta(g) = \theta(x_1) \ldots\ldots \theta(x_k)$

$\in \theta(A_1) \ldots\ldots \theta(A_k)$

$\Rightarrow G' \subseteq \theta(A_1) \ldots\ldots \theta(A_k)$

$\Rightarrow G' = \theta(A_1) \ldots\ldots \theta(A_k)$

Also, $\theta(A_1) \cap \theta(A_2) \ldots \theta(A_k) = \{e'\}$, e' = identity of G'

as $x \in \theta(A_1), x \in \theta(A_2) \ldots\ldots \theta(A_k)$

$\Rightarrow x = \theta(x_1) = \theta(x_2) \ldots\ldots \theta(x_k),\ x_i \in A_i$

$\Rightarrow \theta(x_1) = \theta(x_2 \ldots\ldots x_k)$

$\Rightarrow x_1 = x_2 \ldots\ldots x_k$

$\Rightarrow x_1^{-1} x_2 \ldots\ldots x_k = e$

$\Rightarrow x_i = e$ for all i

$\Rightarrow x = e$.

Similarly for other intersections.

$\therefore\ G' = \theta(A_1) \times ... \times \theta(A_k)$. Since $A_i = < a_i >$, $\theta(A_i) = < \theta(a_i) >$.

So $o(\theta(A_i)) = o(\theta(a_i)) = o(a_i)$ for all i

$= p^{n_i}$ for all i

NOTES

Thus, G and G' have same invariants.

Conversely, suppose G and G' have same invariants.

Let $G = A_1 \times ... \times A_k$, $A_i = < a_i >$

Then $G' = B_1 \times ... \times B_k$, $B_i = < b_i >$, $o(A_i) = o(B_i)$

as G and G' have same invariants.

But any two cyclic groups of same order are isomorphic. A_i and B_i are isomorphic for all i. So $A_1 \times ... \times A_k = G$ and $B_1 \times ... \times B_k = G'$ are isomorphic.

We are now in a position to specify the number of non-isomorphic finite abelian groups of order p^n through

Theorem 6: *The number of non-isomorphic abelian groups (or number of distinct isomorphism classes of abelian groups) of order p^n, p a prime, equals the number of partitions of n.*

Proof: Let G be an abelian group of order p^n.

By theorem 4, $G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$

$o(G) = o(A_1) \ ... \ o(A_k)$

$\Rightarrow\ p^n = p^{n1} ... \ p^{nk} = p^{n1 + ... + nk}$

$\Rightarrow\ n = n_1 + ... + n_k,\ \ n_1 \geq n_2 \geq ..... \geq n_k > 0$

is a partition of n.

Conversely, consider any partition of n.

Let $n = n_1 + ... + n_k,\ \ n_1 \geq n_2 \geq ... \geq n_k > 0$

be a partition of n.

Let A_i be a cyclic group of order p^{n_i} for all i.

Let $G = A_1 \times ... \times A_k$. Then G is an abelian groups of order $p^{n1 + ... + nk} = p^n$.

Let A = set of all non-isomorphic abelian groups of order p^n.

B = set of all partitions of n.

Define θ: A $\rightarrow$ B as follows:

Let $G \in$ A. Let $G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$.

Let $\theta(G) = n_1 + ... + n_k = n$

Clearly, θ is well defined.

Also $\theta(G) = \theta(G')$

$\Rightarrow\ n_1 + ... + n_k = m_1 + ... + m_l = n$

$\Rightarrow\ k = l,\ n_i = m_i$ for all i

NOTES

$\Rightarrow$ G and G' have same invariants

$\Rightarrow$ G and G' are isomorphic

$\Rightarrow$ $G = G'$

$\Rightarrow$ θ is 1–1

Let $n = n_1 + ... + n_k$, $n_1 \geq n_2 \geq ... \geq n_k > 0$ be a partition of n. Then as seen above $G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$ is an abelian group of order p^n and

$$\theta(G) = n_1 + ... + n_k$$

$\therefore$ θ is onto.

$\therefore$ $o(\text{A}) = o(\text{B})$, which proves the result.

It is not difficult to prove that two finite abelian groups are isomorphic if and only if their Sylow subgroups are isomorphic. Now from theorem 6, we get

Theorem 7: *Let $n = p_1^{\alpha 1} ... p_r^{\alpha r}$ where p_is are distinct primes. Then the number of non-isomorphic abelian groups of order n is $p(\alpha_1)\ p(\alpha_2).....p(\alpha_r)$ where $p(\alpha_i)$ denotes the number of partitions of α_i.*

Problem 2: *Find all the non-isomorphic abelian groups of order*

(*i*) 8 (*ii*) 6 (*iii*) 20 (*iv*) 360.

Solution:

(*i*) Since $8 = 2^3$, the number of non-isomorphic abelian groups of order 8 is given by $p(3)$, where $p(3)$ denotes the number of partitions of 3.

Since $p(3) = 3$ and $3 = 3$

$$3 = 2 + 1$$

$$3 = 1 + 1 + 1$$

The number of non isomorphic abelian groups of order 8 is 3. The groups are

$$\mathbf{Z}_{2^3},\ \mathbf{Z}_{2^2} \times \mathbf{Z}_2,\ \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$$

i.e., $\mathbf{Z}_8,\ \mathbf{Z}_4 \times \mathbf{Z}_2,\quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

(*ii*) As $6 = 2^1 \times 3^1$, the number of non-isomorphic abelian groups is $p(1)\,p(1) = 1.\ 1 = 1$. The groups being the cyclic groups $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.

(*iii*) As $20 = 2^2 \times 5^1$, the number of non-isomorphic abelian groups of order 20 is given by

$$p(2)\ p(1) = 2.\ 1 = 2$$

The groups being $\mathbf{Z}_4 \times \mathbf{Z}_5$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5$.

(*iv*) $o(G) = 360 = 2^3 \times 3^2 \times 5^1$

The number of non isomorphic abelian groups of order 360 is

$p(3)p(2)p(1) = 3 \times 2 \times 1 = 6$ and as

NOTES

$3 = 3, \quad 3 = 2 + 1, \quad 3 = 1 + 1 + 1$

$2 = 2, \quad 2 = 1 + 1,$ we have these six groups to be

$\mathbf{Z}_{2^3} \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_8 \times \mathbf{Z}_9 \times \mathbf{Z}_5 \cong Z_{360}$

$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_5$

$\mathbf{Z}_{2^3} \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 = \mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5 = \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

Problem 3: *Suppose G is an abelian group of order 120 and suppose G has exactly three elements of order 2. Find the isomorphism class of G.*

Solution: $o(G) = 120 = 2^3 \times 3 \times 5$

So the number of non isomorphic abelian groups of order 120 will be $p(3)p(1)p(1) = 3.1.1 = 3$ and these are

$$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \cong \mathbf{Z}_{120}$$
$$\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$$
$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5.$$

$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has only one element (4, 0, 0) of order 2 so it cannot be G

Again, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has (1,1,1,0,0), (1,0,1,0,0), (0,1,1,0,0) and (1,1,0,0,0) as elements of order 2,

so it cannot be G,

whereas $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ has exactly three elements

(2, 1, 0, 0), (0, 1, 0, 0), (2, 0, 0, 0)

which have order 2 and hence G is $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

Problem 4: *Let G be a finite abelian group under addition. Let n be a +ve integer. Define* $nG = \{nx \mid x \in G\}$ *and* $G[n] = \{x \in G \mid nx = 0\}$ *then show that nG and G[n] are subgroups of G and* $\frac{G}{G[n]} \cong nG$.

Solution: We use 0 to denote identity of G.

Since $nx, ny \in nG \Rightarrow nx - ny = n(x - y) \in nG, 0 = n.0 \in nG, nG$ is a subgroup. Similarly one can see that $G[n]$ is a subgroup.

Define a mapping $\theta : G \to nG$, s.t.,

$$\theta(x) = nx$$

then θ is a well defined onto homomorphism

$$\theta(x + y) = n(x + y) = nx + ny = \theta(x) + \theta(y) \text{ etc.,}$$

Thus by Fundamental theorem of group homomorphism $nG \cong \frac{G}{Ker\,\theta}$

NOTES

Now $x \in Ker\theta \Rightarrow \theta(x) = 0 \Rightarrow nx = 0 \Rightarrow n \in G[n]$

confirms that $\frac{G}{G[n]} \cong nG$.

Remark: If binary composition of G is multiplication, the above subgroup $G[n]$ will be $\{x \in G \mid x^n = e\}$ and we can denote it by G_n. Again the subgroups nG will be $\{x^n \mid x \in G\}$ and we can denot it by G^n. We have thus shown that $\frac{G}{Gn} \cong G^n$.

It can be a good exercise for the reader to write the above proof independently under the multiplicative composition.

Problem 5: *Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ be the group under multiplication modulo 69. Express G as EDP and IDP of cyclic groups.*

Solution: $o(G) = 8 = 2^3$, thus as seen in problem 2 above the number of non isomorphic abelian groups is $p(3) = 3$ and these are

$$\mathbf{Z}_8,\ \mathbf{Z}_2 \times \mathbf{Z}_4 \quad \mathbf{Z}_2,\ \mathbf{Z}_2 \times \mathbf{Z}_2$$

Again, we notice that the elements 7, 23, 55 have order 4 and the elements 17, 49, 65, 71 have order 2 in G.

Since $\mathbf{Z}_8$ has an element of order 8 and G has no element of order 8, therefore, G is not $\mathbf{Z}_8$

Again $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ has no element of order 4 and so we are left with the only choice that G is $\mathbf{Z}_4 \times \mathbf{Z}_2$

To write G as IDP of cyclic groups, we pick up an element of maximum order 4 (see theorem 2), say, 7 then $< 7 > = \{7, 49, 55, 1\} = H$ is one of the factors.

Again, taking an element of order 2, say 65, we get $< 65 > = \{65, 1\} = K$. Here

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)} = \frac{4 \times 2}{1} = 8 = o(G)$$

thus $G = HK$, $H \cap K = \{1\}$ and hence this is an expression of G as IDP of H & K.

This expression is not unique as we can have other representations e.g., $G = < 7 > \cdot < 17 >$ or $< 23 > \cdot < 65 >$

Problem 6: *Let G be a finite abelian group. Let $b \in G$ be an element of largest order in G. Show that o(a) divides o(b) $\forall\ a \in G$.*

Solution: Now $G = C_1 \times C_2 \times \ldots \times C_k$, where $C_i = \langle x_i \rangle$, $o(C_i) = o(x_i) = m_i$ such that $m_1 \mid m_2 \mid \ldots \mid m_{k-1} \mid m_k$.

Consider $(e, e, \ldots, e, x_k) \in G$.

NOTES

Then $(e, e, ..., e, x_k)^{mk}$ = identity of G and if $(e, e, ..., e, x_k)^r = e$

$\Rightarrow \quad x_k^r = e \Rightarrow o(x_k) = m_k | r \Rightarrow r \geq m_k$.

So, $o(e, e, ..., e, x_k) = m_k$

Let $(y_1, y_2, ..., y_k) \in G$.

Then $(y_1, y_2, ..., y_k)^{mk} = e$ as $o(y_i) | o(C_i) = m_i \mid m_k \ \forall \ i$

$\Rightarrow \quad o((y_1, y_2, ..., y_k))$ divides m_k

$\Rightarrow \quad m_k$ is the largest order in G and order of each element in G divides m_k.

Problem 7: *Prove that an abelian group of order $2^n (n \geq 1)$ must have an odd number of elements of order 2.*

Solution: Let $o(G) = 2^n$, $n \geq 1$.

Then $G = C_1 \times C_2 \times ... \times C_k$, where each C_i is cyclic.

The elements $(a_1, e, ..., e)$, $(e, a_2, e, ..., e)$, ..., $(e, e, ..., e, a_k)$ are of order 2 where $o(a_i) = 2 \ \forall \ i$.

This gives k_{C_1} elements of order 2.

Similarly, $(a_1, a_2, e, ..., e)$, $(a_1, e, a_3, e, ..., e)$, ..., are elements of order 2. This gives k_{C_2} elements of order 2 in G.

In this way, the number of elements of order 2 in G is $k_{C_1} + k_{C_2} + ... + k_{C_k}$

$$= 1 + k_{C_1} + k_{C_2} + ... + k_{C_k} - 1$$

$$= (1 + 1)^k - 1 = 2^k - 1 \text{ which is odd number.}$$

Note that there is unique element a_i of order 2 in each C_i.

Table showing groups of order upto 15.

Order of group	*Abelian*	*Non-abelian*
15	$\mathbf{Z}_{15}$	Nil
14	$\mathbf{Z}_{14}$	D_{14}
13	$\mathbf{Z}_{13}$	Nil
12	$\mathbf{Z}_{12}, \mathbf{Z}_2 \times \mathbf{Z}_6$	A_4, D_{12}, Q_{12}
11	$\mathbf{Z}_{11}$	Nil
10	$\mathbf{Z}_{10}$	D_{10}
9	$\mathbf{Z}_9, \mathbf{Z}_3 \times \mathbf{Z}_3$	Nil
8	$\mathbf{Z}_8, \mathbf{Z}_2 \times \mathbf{Z}_4$ $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$	D_8, Quaternion group
7	$\mathbf{Z}_7$	Nil
6	$\mathbf{Z}_6$	S_3
5	$\mathbf{Z}_5$	Nil
4	$\mathbf{Z}_4, \mathbf{Z}_2 \times \mathbf{Z}_2$	Nil
3	$\mathbf{Z}_3$	Nil
2	$\mathbf{Z}_2$	Nil
1	$\mathbf{Z}_1$	Nil

Check Your Progress

1. What is an abelian group?
2. Give an example of abelian groups.
3. What is the fundamental theorem on finite abelian groups?

NOTES

7.3 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. An abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written.
2. Cyclic groups are good examples of abelian groups.
3. A finite abelian group is direct product of cyclic groups of prime power order.

7.4 SUMMARY

- A finite abelian group is a direct product of groups of prime power order.
- A finite abelian group is direct product of cyclic groups of prime power order. (Representation being unique).
- Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.
- Two finite abelian groups are isomorphic if and only if their Sylow subgroups are isomorphic.
- The number of non-isomorphic abelian groups of order p^n, where p is prime, equals the number of partitions of n.

7.5 KEY WORDS

- ***p*-group:** A group is called a p-group if order of each element of the group is some power of p, where p is prime.
- **Abelian group:** A group in which the result of applying the group operation to two group elements does not depend on the order in which they are written.
- **Isomorphic:** An isomorphism is a homomorphism or morphism that can be reversed by an inverse morphism. Two mathematical objects are isomorphic if an isomorphism exists between them.

7.6 SELF ASSESSMENT QUESTIONS AND EXERCISES

NOTES

Short Answer Questions

1. Find all the non-isomorphic abelian group of order 8.
2. Find all the non-isomorphic abelian group of order 360.
3. If p is a prime not dividing $o(G)$, show that $pG \cong G$, where G is a finite additive abelian group.

Long Answer Questions

1. Prove the fundamental theorem on finite abelian groups.
2. Show that two abelian groups of order p^n are isomorphic if and only if they have the same invariants.
3. If G is a finite abelian group and $o(G) = p_1 p_2, \ldots . p_n$ where $p_i s$ are distinct primes, show that G is cyclic.
4. Show that $U_{15} \cong U_{16}$.

7.7 FURTHER READINGS

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. Elements of Modern Algebra. Boston: Cengage Learning.

Zassenhaus, Hans J. 2013. *The Theory of Groups*. Chelmsford: Courier Corporation.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

UNIT 8 RING THEORY

NOTES

Structure

8.0 INTRODUCTION

A group you noticed is a system with a non-empty set and a binary composition. One can of course talk about non empty sets with two binary compositions also, the set of integers under usual addition and multiplication being an example. Though this set forms a group under addition and not under multiplication, it does have certain specific properties satisfied with respect to multiplication as well. The unit singles out some of these and generalize the concept in the form of a ring. This unit starts with the formal definition and generalize the concept in the form of a ring.

8.1 OBJECTIVES

After going through this unit, you will be able to:

- Define and generalize various concepts of ring theory
- Solve problems based on rings
- Know about special classes of rings

8.2 DEFINITIONS AND EXAMPLES OF RINGS

Definition: A non empty set R, together with two binary compositions + and . is said to form a *Ring* if the following axioms are satisfied:

(*i*) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$

(*ii*) $a + b = b + a$ for $a, b \in R$

(*iii*) $\exists$ some element 0 (called zero) in R, s.t., $a + 0 = 0 + a = a$ for all $a \in R$

(*iv*) for each $a \in R$, $\exists$ an element $(-a) \in R$, s.t., $a + (-a) = (-a) + a = 0$

(*v*) $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$ for all $a, b, c \in R$

NOTES

(vi) $a \,.\, (b + c) = a \,.\, b + a \,.\, c$

$(b + c) \,.\, a = b \,.\, a + c \,.\, a$ for all $a, b, c \in R$

Remarks: (a) Since we say that + and . are binary compositions on R, it is understood that the closure properties w.r.t. these hold in R. In other words, for all $a, b \in R$, $a + b$ and $a \,.\, b$ are unique in R.

(b) One can use any other symbol instead of + and ., but for obvious reasons, we use these two symbols (the properties look so natural with these). In fact, in future, the statement that R is a ring would mean that R has two binary compositions + and . defined on it and satisfies the above axioms.

(c) Axiom (v) is named associativity w.r.t. . and axiom (vi) is referred to as distributivity (left and right) w.r.t. . and +.

(d) Axioms (i) to (iv) could be restated by simply saying that $< R, + >$ forms an abelian group.

(e) Since 0 in axiom (iii) is identity w.r.t. +, it is clear that this element is unique (see groups).

Definitions: A ring R is called a *commutative* ring if $ab = ba$ for all $a, b \in R$. Again if $\exists$ an element $e \in R$ s.t.,

$$ae = ea = a \quad \text{for all } a \in R$$

we say, R is a ring with *unity*. Unity is generally denoted by 1. (It is also called unit element or multiplicative identity).

It would be easy to see that if unity exists in a ring then it must be unique.

Remark: We recall that in a group by a^2 we meant $a \,.\, a$ where '.' was the binary composition of the group. We continue with the same notation in rings as well. In fact, we also introduce similar notation for addition, and shall write na to mean $a + a + ...+ a$ (n times), n being an integer.

Example 1: Sets of real numbers, rational numbers, integers form rings w.r.t. usual addition and multiplication. These are all commutative rings with unity.

Example 2: Set **E** of all even integers forms a commutative ring, without unity (under usual addition and multiplication).

Example 3: (a) Let M be the set of all 2×2 matrices over integers under matrix addition and matrix multiplication. It is easy to see that M forms a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, but is not commutative.

(b) Let M be set of all matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ over integers under matrix addition and multiplication. Then M forms a non commutative ring without unity.

Example 4: The set $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ forms a ring under addition and multiplication modulo 7. (In fact, we could take n in place of 7).

Example 5: The set $R = \{0, 4, 6\}$ under addition and multiplication modulo 6 forms a commutative ring with unity. The composition tables are

$\oplus$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\odot$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

NOTES

Since $0 \odot 4 = 0$, $2 \odot 4 = 2$, $4 \odot 4 = 4$, we notice 4 is unity of R.

Example 6: Let F be the set of all continuous functions $f : \mathbf{R} \to \mathbf{R}$, where $\mathbf{R}$ = set of real numbers. Then F forms a ring under addition and multiplication defined by:

for any $f, g \in F$

$(f + g)x = f(x)$ for all $x \in \mathbf{R}$

$(f\,g)x = f(x)g(x)$

for all $x \in \mathbf{R}$

zero of this ring is the mapping $O : \mathbf{R} \to \mathbf{R}$, s.t.,

$$O(x) = 0 \text{ for all } x \in \mathbf{R}$$

Also additive inverse of any $f \in F$ is the function $(-f) : \mathbf{R} \to \mathbf{R}$ s.t., $(-f)x = -f(x)$

In fact, F would have unity also, namely the function $i : \mathbf{R} \to \mathbf{R}$ defined by $i(x) = 1$ for all $x \in \mathbf{R}$.

Remark: Although the same notation fg has been used for product here it should not be mixed up with fog defined earlier.

Example 7: Let $\mathbf{Z}$ be the set of integers, then $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ forms a ring under usual addition and multiplication of complex numbers. $a + ib$ where $a, b \in \mathbf{Z}$ is called a Gaussian integer and $\mathbf{Z}[i]$ is called the ring of Guassian integers.

We can similarly get $\mathbf{Z}_n[i]$ the ring of Gaussian integers modulo n. For instance,

$$\mathbf{Z}_3[i] = \{a + ib \mid a, b \in \mathbf{Z}_3 = \{0, 1, 2\} \bmod 3\}$$
$$= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$$

Example 8: Let X be a non empty set. Then $P(X)$ the power set of X (*i.e.*, set of all subsets of X) forms a ring under + and · defined by

$$A + B = (A \cup B) - (A \cap B)$$
$$A \,.\, B = A \cap B$$

In fact, this is a commutative ring with unity and also satisfies the property $A^2 = A$ for all $A \in P(X)$.

Example 9: Let M = set of all 2×2 matrices over members from the ring of integers modulo 2. *It would be a finite non commutative ring*. M would have $2^4 = 16$ members as each element a, b, c, d in matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ can be chosen in 2 ways. Compositions in M are given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \oplus x & b \oplus y \\ c \oplus z & d \oplus u \end{bmatrix}$$

where $\oplus$ denotes addition modulo 2 and

NOTES

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \otimes x \oplus b \otimes z & a \otimes y \oplus b \otimes u \\ c \otimes x \oplus d \otimes z & c \otimes y \oplus d \otimes u \end{bmatrix}$$

$\otimes$ being multiplication modulo 2.

That M is non commutative follows as $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

But $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Example 10: Let $R = \{0, a, b, c\}$. Define + and . on R by

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

Then one can check that R forms a non commutative ring without unity. In fact it is an example of the smallest non commutative ring.

8.3 SOME SPECIAL CLASSES OF RINGS

Theorem 1: *In a ring R, the following results hold*

(*i*) $a \cdot 0 = 0 \cdot a = 0$ *for all* $a \in R$

(*ii*) $a(-b) = (-a)b = -ab$ *for all* $a, b \in R$

(*iii*) $(-a)(-b) = ab$. $\forall\ a, b \in R$

(*iv*) $a(b - c) = ab - ac$. $\forall\ a, b, c \in R$

Proof: (*i*) $a \cdot 0 = a \cdot (0 + 0)$

$\Rightarrow$ $a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow$ $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow$ $0 = a \cdot 0$

using cancellation w.r.t + in the group $< R, + >$.

(*ii*) $a \cdot 0 = 0$

$\Rightarrow$ $a(-b + b) = 0$

$\Rightarrow$ $a(-b) + ab = 0$

$\Rightarrow$ $a(-b) = -(ab)$

similarly $(-a)\,b = -ab$.

(*iii*) $(-a)\,(-b) = -[a\,(-b)] = -[-ab] = ab$

(*iv*) $a\,(b-c) = a\,(b+(-c))$

$= ab + a\,(-c)$

$= ab - ac$.

NOTES

Remarks: (*i*) If R is a ring with unity and $1 = 0$, then since for any $a \in R$, $a = a.1 = a.0 = 0$, we find $R = \{0\}$ which is called the *trivial* ring. We generally exclude this case and thus whenever, we say R is a ring with unity, it will be understood that $1 \neq 0$ in R.

(*ii*) If n, m are integers and a, b elements of a ring, then it is easy to see that

$$n(a+b) = na + nb$$

$$(n+m)a = na + ma$$

$$(nm)a = n(ma)$$

$$a^m\ a^n = a^{m+n}$$

$(a^m)^n = a^{mn}$ (see under groups).

Problem 1: *Let $<R, +, .>$ be a ring where the group $<R, +>$ is cyclic. Show that R is a commutative ring:*

Solution: Let $< R, + >$ be generated by a. Let $x, y \in R$ be any two elements, then $x = ma$, $y = na$ for some integers m, n.

Now $xy = (ma)(na)$

$= (a + a + ... + a)(a + a + ... + a)$

m times $\qquad$ n times

$= (mn)a^2 = (nm)a^2 = (na)(ma) = yx$

We are so much used to the property that whenever $ab = 0$ then either $a = 0$ or $b = 0$ that it may need more than a bit of convincing that the result may not always be true. Indeed in the ring of integers (or reals or rationals) this property holds. But if we consider the ring of 2×2 matrices over integers, we notice, we can have two non zero elements A, B s.t, $AB = 0$, but $A \neq 0$ $B \neq 0$. In fact, take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ then $A \neq 0$, $B \neq 0$. But $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. We formalise this notion through

Definition: Let R be a ring. An element $0 \neq a \in R$ is called a *zero-divisor*, if $\exists$ an element $0 \neq b \in R$ s.t., $ab = 0$ or $ba = 0$.

Definition: A commutative ring R is called an *Integral domain* if $ab = 0$ in $R \Rightarrow$ either $a = 0$ or $b = 0$. In other words, a commutative ring R is called an integral domain if R has no zero divisors.

NOTES

An obvious example of an integral domain is $< \mathbf{Z}, +, \cdot >$ the ring of integers whereas the ring of matrices, talked about above is an example of a ring which is not an integral domain. Again, $\mathbf{Z} \times \mathbf{Z}$ will not be an integral domain.

Remark: Some authors do not insist upon the condition of commutativity as a part of the definition of an integral domain. One can have (see examples 11, 12 ahead), non commutative rings without zero divisors.

The following theorem gives us a necessary and sufficient condition for a commutative ring to be an integral domain.

Theorem 2: *A commutative ring R is an integral domain iff for all* $a, b, c \in R$ $(a \neq 0)$

$$ab = ac \Rightarrow b = c.$$

Proof: Let R be an integral domain

Let $ab = ac \quad (a \neq 0)$

Then $ab - ac = 0$

$\Rightarrow$ $a(b - c) = 0$

$\Rightarrow$ $a = 0$ or $b - c = 0$

Since $a \neq 0$, we get $b = c$.

Conversely, let the given condition hold.

Let $a, b \in R$ be any elements with $a \neq 0$.

Suppose $ab = 0$

then $ab = a.0$

$\Rightarrow$ $b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark: A ring R is said to satisfy *left cancellation law* if for all $a, b, c \in R$, $a \neq 0$

$$ab = ac \Rightarrow b = c.$$

Similarly we can talk of *right cancellation law*. It might, of course, be noted that cancellation is of only non zero elements.

Definition: An element a in a ring R with unity, is called invertible (or a *unit*) w.r.t. multiplication if $\exists$ some $b \in R$ such that $ab = 1 = ba$.

Notice, unit and unit element (unity) are different concepts and should not be confused with each other.

Definition: A ring R with unity is called a *Division ring* or a *skew field* if non zero elements of R form a group w.r.t. multiplication.

In other words, a ring R with unity is a Division ring if non zero elements of R have multiplicative inverse.

NOTES

Definition: A commutative division ring is called a *field*.

Real numbers form a field, whereas integers do not, under usual addition and multiplication. Since a division ring (field) forms groups w.r.t. two binary compositions, it must contain two identity elements 0 and 1 (w.r.t. addition and multiplication) and thus a division ring (field) has at least two elements (see remark on page 227).

Example 11: A *division ring which is not a field*. Let M be the set of all 2×2 matrices of the type $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ where a, b are complex numbers and $\bar{a}, \bar{b}$ are their conjugates, *i.e.*, if $a = x + iy$ then $\bar{a} = x - iy$. Then M is a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ under matrix addition and matrix multiplication.

Any non zero element of M will be $\begin{bmatrix} x+iy & u+iv \\ -(u-iv) & x-iy \end{bmatrix}$

where x, y, u, v are not all zero.

One can check that the matrix $\begin{bmatrix} \frac{x-iy}{k} & -\frac{u+iv}{k} \\ \frac{u-iv}{k} & \frac{x+iy}{k} \end{bmatrix}$

where $k = x^2 + y^2 + u^2 + v^2$, will be multiplicative inverse of the above non zero matrix, showing that M is a division ring. But M will not be a field as it is not commutative as

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

But $$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

Example 12: Consider

$D = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$ with $i^2 = j^2 = k^2 = -1$, then D forms a ring.

Two elements $a + bi + cj + dk$ and $a' + b'i + c'j + d'k$ are equal iff $a = a'$, $b = b'$, $c = c'$, $d = d'$.

Addition and multiplication on D are defined by

$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$

and

NOTES

$(a + bi + cj + dk)\,(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' - bd' + ca' - db')j + (ad' + bc' - ab' + da')k$

The symbol + in the elements of D is just a notation and is not to be a confused with addition in real numbers. We identify element $o + 1i + oj + ok$ by i and so on.

Thus since $i = 0 + 1i + 0j + 0k$

$j = 0 + 0i + 1j + 0k$

We have $ij = k, ji = -k$, etc., In fact that shows that D is non commutative. D has unity $1 = 1 + 0i + 0j + 0k$

If $a + bi + cj + dk$ be any non zero element of D (*i.e.*, at least one of a, b, c, d is non zero) then $(a + bi + cj + dk)\dfrac{(a - bi - cj - dk)}{a^2 + b^2 + c^2 + d^2} = 1$.

Hence D is a division ring but not a field.

The elements of D can also be written as quadruples (a, b, c, d).

This ring D is called the *ring of quaternions*.

Theorem 3: *A field is an integral domain.*

Proof: Let $< R, +, . >$ be a field, then R is a commutative ring.

Let $ab = 0$ in R. We want to show either $a = 0$ or $b = 0$. Suppose $a \neq 0$, then a^{-1} exists (definition of field)

thus $ab = 0$

$\Rightarrow a^{-1}(ab) = a^{-1}0$

$\Rightarrow b = 0.$

which shows that R is an integral domain.

Remark: Similarly we can show that a division ring is an integral domain and thus has no zero divisiors.

A 'partial converse' of the above result also holds.

Theorem 4: *A non zero finite integral domain is a field.*

Proof: Let R be a non zero finite integral domain.

Let R' be the subset of R containing non zero elements of R.

Since associativity holds in R, it will hold in R'. Thus R' is a finite semi group.

Again cancellation laws hold in R (for non zero elements) and therefore, these hold in R'.

Hence R' is a finite semi group w.r.t. multiplication in which cancellation laws hold.

$\therefore < R', \cdot >$ forms a group. Note closure holds in R' as R is an integral domain.

In other words $< R, +, \cdot >$ is a field (it being commutative as it is an integral domain).

NOTES

Aliter: Let $R = \{a_1, a_2, ..., a_n\}$ be a finite non zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, ..., aa_n$ are all in R and if $aa_i = aa_j$ for some $i \neq j$, then by cancellation we get $a_i = a_j$ which is not true. Hence $aa_1, aa_2, ..., aa_n$ are distinct members of R.

Since $a \in R$, $a = aa_i$ for some i

Let $x \in R$ be *any* element, then $x = aa_j$ for some j

Thus $ax = (aa_i)x = a(a_ix)$

i.e., $x = a_ix$

Hence using commutativity we find

$$x = a_ix = xa_i$$

or that a_i is unity of R. Let $a_i = 1$

Thus for $1 \in R$, since $1 = aa_k$ for some k

We find a_k is multiplicative inverse of a. Hence any non zero element of R has multiplicative inverse or that R is a field.

Example 13: An infinite integral domain which is not a field is the ring of integers.

Definition: A ring R is called a *Boolean ring* if $x^2 = x$ for all $x \in R$.

Example 14: The ring $\{0, 1\}$ under addition and multiplication mod 2 forms a Boolean ring.

Problem 2: *Show that a Boolean ring is commutative.*

Solution: Let $a, b \in R$ be any elements

Then $a + b \in R$ (closure)

By given condition

$$(a + b)^2 = a + b$$

$$\Rightarrow \quad a^2 + b^2 + ab + ba = a + b$$

$$\Rightarrow \quad a + b + ab + ba = a + b$$

$$\Rightarrow \quad ab + ba = 0$$

$$\Rightarrow \quad ab = -ba \qquad ...(1)$$

$$\Rightarrow \quad a(ab) = a(-ba)$$

$$\Rightarrow \quad a^2b = -aba$$

$$\Rightarrow \quad ab = -aba \qquad ...(2)$$

Again (1) gives

$$(ab)a = (-ba)a$$

$$\Rightarrow \quad aba = -ba^2 = -ba \qquad ...(3)$$

(2) and (3) give

$$ab = ba \ (= -aba)$$

or that R is commutative.

NOTES

Problem 3: *Show that order of a finite Boolean ring is of the type 2^n, $n = 0, 1, 2,....$*

Solution: : Let $< R, +, . >$ be a finite Boolean ring. Then $a^2 = a \ \forall \ a \in R$,

Thus $(a + a)^2 = a + a$

$\Rightarrow a^2 + a^2 + 2aa = a + a$

$\Rightarrow 2a^2 = 0$ or that $2a = 0 \quad \forall \ a \in R$

Thus each non zero element in the group $< R, + >$ has order 2.

By Cauchy's theorem in groups, we know if p is any prime dividing $o(R)$ then $\exists$ $x \in R$, s.t., $o(x) = p$. But order of each non zero element is 2 and thus 2 is the only prime dividing $o(R)$. Hence $o(R) = 2^n$.

Problem 4: (*a*) *Show that a non zero element a in* $\mathbf{Z}_n$ *is a unit iff a and n are relatively prime*.

(*b*) *If a is not a unit then it is a zero divisor.*

Solution: (*a*) $\mathbf{Z}_n = \{0, 1, 2, ..., n - 1\}$ mod n

Let $a \in \mathbf{Z}_n$ be a unit, then $\exists\ b \in \mathbf{Z}_n$ s.t.,

$$a \otimes b = 1$$

i.e., when ab is divided by n, remainder is 1, in other words,

$$ab = nq + 1$$

or $\quad ab - nq = 1$

$\Rightarrow$ a and n are relatively prime.

Conversely, let $(a, n) = 1$, then $\exists$ integers u, v s.t.,

$$au + nv = 1$$

$$\Rightarrow \quad au = n(-v) + 1$$

Suppose, $u = nq + r, \quad 0 \le r < n, \quad r \in \mathbf{Z}_n$,

Then $\quad au = anq + ar \ = n\ (-v) + 1$

$$\Rightarrow \quad ar \ = n\ (-v - aq) + 1, \quad r \in \mathbf{Z}_n$$

i.e., $\quad a \otimes r = 1, \quad r \in \mathbf{Z}_n$

i.e., $\quad a$ is a unit.

(*b*) Let a be not a unit and suppose g.c.d$(a, n) = d > 1$

Since $d \mid a$, $a = dk$ for some k. Also $d \mid n \Rightarrow n = dt$

$$\Rightarrow a.t = dk\ \frac{n}{d} = kn = 0 \text{ mod } n$$

i.e., a is a zero divisor.

Remark: In $\mathbf{Z}_n$, the set of units is U_n. Thus for instance, in $\mathbf{Z}_8$ 1, 3, 5, 7 are units.

Problem 5: *Show that* $\mathbf{Z}_p = \{0, 1, 2, ..., p-1\}$ *modulo p is a field iff p is a prime.*

NOTES

Solution: Let $\mathbf{Z}_p$ be a field. Suppose p is not a prime, then $\exists\ a, b$, such that $p = ab,\ 1 < a, b < p$

$\Rightarrow a \otimes b = 0$ where a, b are non zero $\Rightarrow \mathbf{Z}_p$ has zero divisors.

i.e. $\mathbf{Z}_p$ is not an integral domain, a contradiction as $\mathbf{Z}_p$ being a field is an integral domain.

Hence p is prime.

Conversely, let p be a prime. We need show that $\mathbf{Z}_p$ is an integral domain (it being finite will then be a field).

Let $a \otimes b = 0 \quad a, b \in \mathbf{Z}_p$

Then ab is a multiple of p

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$ (p being prime)

$\Rightarrow a = 0$ or $b = 0$ (Notice $a, b \in \mathbf{Z}_p \Rightarrow a\ , b < p$)

$\Rightarrow \mathbf{Z}_p$ is an integral domain and hence a field.

Remark : (*i*) We can also use problem 4 to prove this result.

(*ii*) Since $\mathbf{Z}_p$ is a field, all its non zero elements are units by definition of a field.

Problem 6: *If in a ring R, with unity,* $(xy)^2 = x^2y^2$ *for all* $x, y \in R$ *then show that R is commutative.*

Solution: Let $x, y \in R$ be any elements

then $y + 1 \in R$ as $1 \in R$

By given condition

$$(x(y + 1))^2 = x^2 (y + 1)^2$$

$$\Rightarrow (xy + x)^2 = x^2 (y + 1)^2$$

$$\Rightarrow (xy)^2 + x^2 + xyx + xxy = x^2(y^2 + 1 + 2y)$$

$$\Rightarrow x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$$

$$\Rightarrow xyx = x^2y \qquad ...(1)$$

Since (1) holds for all x, y in R, it holds for $x + 1, y$ also. Thus replacing x by $x + 1$, we get

$$(x + 1)\ y(x + 1) = (x + 1)^2y$$

$$\Rightarrow (xy + y)\ (x + 1) = (x^2 + 1 + 2x)y$$

$$\Rightarrow xyx + xy + yx + y = x^2y + y + 2xy$$

$$\Rightarrow yx = xy \text{ using (1)}$$

Hence R is commutative.

Problem 7: *Show that the ring R of real valued continuous functions on* [0, 1] *has zero divisors*.

Solution: Consider the functions f and g defined on [0, 1] by

NOTES

$$f(x) = \frac{1}{2} - x, \quad 0 \le x \le \frac{1}{2}$$

$$= 0, \quad \frac{1}{2} \le x \le 1$$

and $$g(x) = 0, \quad 0 \le x \le \frac{1}{2}$$

$$= x - \frac{1}{2}, \quad \frac{1}{2} \le x \le 1$$

then f and g are continuous functions and $f \neq 0$, $g \neq 0$

whereas $$gf(x) = g(x)\, f(x) \quad = 0 \cdot \left(\frac{1}{2} - x\right) \text{ if } 0 \le x \le \frac{1}{2}$$

$$= \left(x - \frac{1}{2}\right).0 = 0 \text{ if } \frac{1}{2} \le x \le 1$$

i.e., $gf(x) = 0$ for all x

i.e., $gf = 0$ but $f \neq 0$, $g \neq 0$.

Subrings

Definition: A non empty subset S of a ring R is said to be a *subring* of R if S forms a ring under the binary compositions of R.

The ring $< \mathbf{Z}, +, . >$ of integers is a subring of the ring $< \mathbf{R}, +, . >$ of real numbers.

If R is a ring then $\{0\}$ and R are always subrings of R, called *trivial* subrings of R.

It is obvious that a subring of an integral domain will be an integral domain.

In practice it would be difficult and lengthy to check all axioms in the definition of a ring to find out whether a subset is a subring or not. The following theorem would make the job rather easy.

Theorem 5: *A non empty subset S of a ring R is a subring of R iff* $a, b \in S \Rightarrow ab, a - b \in S$.

Proof: Let S be a subring of R

then $$a, b \in S \Rightarrow ab \in S \text{ (closure)}$$

$$a, b \in S \Rightarrow a - b \in S$$

as $< S, + >$ is a subgroup of $< R, + >$.

Conversely, since $a, b \in S \Rightarrow a - b \in S$, we find $< S, + >$ forms a subgroup of $< R, + >$. Again for any $a, b \in S$, since $S \subseteq R$

$$a, b \in R$$
$$\Rightarrow a + b = b + a$$

and so we find S is abelian.

By a similar argument, we find that multiplicative associativity and distributivity hold in S.

In other words, S satisfies all the axioms in the definition of a ring.

Hence S is a subring of R.

Definition: A non empty subset S of a field F is called a *subfield*, if S forms a field under the operations in F. Similarly, we can define a *subdivision ring* of a division ring.

One can prove that S will be a subfield of F iff $a, b \in S$, $b \neq 0 \Rightarrow a - b$, $ab^{-1} \in S$.

We may also notice here that a subfield always contains at least two elements, namely 0 and 1 of the field. (Recall a subgroup contains identity of the group and a subfield is a subgroup of the field under both the compositions).

Sum of Two Subrings

Definition: Let S and T be two subrings of a ring R. We define

$$S + T = \{s + t \mid s \in S, t \in T\}$$

then clearly $S + T$ is a non void subset of R. Indeed $0 = 0 + 0 \in S + T$.

But our enthusiasm of defining the sum ends here when we find that *sum of two subrings may not be a subring*.

Take for instance the ring M of 2×2 matrices over integers.

Let S = set of all matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ a, b integers, and

T = set of all matrices of the type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$, x an integer.

Then S and T are subrings of M, (an easy exercise for the reader).

$S + T$ would have members of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$

i.e., matrices of the type $\begin{bmatrix} a & c \\ b & 0 \end{bmatrix}$

That $S + T$ does not form a subring follows from the fact that closure w.r.t. multiplication does not hold, as

NOTES

$$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}2 & 2\\ 2 & 0\end{bmatrix} = \begin{bmatrix}4 & 2\\ 2 & 2\end{bmatrix} \notin S + T.$$

NOTES

Characteristic of a Ring

Definition: Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then R is said to have *finite characteristic* and also the smallest such positive integer is called the characteristic of R.

Thus it is the smallest positive integer n such that $1 + 1 + ...+ 1 = 0$ in R.
n times

If no such positive integer exists then R is said to have *characteristic zero* (or infinity).

Characteristic of R is denoted by char R or ch R.

Example 15: (*a*) Rings of integers, even integers, rationals, reals, complex numbers are all of ch zero.

(*b*) Consider $R = \{0, 1\}$ mod 2

then ch $R = 2$ as

$$2 \,.\, 1 = 1 \oplus 1 = 0$$

$$2 \,.\, 0 = 0 \oplus 0 = 0$$

thus 2 is the least +ve integer s.t., $2a = 0$ for all $a \in R$.

Note $1 \,.\, 1 = 1 \neq 0$

Product of Rings

Let R_1 and R_2 be two rings.

Let $R = R_1 \times R_2 = \{(a, b) \mid a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \,.\, (a_2, b_2) = (a_1a_2, b_1b_2)$$

i.e., under the usual compositions of component wise addition and multiplication. This ring is called the *direct product* of R_1 and R_2. One can similarly extend the definition to product of more than two rings. R_1 and R_2 are called the *component rings* of the direct product.

Check Your Progress

1. Give two examples of commutative rings.
2. What is an integral domain?
3. What is a division ring?
4. What is a field?

8.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

NOTES

1. Set of real numbers and rational numbers w.r.t. usual addition and multiplication.
2. A commutative ring R is called an integral domain if R has no zero divisors.
3. A ring R with unity is called a division ring or a skew field if non-zero elements of R form a group w.r.t. multiplication.
4. A commutative division ring is called a field.

8.5 SUMMARY

- Ring is a set having an addition that must be commutative ($a + b = b + a$ for any a, b) and associative [$a + (b + c) = (a + b) + c$ for any a, b, c], and a multiplication that must be associative [$a(bc) = (ab)c$ for any a, b, c]. There must also be a zero (which functions as an identity element for addition), negatives of all elements (so that adding a number and its negative produces the ring's zero element), and two distributive laws relating addition and multiplication [$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for any a, b, c].
- A ring R is called a commutative ring if $ab = ba$ for all $a, b \in$ R.
- If $\exists$ an element $e \in R$ s.t., $ae = ea = a$ for all $a \in R$ we say, R is a ring with unity. Unity is generally denoted by 1. (It is also called unit element or multiplicative identity).
- Let R be a ring. An element $0 \neq a \in R$ is called a zero-divisor, if an element $0 \in b \in R$ s.t., $ab = 0$ or $ba = 0$.
- A commutative ring R is called an integral domain if R has no zero divisors.
- An element a in a ring R with unity, is called invertible (or a unit) w.r.t. multiplication if some $b \in R$ such that $ab = 1 = ba$.
- A ring R with unity is called a Division ring or a skew field if non-zero elements of R form a group w.r.t. multiplication.
- A commutative division ring is called a field.
- A ring R is called a Boolean ring if $x^2 = x$ for all $x \in R$.
- A non-empty subset S of a ring R is said to be a subring of R if S forms a ring under the binary composition of R.

8.6 KEY WORDS

- **Modulo:** The modulo operation finds the remainder after division of one number by another.

NOTES

- **Commutative:** involving the condition that a group of quantities connected by operators gives the same result whatever the order of the quantities involved, e.g. a × b = b × a.
- **Integral domain:** an integral domain is a non-zero commutative ring in which the product of any two non-zero elements is non-zero.
- **Identity element:** an identity element is a special type of element of a set with respect to a binary operation on that set, which leaves other elements unchanged when combined with them.
- **Inverse:** an element *a* in a set with a binary operation, an inverse element for *a* is an element which gives the identity when composed with *a*.

8.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Write a brief note on a Ring.
2. Define commutative ring.
3. Show that $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ forms a ring under addition and multiplication modulo 7.
4. Show that in a ring R, $a.0 = 0.a$ for all $a \in R$.
5. What is a Boolean ring? Give an example.

Long Answer Questions

1. Prove that a commutative ring R is an integral domain iff for all $a, b, c \in R$ $(a \neq 0)$ $ab = ac \Rightarrow b = c$.
2. Show that a field is an integral domain.
3. Show that if $1 - ab$ is invertible in a ring with 1 then so is $1 - ba$.
4. Let R be a commutative ring with unity. Show that
   (i) a is a unit iff a^{-1} is a unit. (ii) a, b are units iff ab is a unit.
5. Show that a ring R is commutative iff
   $(a + b)^2 = a^2 + b^2 + 2ab$ for all $a, b \in R$.

8.8 FURTHER READINGS

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. Elements of Modern Algebra. Boston: Cengage Learning.

Zassenhaus, Hans J. 2013. *The Theory of Groups*. Chelmsford: Courier Corporation.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

NOTES

BLOCK - III

RING HOMOMORPHISM, IDEALS AND FIELDS

UNIT 9 IDEALS, QUOTIENT RINGS, RING HOMOMORPHISM

Structure

9.0 INTRODUCTION

This unit discusses about ideals, quotient rings and ring homomorphism. In ring theory, an ideal is a special subset of a ring. Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. An ideal can be used to construct a quotient ring similarly to the way that, in group theory, a normal subgroup can be used to construct a quotient group. In ring theory or abstract algebra, a ring homomorphism is a function between two rings which respects the structure. The composition of two ring homomorphism is a ring homomorphism. It follows that the class of all rings forms a category with ring homomorphism as the morphisms. In particular, one obtains the notions of ring endomorphism, ring isomorphism, and ring automorphism.

9.1 OBJECTIVES

After going through this unit, you will be able to:

- Know about Ideals
- Discuss quotient rings
- Understand the concept of ring homomorphism

NOTES

9.2 IDEALS

The notion of an ideal in a ring is parallel to the concept of normal subgroup in groups. The normal subgroups led us to the formation of quotient groups, ideals do the job when we define quotient rings. Many analogous results follow. We start with

Definition: A non empty subset I of a ring R is called a *right ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in r \Rightarrow ar \in I.$

I is called a *left ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in R \Rightarrow ra \in I.$

I is called a two sided or both sided ideal of R, if it is both left and a right ideal. In fact, if we say I is an ideal of R, it would mean, I is two sided ideal of R.

Example 1: In a ring R, $\{0\}$ and R are always both sided ideals.

Any ideal except these two is called a proper ideal (In fact, the name non trivial ideal will be more appropriate).

Example 2: Let $< \mathbf{Z}, +, \cdot >$ be the ring of integers. Then

$\mathbf{E}$ = set of even integers is an ideal of $\mathbf{Z}$

$$a, b \in \mathbf{E} \Rightarrow a = 2n, b = 2m$$

Thus $$a - b = 2(n - m) \in \mathbf{E}$$

Again, if $2n \in \mathbf{E}, r \in \mathbf{Z}$ then as

$(2n)r$ or $r(2n)$ are both in $\mathbf{E}$, $\mathbf{E}$ is an ideal.

Example 3: Let R = ring of 2×2 matrices over integers.

Let $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \text{ integers} \right\}$

then A is a right ideal of R as

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in A$$

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} ax+bz & ay+ba \\ 0 & 0 \end{bmatrix} \in A$$

But A is not a left ideal of R as

$$\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \in I, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$$

NOTES

But $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \notin A$.

Problem 1: *Let R be a ring such that every subring of R is an ideal of R. Further, ab = 0 in R ⇒ a = 0 or b = 0. Show that R is commutative.*

Solution: Let $0 \neq a \in R$ be any element.

Then $N(a) = \{x \in R \mid xa = ax\}$ is a subring of R and, therefore, an ideal of R. Let $r \in R$ be any element. Since $a \in N(a)$, $r \in R$ we find $ra \in N(a)$ (Def. of ideal)

Also then, $a(ra) = (ra)a$

and so $(ar - ra)a = 0$

$\Rightarrow$ $ar - ra = 0$ as $a \neq 0$

Thus $ar = ra \ \forall \ r \in R, \ \forall \ 0 \neq a \in R$

and as $0.r = r.0 = 0$ we find

$ar = ra \ \forall \ a, r \in R$

Hence R is commutative.

Sum of Two Ideals

Let A and B be two ideals of a ring R. We define $A + B$ to be the set $\{a + b \mid a \in A, b \in B\}$, called sum of the ideals A and B.

Theorem 1: *If A and B are two ideals of R then A + B is an ideal of R, containing both A and B.*

Proof: $A + B \neq \varphi$ as $0 = 0 + 0 \in A + B$

Again, $x, y \in A + B$

$\Rightarrow x = a_1 + b_1$

$y = a_2 + b_2$ for some $a_1, a_2 \in A$; $b_1, b_2 \in B$

Since $x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

we find $x - y \in A + B$

Let $x = a + b \in A + B$, $r \in R$ be any elements then

$xr = (a + b)r = ar + br \in A + B$ as A, B are ideals

$rs = r(a + b) = ra + rb \in A + B$

Thus $A + B$ is an ideal of R.

Again for any $a \in A$, since $a = a + 0 \in A + B$

and for any $b \in B$, since $b = 0 + b \in A + B$

we find $A \subseteq A + B$

$B \subseteq A + B$.

NOTES

Definition: Let S be any subset of a ring R. An ideal A of R is said to be generated by S if

(*i*) $S \subseteq A$

(*ii*) for any ideal I of R, $S \subseteq I \Rightarrow A \subseteq I$.

We denote it by writing $A = < S >$ or $A = (S)$.

In fact $< S >$ will be intersection of all ideals of R that contain S, and is the smallest ideal containing S. If S is finite, we say $A = < S >$ is finitely generated.

If $S = \varphi$ then as $\{0\}$ is an ideal of R containing $S = \varphi$, $< S > \subseteq \{0\}$ and so $< S > = \{0\}$.

If $S = \{a\}$ then we denote $< S >$ by $< a >$ or (a) and this case is of special interest to us as it is used rather extensively. By definition, $a \in < a >$ and as it is an ideal, elements of the type ra, as, $r_1 as_1$, na are in $< a >$, where r, r_1, s, $s_1 \in R$ and n is an integer. Such an ideal is called a *principal ideal* generated by a. One can verify that

(*i*) If R is a commutative ring, then

$$< S > = \{\Sigma n_i x_i + \Sigma r_j y_j \mid n_i \in \mathbf{Z},\ r_j \in R,\ x_i, y_j \in S\}$$

(*ii*) If R is commutative with unity then

$$< S > = \{\Sigma r_j y_j \mid r_j \in R,\ y_j \in S\}$$

(*iii*) If $S = \{a\}$, then

$$< a > = < S > = \{na + ra + as + xay \mid n \in \mathbf{Z},\ r, s, x, y \in R\}$$

(*iv*) Further if R has unity

$$< a > = \{\Sigma\ xay \mid x, y \in R\}$$

Summation being finite everywhere.

Theorem 2: *If A and B be two ideals of a ring R, then*

$$A + B = < A \cup B >.$$

Proof: We have already proved that $A + B$ is an ideal of R, containing A and B, thus $A + B$ is an ideal containing $A \cup B$.

Let I be any ideal of R, s.t., $A \cup B \subseteq I$

Let $x \in A + B$ be any element

Then $x = a + b$ for some $a \in A$, $b \in B$

Since

$a \in A \subseteq A \cup B \subseteq I$

$$b \in B \subseteq A \cup B \subseteq I$$

we find $a + b \in I$ as I is an ideal

$\Rightarrow$ $x \in I$ or that $A + B \subseteq I$

which proves the theorem.

NOTES

Thus $A + B$ is the smallest ideal of R, containing A and B. One can, of course, talk about sum of more than two ideals in the same manner.

Problem 2: *If $a \in R$ be an element and $I = aR = \{ar \mid r \in R\}$ where R is a commutative ring, then I is an ideal of R.*

Solution: $I \neq \varphi$ as $0 = a \,.\, 0 \in I$

$$x, y \in I \Rightarrow x = ar_1,\ y = ar_2 \text{ for some } r_1, r_2 \in R$$

$$\Rightarrow x - y = a(r_1 - r_2) \in I$$

again if $x = ar_1 \in I$ and $r \in R$ be any elements

then $xr = (ar_1)r = a(r_1 r) \in I$ shows that I is a right ideal. R being commutative, it will be both sided ideal.

Remark: If the ring is not commutative, one can show that aR is a right ideal and $Ra = \{ra \mid r \in R\}$ is a left ideal of R.

aR is always contained in $< a >$. If R is a commutative ring with unity then $aR = Ra = (a)$.

Let us understand the difference between aR and $< a >$ through the following example.

Example 4: Let $< \mathbf{E}, +, \cdot >$ be the ring of even integers. It is commutative ring without unity, Let $a = 4 \in \mathbf{E}$.

Then $< 4 > = \{4n + (2m)\ 4 \mid n, m \in \mathbf{Z}\}$

$$= \{4n + 8m \mid n, m \in \mathbf{Z}\}$$

whereas $4\mathbf{E} = \{4(2k) \mid k \in \mathbf{Z}\} = \{8k \mid k \in \mathbf{Z}\}$

We notice then, $< 4 > \neq 4\mathbf{E}$ as $4 \in < 4 >$ but $4 \notin 4\mathbf{E}$.

Problem 3: *If A is an ideal of a ring R with unity such that $1 \in A$ then show that $A = R$.*

Solution: Since $A \subseteq R$ always, all we need show is that $R \subseteq A$.

Let $r \in R$ be any element.

Since $1 \in A$ and A is an ideal

$$r = 1 \,.\, r \in A$$

$$\Rightarrow R \subseteq A \text{ or that } A = R.$$

Product of Two Ideals

Let A, B be two ideals of a ring R. We define the product AB of A and B by

$AB = \{\Sigma\ a_i b_i \mid a_i \in A, b_i \in B\}$

where summation is finite.

Theorem 3: *The product AB of any two ideals A and B of a ring R is an ideal of R.*

Proof: $AB \neq \varphi$ as $0 = 0 \,.\, 0 \in AB$

NOTES

Let $x, y \in AB$ be any two members

then $x = a_1b_1 + a_2b_2 + ... + a_nb_n$

$y = a'_1b'_1 + ... + a'_mb'_m$

for some $a_i, a'_j \in A$, $b_i, b'_j \in B$

$x - y = (a_1b_1 + ... + a_nb_n) - (a'_1b'_1 + ... + a'_mb'_m)$

which clearly belongs to AB, as the R.H.S. can be written as

$x_1y_1 + x_2y_2 + ... + x_ky_k \quad (k = n + m)$

where $x_i \in A, y_i \in B$.

Again, for any $x = a_1b_1 + ... + a_nb_n \in AB$ and $r \in R$,

$rx = r(a_1b_1 + ... + a_nb_n)$

$= (ra_1)b_1 + (ra_2)b_2 + ... + (ra_n)b_n \in AB$

because $ra_i \in A$ as $a_i \in A$, $r \in R$, and A is an ideal.

Similarly $xr \in AB$

showing thereby that AB is an ideal of R.

Remarks: (*i*) Let $S = \{ab \mid a \in A.\ b \in B\}$

then $< S > = AB$.

Clearly $S \subseteq AB$ and as AB is an ideal, $< S > \subseteq AB$.

Again, $x \in AB \Rightarrow x = \Sigma a_ib_i$, $a_i \in A$, $b_i \in B$

$a_i \in A$, $b_i \in B$

$\Rightarrow a_ib_i \in S, \ \forall\, i = 1, 2, ...,$

$\Rightarrow a_ib_i \in < S > \ \forall\, i$

$\Rightarrow x \in < S >$

$\Rightarrow AB \subseteq < S >$

and hence $< S > = AB$.

(*ii*) If R is a commutative ring with unity and A, B are finitely generated ideals of R then so are $A + B$ and AB. In fact if $A = < a_1, a_2, ..., a_n >$ and $B = < b_1, b_2, ..., b_s >$ then

$A + B = < a_1, a_2, ..., a_r, b_1, b_2, ..., b_s >$

$AB = < a_1b_1, ..., a_1b_s, ..., a_rb_1, ..., a_rb_s >$

This, however, may not be true for $A \cap B$.

The following problem gives us little more information about product of ideals.

Problem 4: *If A , B, C are ideals of a ring R, s.t., $B \subseteq A$ then show that*

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

Solution: Let $x \in A \cap (B + C)$ be any element

Then $x \in A$ and $x \in B + C$

NOTES

$\Rightarrow x = b + c$ for some $b \in B, c \in C$

Now $b \in B \subseteq A$, also $b + c = x \in A$

$\Rightarrow (b + c) - b \in A$

$\Rightarrow c + b - b \in A$

$\Rightarrow c \in A$

$\Rightarrow x \in A \cap C$

i.e., $x = b + c, b \in B, c \in A \cap C$

thus $x \in B + (A \cap C)$

Hence $A \cap (B + C) \subseteq B + (A \cap C)$.

Again let $x \in B + (A \cap C)$

Then $x = b + k$ for some $b \in B, k \in A \cap C$

Since $b \in B, k \in C$

$x = b + k \in B + C$

and $b \in B \subseteq A, k \in A \Rightarrow b + k \in A$

$\Rightarrow x \in A$

$\Rightarrow x \in A \cap (B + C)$

or that $B + (A \cap C) \subseteq A \cap (B + C)$

which finally gives $A \cap (B + C) = B + (A \cap C)$

Also as $B \subseteq A, A \cap B = B$

thus $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

Remark: The above is sometimes called modular equality.

Definition: A ring $R \neq \{0\}$ is called a *simple ring* if R has no ideals except R and $\{0\}$.

Theorem 4: *A division ring is a simple ring*.

Proof: Let R be a division ring. Let A be any ideal of R s.t., $A \neq \{0\}$ then $\exists$ at least one $a \in A$ s.t., $a \neq 0$. R being a division ring, $a^{-1} \in R$ and $aa^{-1} = 1$.

Since $a \in A, a^{-1} \in R, aa^{-1} \in A$ (def. of ideal)

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

i.e., only ideals that R can have are R and $\{0\}$ or that R is a simple ring.

Problem 5: *Let R be a ring with unity, such that R has no right ideals except* $\{0\}$ *and R. Show that R is a division ring.*

Solution: All that we need prove is that non zero elements of R form a group under multiplication.

Let $0 \neq a \in R$ be any non zero element.

NOTES

Let $aR = \{ar \mid r \in R\}$

Then aR is a right ideal. See problem 2.

By given condition, then

$$aR = R$$

or $aR = \{0\}$

But $aR \neq \{0\}$ as $a \neq 0$ and $a = a.1 \in aR$

Hence $aR = R$.

Now $1 \in R \Rightarrow 1 \in aR \Rightarrow \exists\, b \in R$, s.t. $1 = ab \Rightarrow b$ is right inverse of a (w.r.t. multiplication). Thus $<R - \{0\}, \cdot>$ is a system in which associativity holds, right identity (unity) and right inverse exist (for every element).

i.e., $< R - \{0\}, \cdot >$ forms a group or that R is a division ring.

9.3 QUOTIENT RINGS

Let R be a ring and let I be an ideal of R. Since $a, b \in I \Rightarrow a - b \in I$, we find I is a subgroup of $< R, + >$. Again as $< R, + >$ is abelian, I will be a normal subgroup of R and thus we can talk of $\frac{R}{I}$, the quotient group

$\frac{R}{I} = \{r + I \mid r \in R\}$ = set of all cosets of I in R (clearly left or right cosets are equal).

We know R/I forms a group under 'addition' defined by

$$(r + I) + (s + I) = (r + s) + I$$

We now define a binary composition (product) on R/I by

$$(r + I) \cdot (s + I) = rs + I$$

We show this product is well defined

Let $r + I = r' + I$ and $s + I = s' + I$

$\Rightarrow r - r' \in I$ and $s - s' \in I$

$\Rightarrow r - r' = a$ and $s - s' = b$ for some $a, b \in I$

$\Rightarrow r = r' + a,\ s = s' + b$

$\Rightarrow rs = (a + r')(b + s')$

$\Rightarrow rs + I = (ab + as' + r'b + r's') + I = r's' + I$

(using $x + I = I$ iff $x \in I$)

Hence the multiplication is well defined.

Since $(a + I)[(b + I)(c + I)]$

$= (a + I)(bc + I)$

NOTES

$$= a(bc) + I$$
$$= (ab)c + I$$
$$= (ab + I)(c + I)$$
$$= [(a + I)(b + I)](c + I)$$

Associativity holds w.r.t. this product.

Again, as $(a + I)[(b + I) + (c + I)] = (a + I)(b + c + I)$

$$= a\ (b + c) + I$$
$$= (ab + ac) + I$$
$$= (ab + I) + (ac + I)$$
$$= (a + I)(b + I) + (a + I)(c + I)$$

We find left distributivity holds. Similarly one can check that right distributivity also holds in R/I and hence R/I forms a ring, called the *quotient ring* or *factor ring* or *residue class ring* of R by I.

We look at it from another angle. Let R be a ring and I an ideal of R. Define, for $a, b \in R$, $a \equiv b \pmod{I}$ if $a - b \in I$. It is easy to check that this relation is an equivalence relation on R. Thus it partitions R into equivalence classes. Let for any $a \in R$, $cl(a)$ be the corresponding equivalence class of a.

Then
$$cl(a) = \{r + R \mid r \equiv a \pmod{I}\}$$
$$= \{r \in R \mid r - a \in I)\}$$
$$= \{r \in R \mid r - a = x \text{ for some } x \in I\}$$
$$= \{r \in R \mid r = a + x \text{ for some } x \in I\}$$
$$= \{a + x \mid x \in I\}$$
$$= a + I$$

Thus, the quotient ring $\frac{R}{I}$ is nothing but the ring of all equivalence classes as defined above.

In fact, the binary compositions defined earlier would translate to

$$cl(a) + cl(b) = cl(a + b) \qquad a, b \in R$$
$$cl(a)\ .\ cl(b) = cl(ab)$$

It would be an interesting exercise for the reader to verify that R/I thus defined forms a ring. In fact, if R has unity 1 then $cl(1)$ will be unity of R/I.

R/I is therefore also called *quotient ring* of R modulo I.

Remarks: (i) It may be noticed that R/I is defined only when I is an ideal of R. If I happens to be only a subring of R then R/I may not form a ring as there the multiplication rule may not be valid. Suppose I is only a subring of R (and is not an ideal) then let $r \in R$, $a \in I$ s.t., $ar \notin I$.

NOTES

Then $(a + I)(r + I) = ar + I$

gives $(0 + I)(r + I) = ar + I$

i.e., $0.r + I = ar + I$ or that $ar \in I$ which is not true.

(*ii*) If $I = R$ then R/I is isomorphic to the zero ring $\{0\}$ and if $I = \{0\}$ then $\frac{R}{I} \cong R$.

Example 5: Let $H_4 = \{4n \mid n \in \mathbf{Z}\}$, where $< \mathbf{Z}, +, \cdot >$ is the ring of integers. Then H_4 is an ideal of $\mathbf{Z}$ and thus $\frac{\mathbf{Z}}{H_4}$ is a quotient ring and is given by

$$\frac{\mathbf{Z}}{H_4} = \{H_4, H_4 + 1, H_4 + 2, H_4 + 3\}$$

This example also shows us that quotient ring of an integral domain may not be an integral domain.

Notice $(H_4 + 2)(H_4 + 2) = H_4 + 4 = H_4 =$ zero of $\frac{\mathbf{Z}}{H_4}$ but $H_4 + 2 \neq H_4$.

On the other hand if we cosider

$$R = \{0, 2, 4, 6, 8, 10\} \bmod 12$$

$$S = \{0, 6\} \bmod 12$$

then R is not an integral domain whereas R/S is an integral domain.

We have $R/S = \{S, S + 2, S + 4\}$

Since $(S + 2)(S + 2) = S + 2$, $(S + 2)(S + 4) = S + 8 = S + 2$

and $(S + 4)(S + 4) = (S + 16) = S + 4$, we find

$\frac{R}{S}$ has no zero divisors.

9.4 RING HOMOMORPHISMS

Let $< R, +, . >$, $< R', *, o >$ be two rings. A mapping $\theta : R \to R'$ is called a *homomorphism* if

$$\theta(a + b) = \theta(a) * \theta(b)$$

$$\theta(ab) = \theta(a)\ o\ \theta(b) \qquad a, b \in R$$

Since we prefer to use the symbols + and . for the binary compositions in a ring, we will use these symbols, even while dealing with more than one ring. In that case, the above definition *simplifies* to saying that a mapping $\theta : R \to R'$ is called a homomorphism if

$$\theta(a + b) = \theta(a) + \theta(b)$$
$$\theta(ab) = \theta(a) \cdot \theta(b)$$

One can similarly talk about *isomorphism* in rings as a one-one onto homomorphism.

NOTES

Example 6: Consider the map $f: \mathbf{C} \to \mathbf{C}$, s.t.,

$$f(a + ib) = a - ib$$

then f is a homomorphism, where $\mathbf{C}$ = complex numbers,

as $f[(a + ib) + (c + id)] = f((a + c) + i(b + d))$
$= (a + c) - i(b + d)$
$= (a - ib) + (c - id)$
$= f(a + ib) + f(c + id)$

and $f[(a + ib)(c + id)] = f((ac - bd) + i(ad + bc))$
$= (ac - bd) - i(ad + bc)$
$= (a - ib)c - id(a - ib)$
$= (a - ib)(c - id)$
$= f(a + ib) f(c + id)$

Example 7: Let R be a commutative ring and suppose $px = 0$ for all $x \in R$, where p is a prime number. Then the mapping $f: R \to R$ defined by $f(x) = x^p$, $x \in R$ is a homomorphism.

In fact the result follows rather easily, if we can show that $p \mid p_{Cr}$, $1 \le r \le p-1$.

Now $n = p_{Cr} = \dfrac{p!}{(p-r)!r!}$

$$= \frac{p(p-1).....(p-r+1)(p-r)!}{(p-r)!1.2....r}$$

$\Rightarrow$ $nr! = p(p-1)\ .....(p - r + 1)$

Since p divides R.H.S., it will divide $nr!$

$\Rightarrow p \mid n$ or $p \mid r!$ (whenever a prime divides product ab, it must divide at least one of a or b). But $p \nmid r!$ as $1, 2, ..., r-1$ are all less than p, so p cannot divide any one of them. Thus $p \nmid r!$

i.e., $p \mid n$

Now for any $x, y \in R$

$$f(x + y) = (x + y)^p = x^p + p_{C1}\, x^{p-1}\, y + p_{C2}\, x^{p-2}\, y^2 + ... + y^p$$

(R being commutative)

Now $p_{C1}\, x^{p-1}\, y = px^{p-1}\, y = 0$ as $x^{p-1}\, y \in R$

$p_{C2}\, x^{p-2}\, y^2 = (kp)\, x^{p-2}\, y^2 = 0$ as $p \mid p_{C2} \Rightarrow p_{C2} = kp$ for some k

NOTES

Similarly each p_{Cr} would be some multiple of p giving that other terms are also zero.

Hence $f(x + y) = x^p + y^p = f(x) + f(y)$

Also $f(xy) = (xy)^p = x^p y^p$ (R commutative)

$= f(x) f(y)$

Thus f is a homomorphism.

Theorem 5: *If* $\theta : R \to R'$ *be a homomorphism, then*

(*i*) $\theta(0) = 0'$

(*ii*) $\theta(-a) = -\theta(a)$

where 0, 0′ *are zeros of the rings* R and R' *respectively*.

Proof: (*i*) Since $0 + 0 = 0$

we have $\theta(0 + 0) = \theta(0)$

$\Rightarrow \quad \theta(0) + \theta(0) = \theta(0) + 0'$

$\Rightarrow \quad \theta(0) = 0'$

(*ii*) Again, as $a + (-a) = 0$

$\theta(a + (-a)) = \theta(0)$

$\Rightarrow \quad \theta(a) + \theta(-a) = \theta(0) = 0$

$\Rightarrow \quad -\theta(a) = \theta(-a)$

Cor.: It is clear that

$\theta(a - b) = \theta(a + (-b))$

$= \theta(a) - \theta(b)$

Remark: The terminology of epimorphism, monomorphism etc. is extended to rings also in the same way as in groups.

Definition: Let $f : R \to R'$ be a homomorphism, we define *Kernel* of f by

$$\text{Ker } f = \{x \in R \mid f(x) = 0'\}$$

where 0′ is zero of R'.

The following two theorems are easy to prove so we'll state the results without proof.

If : $R \to R'$ is a homomorphism then

Theorem 6: *Ker f is an ideal of R*.

Theorem 7: *Ker f* = (0) *iff f is one-one*.

Problem 6: *If R is a ring with unity and* $f : R \to R'$ *is a homomorphism where* R' *is an integral domain such that Ker* $f \neq R$ *then show that* $f(1)$ *is unity of* R'.

Solution: Let $a' \in R'$ be any element. We show

$$f(1)\, a' = a' f(1) = a'$$

NOTES

Now $f(1)\,a' - f(1)\,a' = 0'$

$\Rightarrow f(1.1)\,a' - f(1)\,a' = 0'$

$\Rightarrow f(1)\,f(1)\,a' - f(1)\,a' = 0'$

$\Rightarrow f(1)\,[f(1)\,a' - a'\,] = 0'$

$\Rightarrow$ either $f(1) = 0'$ or $f(1)\,a' - a' = 0'$ as R' is an integral domain.

$f(1) = 0' \Rightarrow 1 \in \text{Ker}\, f \Rightarrow \text{Ker}\, f = R$ which is not true.

Hence $f(1)a' - a' = 0'$

$\Rightarrow \quad f(1)\,a' = a'$

Similarly, we can show $a' = a'f(1)$.

Problem 7: *Let $f: R \to R'$ be an onto homomorphism, where R is a ring with unity. Show that $f(1)$ is unity of R'.*

Solution: Let $a' \in R'$ be any element.

Since f is onto, $\exists\ a \in R$, s.t., $f(a) = a'$

Now $a'.f(1) = f(a)\ .f(1) = f(a\ .\ 1) = f(a) = a'$

Similarly $f(1)\ .\ a' = a'$.

Showing, thereby that $f(1)$ is unity of R'.

Problem 8: *Show by an example that we can have a homomorphism $f: R \to R'$, such that $f(1)$ is not unity of R', where 1 is unity of R.*

Solution: Consider the map $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 0 \quad \text{for all } x \in \mathbf{Z}$$

where $\mathbf{Z}$ = ring of integers

then f is a homomorphism (verify)

Again $f(1) = 0$, but 0 is not unity of $\mathbf{Z}$.

Thus although $\mathbf{Z}$ (on R.H.S.) has unity it does not equal $f(1)$.

Remarks: (*i*) If we take the map $f: \mathbf{Z} \to \mathbf{E}$, where $\mathbf{E}$ = ring of even integers, defined by $f(x) = 0$ for all x, we find, $\mathbf{E}$ does not have unity, whereas 1 is unity of $\mathbf{Z}$.

(*ii*) We recall that the map $f: \mathbf{Z} \to \mathbf{E}$, s.t., $f(x) = 2x$ is a group isomorphism. Thus $\mathbf{Z}$ and $\mathbf{E}$ are isomorphic as groups whereas $\mathbf{Z}$ and $\mathbf{E}$ are not isomorphic as rings. Indeed, $\mathbf{Z}$ has unity but $\mathbf{E}$ does not possess unity. In fact, f will not be a ring homomorphism.

Problem 9: *Find all the ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.*

Solution: Let $f: \mathbf{Z}_{20} \to \mathbf{Z}_{30}$ be any ring homomorphism.

Let $f(1) = a$, then $f(x) = xa$ and we find $o(a) | o(\mathbf{Z}_{30}) = 30$ and $o(a) \mid 20 = o(\mathbf{Z}_{20})$

Thus possible values of $o(a)$ are 1, 2, 5, 10 and so possible values of a will be

$$0, 3, 6, 9, 12, 15, 18, 21, 24, 27$$

which give us the ten group homomorphisms.

NOTES

Since f is a ring homomorphism and in $\mathbf{Z}_{20}$, $1.1 = 1$, we find $f(1.1) = f(1)$

or $f(1)(1) = f(1)$

or $a^2 = a$ in $\mathbf{Z}_{30}$

This is satisfied by 0, 6, 15, 21 values of a.

Hence there exist four ring homomorphisms from $\mathbf{Z}_{20} \to \mathbf{Z}_{30}$.

Problem 10: *Let* $\mathbf{Z}$ *be the ring of integers. Show that the only homomorphisms from* $\mathbf{Z} \to \mathbf{Z}$ *are the identity and zero mappings.*

Solution: Let $f: \mathbf{Z} \to \mathbf{Z}$ be a homomorphism

Since $(f(1))^2 = f(1) f(1) = f(1.1) = f(1)$

$$f(1)[f(1) - 1] = 0$$

$$\Rightarrow f(1) = 0 \text{ or } f(1) = 1$$

If $f(1) = 0$ then $f(x) = 0 \ \forall$ integers x

as $f(x) = f(1 \cdot x) = f(1) f(x) = 0 \cdot f(x) = 0 \ \forall \ x$

Thus in this case f is the zero homomorphism.

If $f(1) = 1$, then for any $x \in \mathbf{Z}$

$$f(x) = f(1 + 1 + \ldots + 1) = x f(1) = x \qquad (x > 0)$$

$$f(x) = f(-y) = -f(y) = -[f(1 + 1 + \ldots + 1)] = -y f(1) = x f(1) = x \qquad (x < 0, y = -x)$$

$$f(0) = 0$$

So in this case f is identity map, which proves the result.

Theorem 8: (Fundamental Theorem of Ring Homomorphism)

If $f: R \to R'$ *be an onto homomorphism, then* R' *is isomorphic to a quotient ring of* R. *In fact,* $R' \cong \dfrac{R}{\text{Ker } f}$.

Proof: Let $f: R \to R'$ be onto homomorphism

Define $\varphi : \dfrac{R}{\text{Ker } f} \to R'$, s.t.,

$$\varphi(x + I) = f(x) \quad \text{for all } x \in R \text{ where } I = \text{Ker } f$$

then φ is well defined as

$$x + I = y + I$$

$$\Rightarrow \ x - y \in I = \text{Ker } f$$

$\Rightarrow \quad f(x - y) = 0$

$\Rightarrow \quad f(x) - f(y) = 0$

$\Rightarrow f(x) = f(y)$

$\Rightarrow \varphi(x + I) = \varphi(y + I)$

Retracing the steps backwards we prove φ is 1–1.

Again, as

$$\varphi[(x + I) + (y + I)] = \varphi((x + y) + I) = f(x + y) = f(x) + f(y)$$
$$= \varphi(x + I) + \varphi(y + I)$$
$$\varphi[(x + I)(y + I)] = \varphi(xy + I) = f(xy) = f(x)\, f(y)$$
$$= \varphi(x + I)\ \varphi(y + I)$$

φ is a homomorphism.

Now if $r' \in R'$ be any element then as $f : R \to R'$ is onto, $\exists\ r \in R$, s.t., $f(r) = r'$ for this r, as $\varphi(r + I) = f(r) = r'$

We find $r + I$ is required pre-image of r' under φ showing thereby that φ is onto and hence an isomorphism.

Thus $\dfrac{R}{\text{Ker } f} \cong R'$. By summetry $R' \cong \dfrac{R}{\text{Ker } f}$.

Theorem 9: (First Theorem of Isomorphism)

Let $B \subseteq A$ be two ideals of a ring R. Then

$$\frac{R}{A} \cong \frac{R/B}{A/B}.$$

Proof: Define a mapping $f : \dfrac{R}{B} \to \dfrac{R}{A}$ s.t.,

$$f(r + B) = r + A$$

then f is an onto homomorphism (Prove!)

By fundamental theorem, $\dfrac{R}{A} \cong \dfrac{R/B}{\text{Ker } f}$

Again, since $r + B \in \text{Ker } f \qquad \Leftrightarrow f(r + B) = A$

$$\Leftrightarrow r + A = A$$
$$\Leftrightarrow r \in A$$
$$\Leftrightarrow r + B \in \frac{A}{B}$$

we find $\text{Ker } f = A/B$

Hence $\dfrac{R}{A} \cong \dfrac{R/B}{A/B}$.

NOTES

Theorem 10: (Second Theorem of Isomorphism)

Let A, B *be two ideals of a ring R, then*

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

Proof: Define a mapping $f: B \to \frac{A+B}{A}$ s.t.,

$$f(b) = b + A \quad \text{for all } b \in B$$

Then f is a well defined homomorphism.

Again if $x + A \in \frac{A+B}{A}$ be any element then

$$x \in A + B \Rightarrow x = a + b, \ a \in A, \ b \in B$$

So, $x + A = (a + b) + A = (b + a) + A = b + (a + A) = b + A$

thus $x + A = b + A = f(b)$

i.e., b is the pre-image of $x + A$ under f or that f is onto.

By fundamental theorem then $\frac{A+B}{A} \cong \frac{B}{\text{Ker } f}$

Now $x \in \text{Ker } f \Leftrightarrow f(x) = A$

$$\Leftrightarrow x + A = A \Leftrightarrow x \in A$$

$$\Leftrightarrow x \in A \cap B \qquad (x \in \text{Ker } f \subseteq B)$$

Hence $\text{Ker } f = A \cap B$

and thus $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

Remark: Clearly then $\frac{A+B}{B} \cong \frac{A}{A \cap B}$.

Problem 11: Show that $\frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$.

Solution: Take $A = <2>$, $B = <5> = 5\mathbf{Z}$, the ideals of $\mathbf{Z}$.

Then $A + B = <d>$, where d = g.c.d. (2, 5) = 1

$A \cap B = <l>$ where l = l.c.m. (2, 5) = 10

So $A + B = <1> = \mathbf{Z}$

$A \cap B = <10> = 10\mathbf{Z}$

Hence using the above result that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B} \text{ we get } \frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$$

NOTES

Problem 12: *Show that* $\mathbf{Z}_m$ *can be regarded as a subring of* $\mathbf{Z}_n$ *iff* $m \mid n$.

Solution: If $\mathbf{Z}_m$ is a subring of $\mathbf{Z}_n$ then it is a subgroup of $\mathbf{Z}_n$ under addition and so $m \mid n$.

Conversely, let $m \mid n$, and suppose $n = um$.

Define a mapping $\theta: \mathbf{Z}_m \to \mathbf{Z}_n$ s.t.,

$$\theta(a) = a$$

Consider $\theta(a \oplus_m b) = \theta(c)$ = Remainder obtained by dividing $a + b$ by m and $\theta(a) \oplus_n \theta(b)$ = remainder obtained by dividing $a + b$ by $n = um$ = remainder obtained by dividing $a + b$ by m.

Similarly $\theta(a \otimes_m b) = \theta(a) \otimes_n \theta(b)$

So, θ is a ring homomorphism $\Rightarrow \mathbf{Z}_m \cong \theta(\mathbf{Z}_m)$ is a subring of $\mathbf{Z}_n$ implying $\mathbf{Z}_m$ can be regarded as a subring of $\mathbf{Z}$.

Problem 13: *Show that* $x^2 + 1 = 0$ *has infinite number of solutions over D, the ring of quaternions.*

Solution: Let $u = a + bi + cj + dk$ be a solution of $x^2 + 1 = 0$ Then $u^2 = -1$.

Let $\theta: D \to M$ be the isomorphism

where $$\mathrm{M} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in c \right\}$$

$$\text{s.t. } \theta(a + bi + cj + dk) = \begin{bmatrix} a + bi & c + di \\ -cc - di & a - bi \end{bmatrix}$$

Then $\theta(u)^2 = -\theta(1) = -I$, where I denotes the 2×2 identity matrix.

Let $$\theta(u) = A = \begin{bmatrix} a + bi & c + di \\ -(c - di) & a - bi \end{bmatrix}.$$

Then $A^2 = -I$ and Trace $A = 2a$

Now $$A^2 = \begin{bmatrix} a + bi & c + di \\ -(c - di) & a - bi \end{bmatrix} \begin{bmatrix} a + bi & c + di \\ -(c - di) & a - bi \end{bmatrix}$$

$$= \begin{bmatrix} a^2 - b^2 + 2a\,bi - c^2 - d^2 & - \\ - & -c^2 - d^2 + a^2 - b^2 - 2abi \end{bmatrix}$$

$$= -I$$

implies Trace $A^2 = 2(a^2 - b^2 - c^2 - d^2) = \text{Trace } (-I) = -2$

implies $b^2 + c^2 + d^2 = a^2 + 1$

Now $\det A = a^2 + b^2 + c^2 + d^2$

So $\det A^2 = (\det A)^2 = (a^2 + b^2 + c^2 + d^2)^2 = +1$

NOTES

Therefore, $a^2 + b^2 + c^2 + d^2 = 1$. But $b^2 + c^2 + d^2 = a^2 + 1$

So, $a^2 + a^2 + 1 = 1 \Rightarrow 2a^2 = 0 \Rightarrow a = 0$

This gives $b^2 + c^2 + d^2 = 1$ and $u = 0 + bi + cj + dk$

Also $(0 + bi + cj + dk)^2 = -(b^2 + c^2 + d^2) + 0i + 0j + 0k = -1$

Therefore, the solutions of $x^2 + 1 = 0$ are given by $u = 0 + bi + cj + dk$, where $b^2 + c^2 + d^2 = 1$

There are infinite real numbers b, c, d such that $b^2 + c^2 + d^2 = 1$. For example, let p be a prime, then take $b = \frac{\sqrt{p-1}}{\sqrt{p}}$, $c = \frac{1}{\sqrt{p}}$, $d = 0$.

So, $b^2 + c^2 + d^2 = \frac{p-1}{p} + \frac{1}{p} = 1$. But the number of primes are infinite.

Hence, $x^2 + 1 = 0$ has infinite number of solutions over D.

Check Your Progress

1. What is the fundamental theorem of ring homomorphism?
2. What is right ideal of a ring R?
3. What is a simple ring?

9.5 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. If $f : R \to R'$ be an onto homomorphism, then R' is isomorphic to a quotient ring of R. In fact,

   $R' \cong \frac{R}{Ker\, f}$

2. A non-empty subset I of a ring R is called a right ideal of R if

   (i) $a, b \in I \Rightarrow a - b \in I$ (ii) $a \in I, r \in R \Rightarrow ar \in I$.

3. A ring $R = \{0\}$ is called a simple ring if R has no ideals except R and $\{0\}$.

9.6 SUMMARY

- A non-empty subset I of a ring R is called a right ideal of R if

  (i) $a, b \in I \Rightarrow a - b \in I$ (ii) $a \in I, r \in R \Rightarrow ar \in I$.

- A non-empty subset I of a ring R is called a left ideal of R if

  (i) $a, b \in I \Rightarrow a - b \in I$ (ii) $a \in I, r \in R \Rightarrow ra \in I$.

- The quotient ring R/I is the set of all cosets of I i.e. all sets $a + I$ for all $a \in R$. The addition and multiplication operations are those defined for cosets. The zero element of R/I is I.
- Let $< R, +, . >$, $< R', *, o >$ be two rings. A mapping $\theta: R \to R'$ is called a homomorphism if $\theta(a + b) = \theta(a) * \theta(b)$

  $\theta(ab) = \theta(a)\ o\ \theta(b) \quad a, b \in R$
- Let $f : R \to R'$ be a homomorphism, we define Kernel of f by Ker $f = \{x \in R \mid f(x) = 0'\}$ where 0' is zero of R'.
- Ker f is an ideal of R.
- Ker $f = (0)$ iff f is one-one.
- If $f: R \to R'$ be an onto homomorphism, then R' is isomorphic to a quotient ring of R. In fact $R' \cong \frac{R}{Ker\ f}$,

9.7 KEY WORDS

- **Homomorphism:** a transformation of one set into another that preserves in the second set the relations between elements of the first.
- **One-to-one:** The function is o**ne-to-one** if each element of the codomain is mapped to by *at most* one element of the domain.
- **Onto:** The function is (onto) if each element of the codomain is mapped to by at least one element of the domain. (That is, the image and the codomain of the function are equal.)
- **Isomorphism:** an isomorphism is a homomorphism or morphism that can be reversed by an inverse morphism.

9.8 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Define ring homomorphism.
2. Show that intersection of two ideals is an ideal.
3. If A is an ideal of a ring R, let $[R : A] = \{x \in R \mid rx \in A \text{ for all } r \in R\}$

   Show that $[R : A]$ is an ideal of R, containing A.
4. Let R and S be two commutative rings with unity and let f: R $\to$ S be an onto homomorphism. If $ch\ R \neq 0$, show that $ch\ S$ divides $ch\ R$.

NOTES

Long Answer Questions

1. Show that homomorphic image of a commutative ring is commutative. Prove also that the converse may not hold.
2. Find all six ring homomorphism from $Z_{12} \rightarrow Z_{30}$.
3. Show that homomorphic image of a ring with unity is a ring with unity but the converse is not true.
4. Show that there exists an onto homomorphism from R to R/I, a quotient ring of R.

9.9 FURTHER READINGS

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. Elements of Modern Algebra. Boston: Cengage Learning.

Gorodentsev, Alexey L. 2016. *Algebra I: Textbook for Students of Mathematics*. Berlin: Springer.

Herstein , I.N. 2006. *TOPICS IN ALGEBRA, 2ND ED*. New Jersey: John Wiley & Sons.

UNIT 10 MORE IDEALS RINGS

NOTES

Structure

10.0 INTRODUCTION

You have already learned ideals and quotient rings in the previous unit. In this unit, you will learn more definitions and theorems on ideals and the quotients rings.

10.1 OBJECTIVES

After going through this unit, you will be able to:

- Know more about ideal rings
- Solve problems on quotient rings

10.2 MORE IDEALS RINGS

Definition: Two ideals A and B are called comaximal if $A + B = R$.

Theorem 1: *If R is a commutative ring with unity and A, B are comaximal ideals of R, then* $AB = A \cap B$.

Proof: One can prove that, in general,

$AB \subseteq A \cap B$

Let now $x \in A \cap B$ be any element.

Then $x \in A$ and $x \in B$

Since $1 \in R = A + B$

$\exists\ a \in A, b \in B$ s.t., $1 = a + b$

$\Rightarrow x \,.\, 1 = x \,.\, (a + b)$

$\Rightarrow x = xa + xb$

$\Rightarrow x = ax + xb$

NOTES

Now $a \in A,\ x \in B;\ x \in A,\ b \in B \Rightarrow ax + xb \in AB$

i.e., $x \in AB$

or that $A \cap B \subseteq AB$

and thus $AB = A \cap B$.

Theorem 2: *Let R be a commutative ring with unity and let I_1 and I_2 be two ideals of R. Then*

(*i*) $\varphi : R \to \frac{R}{I_1} \times \frac{R}{I_2}$, s.t., $\varphi(x) = (x + I_1, x + I_2)$ *is a homomorphism s.t., Ker* $\varphi = I_1 \cap I_2$.

(*ii*) I_1 *and* I_2 *are comaximal ideals of R iff* φ *is onto*

Proof: (*i*) We leave it for the reader to verify that φ is a homomorphism.

Since $x \in \text{Ker } \varphi \Leftrightarrow \varphi(x) = (I_1, I_2)$

$\Leftrightarrow (x + I_1, x + I_2) = (I_1, I_2)$

$\Leftrightarrow x + I_1 = I_1, x + I_2 = I_2$

$\Leftrightarrow x \in I_1, x \in I_2$

$\Leftrightarrow x \in I_1 \cap I_2$

we find $\text{Ker } \varphi = I_1 \cap I_2$.

(*ii*) Suppose φ is onto. Then given $(1 + I_1, 0 + I_2) \in \frac{R}{I_1} \times \frac{R}{I_2}$, $\exists\, x \in R$, s.t.,

$\varphi(x) = (1 + I_1, I_2)$

$\Rightarrow (x + I_1, x + I_2) = (1 + I_1, I_2)$

$\Rightarrow x + I_1 = 1 + I_1, \quad x + I_2 = I_2$

$\Rightarrow 1 - x \in I_1, \quad x \in I_2,$

$\Rightarrow (1 - x) + x \in I_1 + I_2 \Rightarrow 1 \in I_1 + I_2 \Rightarrow I_1 + I_2 = R$

or that I_1 and I_2 are comaximal.

Conversely, let $I_1 + I_2 = R$ (i.e., I_1, I_2 be comaximal)

Since $1 \in R$, $1 \in I_1 + I_2$ we get $1 = x + y,\ x \in I_1,\ y \in I_2$

Now $(1 + I_1, I_2) = (x + y + I_1, I_2)$

$= (y + I_1, I_2)$

$= (y + I_1, y + I_2) = \varphi(y)$

Similarly, $(I_1, x + I_2) = \varphi(x)$

Now for any $(a_1 + I_1, a_2 + I_2) \in \frac{R}{I_1} \times \frac{R}{I_2}$, since

$$(a_1 + I_1,\ a_2 + I_2) = (1 + I_1, I_2)\,(a_1 + I_1, a_1 + I_1) + (I_1, 1 + I_2)\,(a_2 + I_1, a_2 + I_2)$$

$= \varphi(y)\varphi(a_1) + \varphi(x)\varphi(a_2)$

$= \varphi(ya_1 + xa_2)$

we find φ is onto.

NOTES

Remarks: (*i*) If φ is onto, by Fundamental theorem,

$$\frac{R}{\text{Ker}\,\varphi} \cong \frac{R}{I_1} \times \frac{R}{I_2}$$

i.e.,
$$\frac{R}{I_1 \cap I_2} \cong \frac{R}{I_1} \times \frac{R}{I_2}.$$

(*ii*) Let $R = \mathbf{Z}$ the integers and suppose m, n are co-prime integers.

Then $\exists$ integers x, y s.t.,

$$1 = mx + ny \in (m) + (n)$$

$$\Rightarrow (m) + (n) = R$$

$$\Rightarrow (m), (n) \text{ are comaximal ideals}$$

$$\Rightarrow \varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto}$$

$$\Rightarrow \frac{\mathbf{Z}}{(m) \cap (n)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$$

$$\Rightarrow \frac{\mathbf{Z}}{(mn)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$$

$$\Rightarrow \mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n \text{ if } m, n \text{ are co-prime.}$$

(*iii*) Let m, n be co-prime integers, then

$$\varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto}$$

Consider $(a + (m), b + (n)) \in \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$, then $\exists$ an integer x s.t.,

$$\varphi(x) = (a + (m), b + (n))$$

Thus
$$(x + (m), x + (n)) = (a + (m), b + (n))$$

$$\Rightarrow x + (m) = a + (m), x + (n) = b + (n)$$

$$\Rightarrow x - a \in (m), \; x - b \in (n)$$

$$\Rightarrow x - a = \text{multiple of } m, \; x - b = \text{multiple of } n$$

$$\Rightarrow x \equiv a \pmod{m}, \; x \equiv b \pmod{n}$$

Proving what is popularly known as the *Chinese Remainder theorem*.

We now come to an important class of ideals which are not contained in any (other) proper ideal.

Maximal Ideals

Definition: Let R be a ring. An ideal $M \neq R$ of R is called a *maximal ideal* of R if whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

NOTES

Example 1: A field F has only two ideals F and $\{0\}$. It is easy to see then that $\{0\}$ is the only maximal ideal of F.

Example 2: Let $< \mathbf{E}, +, . >$ be the ring of even integers.

Let $H_4 = \{4n \mid n \text{ an integer}\}$

then H_4 is an ideal of $\mathbf{E}$ and as $2 \notin H_4$, $H_4 \neq \mathbf{E}$.

Let A be any ideal of $\mathbf{E}$, s.t., $H_4 \subseteq A \subseteq \mathbf{E}$

Suppose $H_4 \neq A$. We show $A = \mathbf{E}$.

Since $H_4 \subset A$, $\exists$ some $x \in A$ s.t., $x \notin H_4$

By division algorithm, we can write

$x = 4q + r$ where $0 < r < 4$

Note $r = 0$ would mean $x = 4q \in H_4$. But $x \notin H_4$ so $r \neq 0$. Again, $r = 1, 3$ would imply x is odd which is not true. Hence the only value that r can have is 2.

Thus $x = 4q + 2 \Rightarrow 2 = x - 4q \in A$

as $x \in A$, $4q \in H_4 \subseteq A \Rightarrow x - 4q \in A$

$2 \in A \Rightarrow$ members of the type $2 + 2$, $2 + 2 + 2$, ..., $0 - 2$ are all in A

$\Rightarrow \mathbf{E} \subseteq A$. But $\mathbf{A} \subseteq \mathbf{E}$

Hence $A = \mathbf{E}$ and H_4 is, therefore, a maximal ideal of $\mathbf{E}$.

Example 3: $\{0\}$ in the ring $\mathbf{Z}$ of integers is not a maximal ideal as $\{0\} \subset H_4 \subset \mathbf{Z}$

where $H_4 = \{4n \mid n \in \mathbf{Z}\}$

Example 4: Let R^c = ring of all real valued continuous functions on [0, 1], under the operations

$$(f + g)x = f(x) + g(x)$$

$$(fg)x = f(x)g(x)$$

Let $M = \{f \in R^c \mid f(\tfrac{1}{2}) = 0\}$

then M is a maximal ideal of R^c.

Let g be a function from [0, 1] to the real nos., defined by

$g(x) = 0$ for all $x \in [0, 1]$

then g is a real valued function and $g(\tfrac{1}{2}) = 0$, hence $g \in M$. Thus $M \neq \varphi$.

Again, if $f, g \in M$ be any two members, then

$$f(\tfrac{1}{2}) = g(\tfrac{1}{2}) = 0$$

$$(f - g)(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2}) = 0 - 0 = 0 \Rightarrow f - g \in M$$

Also for $f \in M$, $h \in R^c$

$$(hf)^{1/2} = h(\tfrac{1}{2})\, f(\tfrac{1}{2}) = h(\tfrac{1}{2}).\ 0 = 0 = (fh)^{1/2}$$

$$\Rightarrow hf, fh \in M$$

or that M is an ideal.

Define now, θ a function from [0, 1] to the reals by

$$\theta(x) = 1 \text{ for all } x \in [0, 1]$$

then θ is a continuous function. Thus $\theta \in R^c$.

But $\theta \notin M$ as $\theta(\tfrac{1}{2}) = 1 \neq 0$

So $M \neq R^c$.

Let I be any ideal of R^c s.t. $M \subset I \subseteq R^c$

then $\exists\ \lambda \in I$ s.t., $\lambda \notin M$

i.e., $\lambda(\tfrac{1}{2}) \neq 0$

Let $\lambda(\tfrac{1}{2}) = c \neq 0$

Define β from [0, 1] to reals such that

$$\beta(x) = c \text{ for all } x \in [0, 1]$$

then $\beta \in R^c$

Let $\psi = \lambda - \beta$

then $\psi(\tfrac{1}{2}) = \lambda(\tfrac{1}{2}) - \beta(\tfrac{1}{2}) = c - c = 0$

$$\Rightarrow \psi \in M$$

$$\Rightarrow \psi \in I \text{ as } M \subseteq I$$

i.e., $\beta = \lambda - \psi \in I$ [λ, ψ belong to I]

If γ be the function from [0, 1] to reals s.t.,

$$\gamma(x) = \frac{1}{c} \quad (c \neq 0)$$

then $\gamma \in R^c$

Now $(\gamma\beta)(x) = \gamma(x)\ \beta(x) = \frac{1}{c}.\ c = 1 = \theta(x)$ for all x

$$\Rightarrow \gamma\beta = \theta$$

Since $\beta \in I$, $\gamma\beta \in I$

we find $\theta \in I$

But θ is unity of the ring R^c,

thus I is an ideal containing unity

$$\Rightarrow I = R^c$$

Hence M is maximal.

NOTES

NOTES

Aliter: That M is maximal ideal can also be proved by using the Fundamental theorem of homomorphism.

Define a function $\theta : R^c \to \mathbf{R}$, s.t.,

$$\theta(f) = f(½) \text{ for all } f \in R^c$$

where $\mathbf{R}$ = set of real numbers

then θ is a homomorphism as

$$\theta(f + g) = (f + g)(½) = f(½) + g(½) = \theta(f) + \theta(g)$$

$$\theta(fg) = (fg)(½) = f(½)\, g(½) = \theta(f)\ \theta(g)$$

To check ontoness, we notice, if $r \in \mathbf{R}$ be any element we can define another map $\varphi : [0, 1] \to \mathbf{R}$, s.t.,

$$\varphi(x) = r \text{ for all } x \in [0, 1]$$

then φ being constant function will be continuous.

Thus $\varphi \in R^c$

Also $\theta(\varphi) = \varphi(½) = r$, showing that φ is pre-image of r under θ

i.e., θ is onto.

Thus by Fundamental theorem of homomorphism

$$\frac{R^c}{\text{Ker } \theta} \cong \mathbf{R}$$

Now $f \in \text{Ker } \theta \Leftrightarrow \theta(f) = 0$

$$\Leftrightarrow f(\tfrac{1}{2}) = 0$$

$$\Leftrightarrow f \in M$$

$$\Rightarrow \text{Ker } \theta = M$$

Hence $\frac{R^c}{M} \cong \mathbf{R}$, but $\mathbf{R}$ being a field, $\frac{R^c}{M}$ will be a field.

i.e. M is maximal ideal of R^c (see theorem 3 below).

Problem 1: *Let R^c be the ring of real valued continuous functions on* [0, 1]. *Let* $M = \{f \in R^c \mid f(\tfrac{1}{2}) = 0\}$. Let $g \in R^c$ be such that $g(x) = x - \tfrac{1}{2}\ \forall\ x \in [0, 1]$. *Then g is continuous and is in M. Show that* $M = < g >$.

Solution: Let $f \in M$ be any member

Define: h: $[0, 1] \to \mathbf{R}$ s.t.,

$$h(x) = \frac{f(x)}{x - \frac{1}{2}} \text{ when } x \neq \tfrac{1}{2}$$

$$= f(x) \text{ when } x = \tfrac{1}{2}$$

where **R** is the field of reals.

Then for $x \neq \frac{1}{2}$

$$(gh)x = g(x)h(x) = g(x)\frac{f(x)}{g(x)} = f(x)$$

and for $x = \frac{1}{2}$

$$(gh)x = g(x)h(x) = 0 = f(x)$$

and hence $f = gh$ (Note $h \in R^c$ as f and g are continuous)

Thus $M \subseteq < g > \subseteq M \Rightarrow M = < g >$

Theorem 3: *Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R iff* $\frac{R}{M}$ *is a field.*

Proof: Let M be maximal ideal of R. Since R is commutative ring with unity, $\frac{R}{M}$ is also a commutative ring with unity. Thus all that we need prove is that non zero elements of $\frac{R}{M}$ have multiplicative inverse.

Let $x + M \in \frac{R}{M}$ be any non zero element

then $x + M \neq M \Rightarrow x \notin M$

Let $xR = \{xr \mid r \in R\}$

It is easy to verify that xR is an ideal of R. Since sum of two ideals is an ideal, $M + xR$ will be an ideal of R.

Again as $x = 0 + x \,.\, 1 \in M + xR$ and $x \notin M$ we find

$$M \subset M + xR \subseteq R$$

M maximal $\Rightarrow M + xR = R$

Thus $1 \in R \Rightarrow 1 \in M + xR$

$\Rightarrow 1 = m + xr$ for some $m \in M, r \in R$

$\Rightarrow 1 + M = (m + xr) + M$

$= (m + M) + (xr + M) = xr + M$

$= (x + M)(r + M)$

$\Rightarrow (r + M)$ is multiplicative inverse of $x + M$

Hence $\frac{R}{M}$ is a field.

Conversely, let $\frac{R}{M}$ be a field.

NOTES

NOTES

Let I be any ideal of R s.t., $M \subset I \subseteq R$

then $\exists$ some $a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is a non zero element of $\frac{R}{M}$, which being a field, means $a + M$ has multiplicative inverse. Let $b + M$ be its inverse. Then

$$(a + M)(b + M) = 1 + M$$
$$\Rightarrow ab + M = 1 + M$$
$$\Rightarrow ab - 1 \in M$$
$$\Rightarrow ab - 1 = m \text{ for some } m \in M$$
$$\Rightarrow 1 = ab - m \in I \text{ (using def. of ideal)}$$

$\Rightarrow I = R$ (ideal containing unity, equals the ring)

Hence M is maximal ideal of R.

Remarks: (*i*) $\frac{R}{M}$ being a field contains at least two elements and thus unity and zero elements of $\frac{R}{M}$ are different *i.e.*, $0 + M \neq 1 + M$ *i.e.*, $1 \notin M$ or that $M \neq R$.

(*ii*) In the converse part of the above theorem we do not require R to have unity or it to be commutative, *i.e.*, if R is a ring and M is an ideal of R s.t., $\frac{R}{M}$ is a field then M is maximal.

Suppose I is an ideal of R s.t., $M \subset I \subseteq R$. Then $\exists\ a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is non zero element of $\frac{R}{M}$ and therefore has multiplicative inverse, say, $b + M$. If $c + M$ be unity of $\frac{R}{M}$. (Note $\frac{R}{M}$ can have unity even if R doesn't have unity. See exercises on page 394).

Now $(a + M)(b + M) = c + M$.

$\Rightarrow ab + M = c + M$

$\Rightarrow c - ab \in M \subset I$

But $a \in I \Rightarrow ab \in I$ and so $(c - ab) + ab \in I$

$\Rightarrow c \in I$

Let $r \in R$ be any element

Then $(r + M)(c + M) = r + M$

$\Rightarrow rc + M = r + M$

$\Rightarrow r - rc \in M \subset I$

Since $c \in I$, $rc \in I$ and thus $(r - rc) + rc \in I \Rightarrow r \in I \Rightarrow R \subseteq I$.

Hence $I = R$ and thus M is maximal ideal of R.

(*iii*) Again, the condition of commutativity is essential in the theorem is established by the fact that we can have M, a maximal ideal in R where R/M is not a field and R is a non commutative ring with unity. See next problem.

Cor.: A commutative ring R with unity is a field iff it has no proper (non trivial) ideals.

If R is a field then it has no proper ideals

Conversely, if R has no proper ideals then $\{0\}$ must be a maximal ideal. Thus $\frac{R}{\{0\}}$ is a field and as $\frac{R}{\{0\}} \cong R$, R is a field.

Problem 2: *Let R be the ring of $n \times n$ matrices over reals. Show that R has only two ideals namely $\{0\}$ and R. Hence show that $\{0\}$ is maximal ideal of R.*

Solution: Let J be a non zero ideal of R. Let A be a non zero matrix in J. Since $A \neq 0$, it has some non zero entry. Suppose $A = (a_{ij})$ and suppose $a_{rs} \neq 0$ in A.

If E_{ij} denotes the unit matrix in R whose (i, j)th entry is 1 and 0 elsewhere

then $E_{ij} E_{kr} = 0$ if $j \neq k$

$= E_{ir}$ if $j = k$

Now $A = a_{11}E_{11} + a_{12}E_{12} + ...+a_{nn} E_{nn}$

Consider $E_{ir} A E_{si} = E_{ir}(a_{11}E_{11} + a_{12}E_{12} + ...+a_{nn} E_{nn})E_{si}$

$= E_{ir}(a_{rs} E_{rs})E_{si}$

$= a_{rs} E_{ir} E_{si}$

$= a_{rs} E_{ii} \in J$ as $A \in J \quad \forall i$

So $(a_{rs}^{-1} E_{ii})(a_{rs} E_{ii}) \in J$

$\Rightarrow E_{ii} \in J, \quad \forall i = 1, 2, 3,...n$

Thus identity matrix I in R can be written as $I = E_{11} + E_{12} + ...+E_{nn} \in J$.

So unity of R belongs to J or that $J = R$. Hence $\{0\}$ and R are the only ideals of R and so $\{0\}$ is maximal ideal of R.

Note: Since $R \cong \frac{R}{\{0\}}$, and R is not a field, we find $\frac{R}{\{0\}}$ is not a field even though $\{0\}$ is maximal. See remark above.

Definition:

Prime Ideal: An ideal P of a ring R is called a *prime ideal* if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Example 5: $\{0\}$ in the ring $\mathbf{Z}$ of integers is a prime ideal as $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

It is an example of a prime ideal which is not maximal.

Example 6: $H_4 = \{4n \mid n \in \mathbf{Z}\}$ we've seen is a maximal ideal in the ring **E** of even integers.

NOTES

H_4, however, is not a prime ideal as $2 \,.\, 2 = 4 \in H_4$ but $2 \notin H_4$.

In fact, H_4 is neither a maximal nor a prime ideal in **Z**.

Example 7: $H_p = \{pn \mid n \in \mathbf{Z}\}$ will be a prime ideal in **Z** for any prime p.

It will also be a maximal ideal in **Z**

Remark: In view of the above examples we observe that in the ring **Z** of integers

(*i*) every ideal in **Z** is generated by some $n \in \mathbf{Z}$.

(*ii*) An ideal in **Z** is maximal iff it is generated by a prime.

(*iii*) One can show that in **Z** a prime ideal is either generated by a prime or is the zero ideal. Consequently, a non zero ideal in **Z** is prime iff it is maximal.

Let $P = < n >$ and suppose n is prime.

Let $ab \in p = < n >$, then $ab = kn \Rightarrow n \mid ab$

$\Rightarrow n \mid a$ or $n \mid b$

$\Rightarrow a \in P$ or $b \in P$

or that P is prime ideal.

Conversely, let $P = < n >$ be a prime ideal

Suppose n is not a prime and

$n = ab, \quad 1 < a, b < n$

Let $A = < a >, B = < b >$, then $P \subseteq A$ and $P \subseteq B$

Now $ab \in P$ and P is prime

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$

$\Rightarrow$ either $A = P$ or $B = P$

i.e, either $b = 1$ or $a = 1$ or that n is a prime.

(*iv*) $\{0\}$ is thus a prime ideal in **Z** but not maximal whereas every maximal ideal is prime.

Theorem 4: *Let R be a commutative ring. An ideal P of R is prime iff* $\frac{R}{P}$ *is an integral domain.*

Proof: Let P be a prime ideal of R

Let $(a + P)(b + P) = 0 + P$

Then $ab + P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow a + P = P$ or $b + P = P$

thus $\frac{R}{P}$ is integral domain.

NOTES

Conversely, let $\frac{R}{P}$ be an integral domain.

Let $ab \in P$ then $ab + P = P$

$\Rightarrow (a + P)(b + P) = P$

$\Rightarrow a + P = P$ or $b + P = P$ (R/P is an integral domain)

$\Rightarrow a \in P$ or $b \in P$

Hence the result.

Theorem 5: *Let R be a commutative ring. An ideal P of R is a prime ideal if and only if for two ideals A, B of R, $AB \subseteq P$ implies either $A \subseteq P$ or $B \subseteq P$.*

Proof: Let P be a prime ideal of R and let $AB \subseteq P$ for two ideal A, B of R.

Suppose $A \not\subseteq P$ then $\exists$ some element $a \in A$ s.t., $a \notin P$.

Since $AB \subseteq P$, we get in particular

$aB \subseteq P$

$\Rightarrow ab \in P$ for all $b \in B$

Since P is prime, we get either $a \in P$ or $b \in P$ but $a \notin P$, hence $b \in P$ for all $b \in B$.

$\Rightarrow B \subseteq P$

Conversely, we show P is prime. Let $ab \in P$.

Let A and B be the ideals generated by a and b then $A = (a)$, $B = (b)$. If $x \in AB$ is any element then it is of the type

$$x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n \qquad a_i \in A,\ b_i \in B$$
$$= (\alpha_1 a)\ (\beta_1 b) + (\alpha_2 a)\ (\beta_2 b) + \ldots\ldots + (\alpha_n a)\ (\beta_n b)$$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a)$, $b_i \in B = (b)$

Thus $$x = (\alpha_1\beta_1)\ (ab) + (\alpha_2\beta_2)\ (ab) + \ldots\ldots + (\alpha_n\beta_n)\ (ab)$$

(R is commutative)

$$x = (\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots\ldots + \alpha_n\beta_n)ab$$

Since $ab \in P$, P is an ideal, all multiples of ab are in P. Thus $x \in P$

i.e., $AB \subseteq P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$

$\Rightarrow (a) \subseteq P$ or $(b) \subseteq P$

$\Rightarrow a \in P$ or $b \in P \Rightarrow P$ is prime.

NOTES

Problem 3: *Let R be a commutative ring with unity such that* $a^2 = a \ \forall a \in R$. *If I be any prime ideal of R, Find all the elements of R/I.*

Solution: Since I is a prime ideal of R, R/I is an integral domain, and $1 + I$ is unity of R/I.

Let $r + I \in R/I$ be any member

then $(r + I)^2 = r^2 + I = r + I$ (given condition)

$\Rightarrow (r + I)[(r + I) - (1 + I)] = 0 + I$

But R/I is an integral domain and therefore, either $r + I = 0 + I$ or $(r + I) = 1 + I$

or that R/I contains only two elements $0 + I$ and $1 + I$.

Problem 4: *Let R be a non zero commutative ring with unity. If every ideal of R is prime show that R is a field and conversely.*

Solution: To show that R is a field, we need show that every non zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ st., $ab = 0$

Then $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

i.e., $a = 0$ or $b = 0$

thus R is an integral domain.

Let now $a \in R$ be any non zero element and let

$a^2R = \{a^2r \mid r \in R\}$

then a^2R is an ideal of R (Verify!) and is therefore prime ideal.

Now $a \,.\, a = a^2 = a^2 \,.\, 1 \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

$\Rightarrow a\,(1 - ab) = 0$

$\Rightarrow 1 - ab = 0$ as $a \neq 0$

$\Rightarrow b$ is multiplicative inverse of a.

Hence R is a field.

Converse follows easily as a field R has no ideals except $\{0\}$ and R.

Problem 5: *Let R be a commutative ring with unity. Show that every maximal ideal of R is prime.*

Solution: We know that an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

Thus if M is maximal, then $\frac{R}{M}$ is a field and hence an integral domain.

$\Rightarrow M$ is a prime ideal (theorem 4).

NOTES

Problem 6: *Let R be a commutative ring with unity and let M be a maximal ideal of R such that* $M^2 = \{0\}$. *Show that if N is any maximal of R then N = M.*

Solution: Let $m \in M$ be any element

then $m \cdot m \in M^2 = (0)$

$\Rightarrow m^2 = 0 \in N$ (N is an ideal)

By previous problem, N will be prime

$\Rightarrow m \in N$

$\Rightarrow M \subseteq N$

Thus $M \subseteq N \subseteq R$

Since M is maximal, $N = M$ or $N = R$

But N is maximal in R, thus $N \neq R$

Hence $N = M$.

Problem 7: *Show that in a Boolean ring R, every prime ideal* $P \neq R$ *is maximal*.

Solution: Let P be prime and I be any ideal s.t.,

$P \subset I \subseteq R$

then $\exists$ some $x \in I$, s.t., $x \notin P$ and as $x \in R$, $x^2 = x$.

Let now, $y \in R$ be any element, then

$x^2y = xy$

$\Rightarrow x(xy - y) = 0 \in P$ (P is an ideal)

$\Rightarrow xy - y \in P$ as $x \notin P$ and P is prime

$\Rightarrow xy - y = p$ for some $p \in P$

Then $y = xy - p \in I$

as $x \in I$, $y \in R$, $xy \in I$ and also $p \in P \subseteq I$,

Thus $y \in I$

$\Rightarrow R \subseteq I \Rightarrow I = R \Rightarrow P$ is maximal.

Problem 8: *Show by an example that we can have a finite commutative ring in which every maximal ideal need not be prime.*

Solution: Consider the ring $R = \{0, 2, 4, 6\}$ under addition and multiplication modulo 8.

Let $M = \{0, 4\}$ then M is easily seen to be an ideal of R.

Again as $2 \otimes 6 = 4 \in M$ but $2, 6 \notin M$, we find M is not a prime ideal. We show M is maximal.

Let $M \subseteq N \subseteq R$, where N is an ideal of R.

Since $< M, + >$ will be a subgroup of $<N, + >$, by Lagrange's theorem $o(M) \mid o(N)$. Similarly, $o(N) \mid o(R) = 4$

i.e., $2 \mid o(N)$, $o(N) \mid 4$

i.e., $o(N) = 2$ or 4

if $o(N) = 2$, then $M = N$ as $M \subseteq N$

if $o(N) = 4$, then $N = R$ as $N \subseteq R$

Hence M is maximal ideal of R.

NOTES

Remark: In case the finite commutative ring contains unity, then every prime ideal is maximal.

Definition: An ideal I of a commutative ring R is called semi prime ideal if $a^2 \in I \Rightarrow a \in I$, for all $a \in R$ clearly then every prime ideal is semi prime.

Example 8: Consider the ideal $I = \{6n \mid n \in \mathbf{Z}\}$ in the ring of integers. Suppose $a^2 \in I$

Then a^2 is a multiple of 6

i.e., $6 \mid a^2$

Since $2 \mid 6$, we find $2 \mid a^2 \Rightarrow 2 \mid a$ (as 2 is prime)

Similarly $3 \mid a$

$\Rightarrow 6 \mid a$ as g.c.d.(2, 3) = 1

$\Rightarrow a \in I$

Hence I is semi prime, but I is not prime as $2 \cdot 3 = 6 \in I$ but $2, 3 \notin I$.

10.3 MORE QUOTIENT RINGS AND RELATED PROBLEMS

Definition: Let R be a ring and N be any ideal of R, then the system $<R/N, +, .>$ where $R/N = \{r+N \mid r \in R\}$ and $+$ &. are binary compositions on R/N defined by $(r + N) + (s + N) = (r + s) + N$ and $(r + N).(s + N) = rs + N$ for all $r, s \in R$, is a ring. This ring is called the *quotient ring* of R with respect to the ideal N.

NOTATION We shall usually denote the element $x + N$ of R/N by $\bar{x}$; thus $\bar{0}$ in this notation will mean N, the zero of R/N. One finds from definition that for any $\bar{x}, \bar{y} \in R/N, \bar{x} + \bar{y} = \overline{x + y}$ and $\overline{xy} = \overline{xy}$.

Example 9: Let $N = \{6n \mid n \in Z\}$. N. is an ideal of Z. The elements of Z/N are the cosets N, $1 + N$, $2 + N$, $3 + N$, $4 + N$ and $5 + N$ which according to our notation can be denoted by $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$, and $\bar{5}$ respectively. Then $<Z/N, +, .>$ is a ring where both addition and multiplication are modulo 6. See the following tables.

Addition Table

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Multiplication table

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

NOTES

Definition: *(Prime ideal)* Let R be a commutative ring. An ideal P of R is called a *Prime Ideal* if $\forall a, b \in R, ab \in P \Rightarrow a \in P$ or $b \in P$.

Example 10: In an integral domain D, (0) is a prime ideal. Since $\forall$ $a, b \in D$, $ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0$ *as* D is integral deomain.

Example 11: In $\boldsymbol{Z}$, the ideal $(3) = \{3n \mid n \in \mathbf{Z}\}$ is prime, since $ab \in (3) \Rightarrow 3 \mid ab \Rightarrow 3 \mid a$ or $3 \mid b \Rightarrow a \in (3)$. In fact every ideal $(p) = \{pn \mid n \in \mathbf{Z}\}$ where p is a prime number, is a prime ideal of Z.

Theorem 5: An ideal P of commutative ring R is prime if and only if R/P is an integral domain.

Proof Let R/P be an integral domain, then for all $a, b \in R$,

$$\begin{aligned} ab \in P &\Rightarrow \overline{ab} = \bar{0} \Rightarrow \bar{a}\bar{b} = \bar{0} \text{ where } \bar{a} = a + P \\ &\Rightarrow \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0}, \text{ as } R/P \text{ is an integral domain} \\ &\Rightarrow a \in P \text{ or } b \in P. \end{aligned}$$

Thus P is a prime ideal.

Conversely let P be a prime ideal; then

$$\begin{aligned} \bar{a}\bar{b} = \bar{0} &\Rightarrow \overline{ab} = \bar{0} \\ &\Rightarrow ab \in p \\ &\Rightarrow a \in P \text{ or } b \in P \\ &\Rightarrow \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0} \end{aligned}$$

Also R/P is commutative as R is commutative.

Consequently R/P is a commutative ring without proper zero divisors. Hence R/P is an integral domain.

Definition: (*Maximal ideal*)

An ideal M of a ring R is said to be a *maximal ideal of R,* if

(*i*) $M \neq R$,

(*ii*) there exists no ideal J of R such that $M < J < R$.

NOTES

Thus from *(ii)* if $M\ (\neq R)$ is a maximal ideal then for any ideal J of R, $M \subseteq J \subseteq R$ holds only when either $J = M$ or $J = R$.

Example 12: In a division ring D, (0) is a maximal ideal. Trivially $(0) \neq D$ as $1 \in D$ *as* $1 \in D$ and $1 \neq 0$. Let J be any non-zero ideal of D, then $\exists x\,(\neq 0)$ in J. But D is a division ring so $x^{-1} \in D$; which gives $1 = xx^{-1} \in J$. Consequently $J = D$. Hence (0) is a maximal ideal.

Example 13: In the ring E of even integers, ideal (4) is maximal. As $2 \in (4)$, $(4) \neq E$. Further let J be an ideal of E such that $(4) < J$. Then there exists an element $x \in J$ such that $x \notin (4)$. In other workds x is an even integer not divisible by 4. Consequently x=4n + *2* for some integer n. Now $2 = 4x - 4n \in J$ as $4n \in (4) < J$ and $x \in J$. Thus every even integral multiple of 2 is in J. Hence $E = J$. This proves the assertion.

Theorem 7: An ideal M of a commutative ring R with unity is a maximal ideal if and only if R/M is a field.

Proof: Let M be a maximal ideal of R. Since R is commutative, R/M is commutative. Further 1 is the unity of R gives $\overline{1}$ is the unity of R/M. $M \neq R \Rightarrow \overline{1} \neq \overline{0}$. Thus to show that R/M is a field it is sufficient to prove that every non-zero element of R/M is a unit. Let $\bar{x}(\neq \overline{0}) \in R/M$ then $x \notin M$. Consider $xR = \{xr \mid r \in R\}$. xR is an ideal of R and $x = x1 \in R$. Since $x \in M + xR$, $x \notin M$, $M < M + xR$. The maximality of M gives $M + xR = R$. Again $1 \in R = M + xR \Rightarrow' \exists m \in M, r \in R$ such that $1 = m + xr$. This implies that $1 + M = xr + M \Rightarrow \overline{1} = \overline{xr} = \overline{x}\overline{r}$. Therefore, $\bar{x}$ is a unit. Hence R/M is a field.

Conversely as the unity of field is different from zero, $\overline{1} \neq \overline{0}$ *i.e.* $1 \notin M$. Thus $M \neq R$. Let I be any ideal of R such that $M < I$. Choose $a \in I$ such that $a \notin M$. Then $\overline{a} \neq \overline{0}$, so $\overline{a}$ is invertible in R/M. Consequently $\exists \overline{b} \in \overline{R} = R/M$ such that $\overline{a}\overline{b} = \overline{1}$, this yields $1 - ab \in M \Rightarrow 1 - ab \in I$ as $M < I$. This in turn implies that $1 = (1 - ab) + ab \in I$ as $ab \in I$ (I is an ideal and $a \in I$). Hence $I = R$.

Remark: If M is any maximal ideal of a commutative ring R with unity then R/M is a field and we also know that every field is an integral domain, we get M is a prime ideal. *Thus every maximal ideal in a commutative ring with unity is prime.*

However the converse of this statement is not true.

Example 14: Consider the ideal (0) of **Z,** since **Z** is an integral domain, (0) is a prime ideal of **Z,** but (0) is not maximal since (0) < (2) <**Z.**

Worked-Out Exercises

Exercise 1 *Let R be the ring of all real-valued continuous functions on the closed interval* $[0,1]$. *Let* $M = \left\{ f \in R \mid f\left(\frac{1}{3}\right) = 0 \right\}$. *show that M is a maximal ideal of R.*

NOTES

Solution The function $w:[0, 1] \to \mathbf{R}$ *given by* $w(x) = 0 \vee x \in [0,1]$ belongs to *M*. Hence *M* is non-empty.

Let *f, g* $\in M$. Then $(f-g)\left(\frac{1}{3}\right) = f\left(\frac{1}{3}\right) - g\left(\frac{1}{3}\right) = 0 \Rightarrow f - g \in M$. Further let $f \in M, h \in R$ then $hf\left(\frac{1}{3}\right) = h\left(\frac{1}{3}\right) f\left(\frac{1}{3}\right) = 0 \Rightarrow hf \in M$. Since *R* is commutative, $fh - hf \in M$. Hence *M* is an ideal of *R*.

Clearly $M \neq R$ as $\theta \in R$ given by $\theta(x) = 1$ does not belong to *M*.

Let *N* be an ideal of *R* such that $M < N$. There exists $\lambda \in N.\ \lambda \notin M$. This means $\lambda\left(\frac{1}{3}\right) \neq 0$. Put $\lambda\left(\frac{1}{3}\right) = c$ where $c \neq 0$.

Consider $\mu \in R$ given by $\mu = \lambda - \beta$ where $\beta(x) = c \vee x \in [0, 1]$. Then $\mu\left(\frac{1}{3}\right) = \lambda\left(\frac{1}{3}\right) - \beta\left(\frac{1}{3}\right) = c - c = 0 \Rightarrow \mu \in M \Rightarrow \mu \in N$. Therefore, $\beta = \lambda - \mu \in N$.

Define $\gamma \in R$ by $r(x) = \frac{1}{c} \vee x \in [0, 1]$

Then $\vee x \in [0, 1],\ \gamma\beta(x) = \gamma(x)\beta(x) = 1 = \theta(x) \Rightarrow \gamma\beta = \theta \in N$. But θ is unity of *R*. Hence $N = R$.

Consequently *M* is a maximal ideal of *R*.

Exercise 2 *For any two ideals A and B of a ring R such that* $B \subseteq A$, *prove that A/B and B are nilpotent (nil) imply A is nilpotent (nil) ideal.*

Solution Let $\frac{A}{B}$ and *B* be nilpotent. Then $\left(\frac{A}{B}\right)^n = (B)$.

$B^m = (0)$ for some integers, $n,\ m > 0$. $\left(\frac{A}{B}\right)^n = (B) \Rightarrow A^n \subseteq B \Rightarrow (A^n)^m \subseteq B^m \Rightarrow A^{mn} = (0) \Rightarrow A$ is nilpotent ideal.

Now suppose $\frac{A}{B}$ and *B* are nil. Let $a \in A$ then $a + B \in \frac{A}{B}$. Since $\frac{A}{B}$ is nil, there exists an integer $n > 0$ such that $(a + B)^n = B \Rightarrow a^n \in B$.

Again as B is nil, there exists an interger m>0 such that $(a^n)^m=0 \Rightarrow a^{mn} = 0$. This shows that a is nilpotent. Hence A is a nil ideal of R.

NOTES

Check Your Progress

1. When two ideals are called comaximal?
2. What is prime ideal?
3. What is maximal ideal?

10.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. Two ideals A and B are called comaximal if $A + B = R$.
2. An ideal P of a ring R is called a prime ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$.
3. Let R be a ring. An ideal $M \neq R$ of R is called a *maximal ideal* of R if whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

10.5 SUMMARY

- Two ideals A and B are called comaximal if $A + B = R$.
- Let R be a ring. An ideal $M \neq R$ of R is called a *maximal ideal* of R if whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.
- An ideal P of a ring R is called a prime ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$.
- An ideal I of a commutative ring R is called semi prime ideal if $a^2 \in I \Rightarrow a \in I$, for all $a \in R$. Clearly then every prime ideal is semi prime.

10.6 KEY WORDS

- **Ideal:** an ideal is a special subset of a ring. Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3.
- **Commutative ring:** a commutative ring is a ring in which the multiplication operation is commutative.
- **Maximal:** a maximal element of a subset S of some partially ordered set (poset) is an element of S that is not smaller than any other element in S.

10.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

NOTES

Short Answer Questions

1. Show that {0} in the ring of integers is not a maximal ideal.
2. Let R be a commutative ring with unity and let I_1 and I_2 be two ideals of R. Then show that I_1 and I_2 are comaximal ideals of R iff φ is onto.
3. Show that intersection of two prime ideals may not be a prime ideal.
4. Show that an ideal is maximal iff it is generated by a prime.

Long Answer Questions

1. Show that a commutative ring is an integral domain iff {0} is a prime ideal.
2. Show that in a Boolean ring R, every prime ideal $P \neq R$ is maximal.
3. Let $A \neq R$ be an ideal of R, then for any $x \in R$, $x \notin A$, *if* $A + (x) = R$, show that A is maximal ideal of R and conversely.
4. Find all ideals of Z_{12}, Z_{36}. Which of these are maximal?

10.8 FURTHER READINGS

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Gilbert, Linda. 2008. Elements of Modern Algebra. Boston: Cengage Learning.

Gorodentsev, Alexey L. 2016. *Algebra I: Textbook for Students of Mathematics*. Berlin: Springer.

Herstein , I.N. 2006. *TOPICS IN ALGEBRA, 2ND ED*. New Jersey: John Wiley & Sons.

UNIT 11 THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN AND EUCLIDEAN RINGS

Structure

11.0 INTRODUCTION

You have studied about quotient rings in the previous unit and you will expand your knowledge of the field of quotients of an integral domain in this unit. Further, you will understand the concept of Euclidean rings. A Euclidean domain (also called a Euclidean ring) is an integral domain that can be endowed with a Euclidean function which allows a suitable generalization of the Euclidean division of the integers.

11.1 OBJECTIVES

After going through this unit, you will be able to:

- Discuss the field of quotients of an integral domain
- Know about Euclidean rings

11.2 FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

Some types of rings are easier to study and their structures are better known than those of the other types. If one can embed a certain ring R in a ring S, such that the structure of the latter is better known than that of former, then by using the properties of S one can say a lot about the properties of R. The process of embedding of one ring into another has been quite fruitfully used for the development of ring theory.

There are many procedures of embedding of one ring into another. Here in this section we confine ourselves to only two methods: (**I**) Embedding of a ring in a ring with unity, (**II**) Embedding of a domain in a field.

(I) *Embedding of a ring in a ring with unity*

Let R be a ring, consider $R \times \mathrm{Z} = \{(r,n) \mid r \in R, n \in \mathbf{Z}\}$. $\mathrm{R} \times \mathbf{Z}$ can be made into a ring by defining addition and multiplication as under:

For all $(r,n),(s,m) \in R \times \mathbf{Z}, (r,n)+(s,m) = (r+s, n+m)$

and $(r,n)(s,m) = (rs+ns+mr, nm).$

It can be checked that $R \times \mathbf{Z}$ is a ring with unity (0,1).

Theorem 1 Every ring can be embedded in a ring with unity.

Proof Let R be a ring, then as remarked above $R_1 = R \times \mathbf{Z} = \{(r,n) \mid r \in R, n \in \mathbf{Z}\}$ is a ring. We define $f : R \to R_1$ by $f(r) = (r,0) \forall r \in R.$ Clearly f is a homomorphism. f is also 1-1 as $f(r) = f(s) \Rightarrow (r,0) = (s,0) \Rightarrow r = s.$

Hence $R \cong f(R) \subseteq R_1.$ Consequently R is embeddable in R_1 which has unity namely (0,1).

Remark The embedding discussed in the above theorem is *very nice* in the sense that *f(R)* is an ideal of R_1. To check this, note that for (r,0)

$$\in f(R), (s,n) \in R_1, (r,0)(s,n) = (rs+0s+nr, 0n)$$
$$= (rs+nr, 0) \in f(R).$$

Similarly $(s,n)(r,0) = (sr+nr,0) \in R).$ Thus *R, under identification of r with* (*r,* 0), becomes an ideal of R_1.

(II) *Embedding of a domain in a field.*

Every subring of a field is an integral domain. Naturally one can ask that given an integral domain, can we find a field which has that domain, as its subring? Or formally speaking, can an integral domain be embedded in a field? The question is of vital importance when one considers the solution of linear equation $ax = b, a \neq 0,$ in an integral domain D. Of course if a solution exists in D, it must be unique (Why?). It is quite possible that no solution may exist in D. For example in **Z**, 3*x*–5 has no solution. But in a field *F, ax=b,* $a \neq 0$ always has a solution namely $a^{-1}b$. Thus if a domain D can be embedded in a field F then an equation $ax = b, a \neq 0$ with coefficients in D will at least have a solution in F. Now we endeavour to construct a field in which a given integral domain can be embedded. Our procedure is motivated by the method of construction of rational numbers from integers.

Let D be an integral domain with at least two elements and let $D_o = D - \{0\}.$ Consider $D \times D_o = \{(a,b) \mid a,b \in D, b \neq 0\}.$

NOTES

Define a relation '~' on $D \times D_o$ as under:

For all $(a,b)(c,d) \in D \times D_o, (a,b) \sim (c,d)$ if and only if $ad = bc$.

Lemma 1. '~' is an equivalence relation on $D \times D_o$.

Proof Let $(a,b),(c,d),(e,f) \in D \times D_o$.

(*i*) *Reflexivity:* As $ab = ba$, putting $d = b$ and $c = a$ in the definition of '~' we see that $(a, b) \sim (a,b)$.

(*ii*) *Symmetry:* $(a,b) \sim (c,d) \Rightarrow ad = bc$

$$\Rightarrow cb = da \Rightarrow (c,d) \sim (a,b).$$

(*iii*) *Transitivity*: $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

$$\Rightarrow ad = bc \text{ and } cf = de,$$
$$\Rightarrow adf = bcf$$
$$\Rightarrow adf = bde \text{ as } cf = de,$$

$\Rightarrow af = be$ as $d \neq 0$ and cancellation law holds in D_o.

$$\Rightarrow (a,b) \sim (e,f).$$

Hence '~' is an equivalence relation on $D \times D_o$.

Remark From the definition of equivalence relation one sees immediately that for any non-zero elements *a,b* and *c* of *D,* (0,*a*)~(0,*b*); (*a,a*)~(*b,b*) and (*ac, bc*)~*(a,b*).

Let *a/b* be the equivalence class of (*a,b*). By properties of equivalence classes it is evident that *a/b=c/d* if and only if *ad=bc.* Now if *F* is the family of all equivalence classes *a/b* of $D \times D_o$, we shall show that under suitably defined addition and multiplication, *F* becomes a field. Once again the addition and multiplication of rational numbers will give us a clue. So we define for all $a/b, c/d \in F, a/b + c/d = (ad + bc)/bd$ and $(a/b)(c/d) = ac/bd$. Note that as *D* is an integral domain, $b \neq 0, d \neq 0 \Rightarrow bd \neq 0,$ so (*ad* + *bc*)/*bd* and *ac/bd* $\in F$. In order that our definitions should make sense we must show that they are independent of the choice of representatives of equivalence classes involved in the operations. In other words we must show that if $a/b = a'/b'$ and $c/d = c'/d'$ then $(Ad + bc)/bd = (a'd'+b'c')/b'd'$ and $ac/bd = a'c'/b'd'$.

Lemma 2 The addition and multiplication as defined above are well-defined.

Proof Let $a/b = a'/b'$ and $c/d = c'/d'$

then $ab' = a'b$ and $cd' = c'd.$ (1)

Now (1) $\Rightarrow ab'dd' = a'bdd'$ and $bb'cd' = bb'c'd$

$\Rightarrow ab'dd'+bb'cd' = a'bdd'+bb'c'd$

$\Rightarrow (ad+bc)b'd' = (a'd'+b'c')bd$

$\Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. **(Note.** $\frac{x}{y}$ stands for *x/y*)

NOTES

Hence addition is well-defined.

Finally (1) $\Rightarrow ab'cd' = a'bc'd$

$\Rightarrow (ac)(b'd) = (ba)(d'c')$

$\Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Consequently multiplication is also well-defined. Hence the lemma follows.

Theorem 2 <F, + ,.> is a field and D can be embedded into F.

Proof From the remark following Lemma 1, it follows that for $a \neq 0 \in D, \frac{0}{a}$ and $\frac{a}{a} \in F$ and $\frac{0}{a} \neq \frac{a}{a}$. So *F* has at least two elements. Further notice that for any two non-zero elements *a, b* in *D,* $\frac{0}{a} = \frac{0}{b}$; also if $c \neq 0$ then $\frac{ac}{bc} = \frac{a}{b}$.

(1) + is *Associative:* For all $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \boldsymbol{F}$

$$= \frac{(ad+bc)f+(bd)e}{(bd)f}$$

$$= \frac{a(df)+(cf+de)b}{b(df)}$$

$$= \frac{a}{b} + \frac{cf+de}{df}$$

$$= \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right).$$

(2) + *is commutative:* For all $\frac{a}{b}, \frac{c}{d} \in \boldsymbol{F}$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{bc+ad}{db}$$

$$= \frac{c}{d} + \frac{a}{b}.$$

(3) *Existence of zero element:*

Now for $u \neq 0$ in $D, \frac{0}{u} \in \boldsymbol{F}$ is such that $\frac{a}{b} + \frac{0}{u} = \frac{au}{bu} = \frac{a}{b}$.

Hence $\frac{0}{u}$ is zero element of *F.* Let us denote it by 0.

NOTES

(4) *Existence of additive inverse:*

Since $\frac{a}{b}+\left(\frac{-a}{b}\right)=\frac{ab-ba}{b^2}=\frac{0}{b^2}$

and $\frac{0}{u}=\frac{0}{b^2}$, we have $\frac{a}{b}+\left(\frac{-a}{b}\right)=0.$

Thus $-\left(\frac{a}{b}\right)=\frac{(-a)}{b}\in \boldsymbol{F}.$

(5) *Associativity of multiplication:*

For all $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$

$$\left(\frac{a}{b}\frac{c}{d}\right)\left(\frac{e}{-f}\right)=\left(\frac{ac}{bd}\right)\left(\frac{e}{f}\right)=\frac{(ac)e}{(bd)f}$$
$$=\frac{a(ce)}{b(df)}=\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right).$$

(6) *Commutativity of multiplication:*

For all $\frac{a}{b},\frac{c}{d}\in \boldsymbol{F},\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{ab}=\frac{c}{d}\frac{a}{b}.$

(7) *Existence of unity:* Now if $u\neq 0\in D$ then $\frac{u}{u}\in F$ is such that $\frac{a}{b}\frac{u}{u}=\frac{au}{bu}=\frac{a}{b}.$

This gives that $\frac{u}{u}$ is multiplicative identity *i.e.* unity for *F.* We shall denote it by 1.

(8) *Existence of multiplicative inverses of non-zero elements:*

Now $\frac{a}{b}\neq 0\Rightarrow a\neq 0,b\neq 0\Rightarrow \frac{b}{a}\in F$

and $\frac{a}{b}\frac{b}{a}=\frac{ab}{ab}=\frac{u}{u}=1.$

Thus $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}.$

(9) *Distributivity:* For all $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+de}{df}\right)$$
$$=\frac{a(cf+de)}{b(df)}$$

$$\text{Also } \frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}=\frac{ac}{bd}+\frac{ae}{bf}$$

$$=\frac{(ac)bf+(ae)bd}{(bd)bf}$$

$$\frac{[(ac)f+(ae)d]b}{(bdf)b}$$

$$=\frac{a(cf+de)}{b(df)}.$$

Hence multiplication is distributive over addition. Consequently $<F, +, .>$ is a field.

Finally define $f: D \to F$ as under:

Take $a(\neq 0) \in D,$ then $\forall x \in D$ put $f(x)=\frac{xa}{a}.$

Let $x, y \in D,$ then $f(x)=f(y) \Rightarrow \frac{xa}{a}=\frac{ya}{a}$

$$\Rightarrow xa^2=ya^2 \Rightarrow x=y.$$

Thus f is 1–1.

Also $f(x+y)=\frac{(x+y)a}{a}=\frac{(x+y)a^2}{a^2}=\frac{xa}{a}+\frac{ya}{a}$

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

and $f(xy)=\frac{xya}{a}=\frac{(xa)(ya)}{a^2}=\frac{xa}{a}\frac{ya}{a}=f(x)f(y).$

This proves that f is a monomorphism of D into F. Hence D is embeddable in a field F.

Definition Let D be an integral domain with more than one element, than a *field of quotients* of D is a pair (F, σ) where F is a field and σ is a monomorphism of D into F such that every $z \in F$ is expressible as $\sigma(x)/\sigma(y)$ for some $x, y \in D$ with $y \neq 0.$

Remark When there is no confusion regarding the monomorphism σ then F itself will be referred to as the field of quotients of D. Now as $D \cong \sigma(D) \subseteq F,$ we shall normally identify D with its image $\sigma(D)$ and regard D iteself as a subring of F. In that case each $a \in D$ is identified with $\sigma(a)$ and hence, then each $z \in F$ is of the form $x/y; x, y \in D$ with $y \neq 0.$

Theorem 3 *Let D be an integral domain containing at least two elements then D has a field of quotients. If* (F_1, σ_1) (F_1, σ_1) *and* (F_2, σ_2) *are two fields of* quotients then there exists an isomorphism η *of* F_1 *onto* F_2 *such that* $\eta\sigma_1=\sigma_2.$

NOTES

Proof In Theorem 2 we constructed a field F such that $f : D \to F$ with $f(x) = xa / a \forall x \in D$ and a, a non-zero fixed element of D. Also we saw that f was a monomorphism. Now each $z \in F$ is of the form $x / y, x, y \in D, y \neq 0$. Then $z = (xa / a)(a / ya) = f(x) / f(y)$. Hence (F, f) is a field of quotients of D.

Let (F_1, σ_1) and (F_2, σ_2) be two fields of quotients of D.

Define $\eta : F_1 \to F_2$ as under:

Take $z \in F_1$, then by definition $z = \dfrac{\sigma_1(x)}{\sigma_1(y)}$ for some $x, y \in D, y \neq 0$.

Put $\eta(z) = \dfrac{\sigma_2(x)}{\sigma_2(y)}$.

η is well-defined since if $z = \dfrac{\sigma_1(x)}{\sigma_1(y)} = \dfrac{\sigma_1(u)}{\sigma_1(v)}$ for some $x, y, uv \in D,$ with $y \neq 0$ and $v \neq 0,$ we get $\sigma_1(xv) = \sigma_1(uy)$

$\Rightarrow xv = uy$ as σ_1 is 1–1 $\Rightarrow \sigma_2(xv) = \sigma_2(uy)$

$\Rightarrow \sigma_2(x)\sigma_2(v) = \sigma_2(u)\sigma_2(y) \Rightarrow \dfrac{\sigma_2(x)}{\sigma_2(y)} = \dfrac{\sigma_2(u)}{\sigma_2(v)}$.

Hence η is well-defined.

Now for $z = \dfrac{\sigma_1(x)}{\sigma_1(y)}, t = \dfrac{\sigma_1(u)}{\sigma_1(v)} \in F$

$$\eta(z+t) = \eta\left[\frac{\sigma_1(x)}{\sigma_1(y)} + \frac{\sigma_1(u)}{\sigma_1(v)}\right] = \eta\left[\frac{\sigma_1(xv+yu)}{\sigma_1(yv)}\right]$$
$$= \frac{\sigma_2(xv+yu)}{\sigma_2(yv)} = \frac{\sigma_2(x)}{\sigma_2(y)} + \frac{\sigma_2(u)}{\sigma_2(v)}$$
$$= \eta(z) + \eta(t)$$

Also $\eta(zt) = \eta\left[\dfrac{\sigma_1(x)}{\sigma_1(y)}\dfrac{\sigma_1(u)}{\sigma_1(v)}\right] = \eta\left[\dfrac{\sigma_1(xu)}{\sigma_1(yv)}\right] = \dfrac{\sigma_2(xu)}{\sigma 2(yv)}$

$$= \frac{\sigma_2(x)}{\sigma_2(y)}\frac{\sigma_2(u)}{\sigma_2(v)} = \eta(z)\eta(t).$$

This proves that η is a homomorphism. Now we show that η is onto. Let $z' \in F_2$, then by definition $z' = \dfrac{\sigma_2(x')}{\sigma_2(y')}$ for some $x', y' \in D$ with $y' \neq 0$. Clearly $\dfrac{\sigma_1(x')}{\sigma_1(y')} \in F_1$ is such that $\eta\left[\dfrac{\sigma_1(x')}{\sigma 1(y')}\right] = z'$. This shows that η is onto.

Finally $z \in \text{Ker } \eta \Rightarrow \eta(z) = 0 \Rightarrow \dfrac{\sigma_2(x)}{\sigma_2(y)} = 0$ where $z = \dfrac{\sigma 1(x)}{\sigma 1(y)}$.

$$\Rightarrow \sigma_2(x) = 0 \Rightarrow x = 0 \text{ as } \sigma_2 \text{ is 1–1}$$

$$\Rightarrow \sigma_1(x) = 0 \Rightarrow z = \frac{\sigma 1(x)}{\sigma 1(y)} = 0.$$

So that Ker $\eta = (0)$ and η is 1–1 mapping. Hence η is an isomorphism of F_1 onto F_2.

NOTES

As by definition of η, for any $x \in D$, $\eta[\sigma_1(x)] = \sigma_2(x)$ we get $\eta\sigma_1 = \sigma_2$. This completes the proof.

Theorem 4 If a field K contains a non-zero integral domain D then K contains a field of quotients of D.

Proof Let $F = \left\{\frac{a}{b} \mid a, b \in D, b \neq 0\right\}$. (Note that by $\frac{a}{b}$ we mean ab^{-1}). Since D is non-zero, $\exists\ a(\neq 0) \in D$. Then $1 = \frac{a}{a} \in F$. Now for any $x = \frac{a}{b}, y = \frac{c}{d}, x - y = \frac{ad - bc}{bd} \in F$ and $xy = \frac{ac}{bd} \in F$. Thus F is a subring of K containting 1. Now if $x \neq 0$ then $a \neq 0$ and $x' = \frac{b}{a} \in F$ such that $xx' = \frac{a}{b}\frac{b}{a} = 1$. Hence $x^{-1} = x' \in F$. This proves that F is a field.

Given $z(\neq 0) \in D$ we can write $z = za / a$ (under, identification, as remarked earlier) and $(za)/a \in F$. Thus we have $D \subseteq F$. From the definition it is clear that F is the field of quotients of D contained in K. This proves the theorem.

11.3 EUCLIDEAN RINGS

Definition: An integral domain R is called a *Euclidean domain* (or a Euclidean ring) if for all $a \in R$, $a \neq 0$ there is defined a non –ve integer $d(a)$ s.t.,

(i) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $d(a) \leq d(ab)$

(ii) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $\exists$ t and r in R s.t.,

$$a = tb + r$$

where either $r = 0$ or $d(r) < d(b)$.

Example 1: Consider the integral domain $< \mathbf{Z}, +, . >$ of integers. For any $0 \neq a \in \mathbf{Z}$, define $d(a) = |a|$, then $d(a)$ is non –ve integer.

Again, let $a, b \in \mathbf{Z}$ be any elements s.t., $a \neq 0$, $b \neq 0$

then $d(a) = |a|$

$d(ab) = |ab| = |a|\,|b|$

thus $d(a) \leq d(ab)$ as $|a| \leq |a|\,|b|$

Again let $a, b \in \mathbf{Z}$ $(a, b \neq 0)$

NOTES

Suppose $b > 0$, then it is possible to write

$$a = tb + r \quad \text{where } 0 \le r < b$$

$$t, r \in \mathbf{Z}$$

If $r \neq 0$ then $r < b \Rightarrow |r| < |b|$

$$\Rightarrow d(r) < d(b)$$

If $b < 0$ then $(-b) > 0, \therefore \exists\ t, r \in \mathbf{Z}$ s.t.,

$$a = (-b)t + r \quad \text{where } 0 \le r < -b$$

$$a = (-t)\, b + r$$

and if $r \neq 0$, $r < -b \Rightarrow |r| < |b|$

$$\Rightarrow d(r) < d(b)$$

Hence $< \mathbf{Z}, +, . >$ is a Euclidean domain.

Remarks: (*i*) When we say, in the definition, that $\exists$ a non –ve integer $d(a)$ for any $0 \neq a$, we mean, $\exists$ a function d from $R - \{0\}$ to $\mathbf{Z}^+ \cup \{0\}$ where $\mathbf{Z}^+$ is set of +ve integers. This function d is called Euclidean valuation on R. Also the last condition in the definition is called *Euclidean algorithm*.

(*ii*) We can show that the t and r mentioned in the last (Euclidean algorithm) condition in the definition of Euclidean domain are uniquely determined iff

$$d(a + b) \le \text{Max. } \{d(a), d(b)\}.$$

Let $d(a + b) \le \text{Max. } \{d(a), d(b)\}$ and

Suppose $a = tb + r = t_1 b + r_1$

Let $r_1 - r \neq 0$, then $b(t - t_1) = r_1 - r \neq 0$, and so $t - t_1 \neq 0$

Now $d(b) \le d(b(t - t_1))$

$= d(r_1 - r)$

$\le \text{Max. } \{d(r_1), d(-r)\}$ (given condition)

$= \text{Max. } \{d(r_1), d(-r)\}$

$< d(b)$ which is not possible.

Thus $r_1 - r = 0 \Rightarrow b(t - t_1) = 0$

or $t - t_1 = 0$ as $b \neq 0$

$\Rightarrow$ $t = t_1$ and $r = r_1$

Conversely, let t, r be uniquely determined and suppose

$$d(a + b) > \text{Max. } \{d(a), d(b)\} \text{ for some } a, b \text{ (non zero) in } R.$$

Now $b = 0(a + b) + b = 1\ .\ (a + b) - a$

Also $d(-a) = d(a) < d(a + b)$

and $d(b) < d(a + b)$

NOTES

Thus for $b, 1 \in R, \exists\ t = 0, r = b$ or $t_1 = 1, r_1 = -a$ s.t., $b = t.1 + r$, $b = t_1 \cdot 1 + r_1$

where $r \neq r_1$ (as $a + b \neq 0$) $t \neq t_1$, a contradiction to the uniqueness.

Hence $d(a + b) \leq$ Max. $(d(a), d(b))$. Note that a Euclidean domain contains unity.

Theorem 5 *Let R be a Euclidean domain and let A be an ideal of R, then* $\exists$ $a_o \in A$ *s.t.*, $A = \{a_o x \mid x \in R\}$.

Proof: If $A = \{0\}$, we can take $a_o = 0$.

Suppose $A \neq \{0\}$, then $\exists$ at least one $0 \neq a \in A$.

Let $a_o \in A$ be such that $d(a_o)$ is minimal. [Existence is ensured by the well ordering principle which states that every non empty subset of non –ve integers has least element.]

We claim A is generated by this a_o.

Let $a \in A, a \neq 0$ then by definition, $\exists\ t, r \in R$, s.t.,

$$a = a_o t + r \quad \text{where either } r = 0 \text{ or } d(r) < d(a_o)$$

Suppose $r \neq 0$

Then $a_o \in A, t \in R \Rightarrow ta_o \in A$

$\therefore$ $a \in A, ta_o \in A \Rightarrow a - ta_o \in A$

$$\Rightarrow r \in A$$

But $d(a_o)$ is the smallest d-value in A and $d(r) < d(a_o)$, which leads to a contradiction. Hence $r = 0$

$$\Rightarrow a = ta_o$$

Thus any $a \in A$ can be put in the form ta_o

$$\Rightarrow A \subseteq \{a_o x \mid x \in R\}$$

But $\{a_o x \mid x \in R\} \subseteq A$ as $a_o \in A \Rightarrow xa_o \in A$ for all $x \in R$

Hence $A = \{a_o x \mid x \in R\}$

which proves the theorem.

Definition: Such an ideal A which contains multiples of an element a_o, including a_o of R is called a *Principal Ideal* of R, generated by a_o. We denote this by $A = (a_o)$.

In other words, the smallest ideal of R which contains a_o is called Principal Ideal generated by a_o.

In view of this definition the previous theorem will read as

Theorem 6: *Every ideal in a Euclidean domain is a principal ideal.*

Cor.: A Euclidean domain possesses unity.

NOTES

Proof: Let R be a Euclidean domain then R is its own ideal and, therefore, R is generated by some element r_o of R.

Thus each element of R is a multiple of r_o.

In particular r_o is a multiple of r_o

i.e., $r_o = r_o k$ for some $k \in R$

Now if $a \in R$ is any element then as $R = (r_o)$

$$a = xr_o \text{ for some } x$$

hence $ak = (xr_o)\, k = x(r_o k) = xr_o = a$

i.e., k is unity of R.

Definition: An integral domain R with unity is called a *Principal Ideal Domain* (PID) if every ideal of R is a principal ideal.

In fact, if R happens to be a commutative ring with unity with above condition, we call it a principal ideal ring.

In view of the previous theorem and cor., we get

Theorem 6: *A Euclidean domain is a PID.*

In particular thus, the ring $< \mathbf{Z}, +, \cdot >$ of integers is a PID. This result follows independently if we recall that every ideal in $< \mathbf{Z}, +, \cdot >$ is a principal ideal.

Remarks: (*i*) A field F is always a PID as it has only two ideals F and $\{0\}$. F is generated by 1 and $\{0\}$ by 0.

(*ii*) One can show that there exist PIDs which are not Euclidean domains. In particular, $\mathbf{Z}[\sqrt{-19}] = \{a + \sqrt{-19}\, b \mid a, b \in \mathbf{Z}\}$ where a, b are both odd or both even, is a PID but not a Euclidean domain.

Problem 1: *Show that in a PID every non-zero prime ideal is maximal.*

Solution: Let $P = (p)$, $p \neq 0$, be a non zero prime ideal in a PID R.

Suppose $P \subseteq Q = (q) \subseteq R$

Then $p \in P \subseteq Q = (q)$

$\Rightarrow p = qr$

$\Rightarrow qr \in P$

$\Rightarrow q \in P$ or $r \in P$

If $q \in P$ then all multiples of q are in $P \Rightarrow Q \subseteq P$

thus $Q = P$

If $r \in P$ then $r = pt \Rightarrow r = qrt$

$\Rightarrow r(1 - qt) = 0$

$\Rightarrow 1 = qt \quad (r \neq 0)$

But $q \in Q$, $t \in R \Rightarrow qt \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$

Note $r = 0$ would mean $p = q \cdot 0 \Rightarrow p = 0 \Rightarrow P = (0)$.

Problem 2: *Find all the prime ideals of* $\frac{\mathbf{Z}_n}{(n)}$, $(n > 1)$ *and hence of* $\mathbf{Z}_n$.

NOTES

Solution: We know any ideal of R/N is of the type $\frac{A}{N}$, where A is an ideal of R, containing N.

Let $(n) = N$ and $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_r^{\alpha r}$, where p_i are distinct primes.

Let $\frac{A}{N}$ be any prime ideal of $\frac{\mathbf{Z}}{N}$, then A is an ideal of $\mathbf{Z}$. We show it is a prime ideal of $\mathbf{Z}$. Since A is an ideal of $\mathbf{Z}$, it is of the type $A = (a)$. Suppose A is not a prime ideal of $\mathbf{Z}$. Then $\exists\ x, y \in \mathbf{Z}$, s.t., $xy \in A$ but x and y are not in A.

Now $xy \in A \Rightarrow Nxy \in A/N \Rightarrow NxNy \in A/N$

$\Rightarrow Nx$ or $Ny \in A/N$ as A/N is prime ideal

$\Rightarrow x$ or y is in A, a contradiction.

Hence $A = (a)$ is a prime ideal and thus a is a prime. Also

$(n) \subseteq (a)$. Since $n \in (n) \subseteq (a)$ we find $a \mid n$.

But primes dividing n are $p_1, p_2, \ldots, p_r$

Thus $a = p_i$ for same i, $1 \le i \le r$

Hence if $A/(n)$ is any prime ideal of $\frac{\mathbf{Z}}{(n)}$ then it is of the type $\frac{(p_i)}{(n)}$ for some i, $1 \le i \le r$.

Conversely, any ideal of the type $\frac{(p_i)}{(n)}$, $1 \le i \le r$ will be a prime ideal of $\frac{\mathbf{Z}}{(n)}$ as $\frac{\mathbf{Z}/(n)}{(p_i)/(n)} \cong \frac{\mathbf{Z}}{(p_i)}$.

Since (p_i) is a prime ideal of $\mathbf{Z}$, $\frac{\mathbf{Z}}{(p_i)}$ is an integral domain.

Thus $\frac{\mathbf{Z}/(n)}{(p_i)/(n)}$ is an integral domain and hence $\frac{(p_i)}{(n)}$ are prime ideals of $\frac{\mathbf{Z}}{(n)}$, $1 \le i \le r$.

where p_i are all the primes dividing n.

We thus conclude that if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ then $\frac{(p_1)}{(n)}, \frac{(p_2)}{(n)}, \ldots, \frac{(p_r)}{(n)}$ are precisely the prime ideals of $\frac{\mathbf{Z}}{(n)}$.

NOTES

We've seen earlier that

$$\theta : \frac{\mathbf{Z}}{(n)} \to \mathbf{Z}_n \text{ s.t.,}$$

$$\theta(m + (n)) = m,\ 0 \le m < n$$

is an isomorphism.

Now if P is a prime ideal of $\frac{\mathbf{Z}}{(n)}$, then $\theta(P)$ is a prime ideal of $\mathbf{Z}_n$.

Since $\frac{(p_i)}{(n)}$ are all the prime ideals of $\frac{\mathbf{Z}}{(n)}$, their images under θ are the prime ideals of $\mathbf{Z}_n$ i.e., (p_1), (p_2) ,....., (p_r) are all the prime ideals of $\mathbf{Z}_n$.

Remarks: (*i*) In particular, prime ideal of $\mathbf{Z}_p$ where p is prime is $(p) = (0)$ as $p = 0$ in $\mathbf{Z}_p$. Recall, a field has no non-trivial ideals and $\mathbf{Z}_p$ is an ideal when p is prime.

(*ii*) Since a non zero ideal in $\mathbf{Z}$ is maximal iff it is prime, the above result can similarly be proved for maximal ideals.

Problem 3: *Show that* $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$*, the ring of Gaussian integers is a Euclidean domain.*

Solution: We know that $\mathbf{Z}[i]$ is an integral domain.

For any $0 \neq x \in \mathbf{Z}[i]$, where $x = a + ib$, define

$$d(x) = d(a + ib) = a^2 + b^2$$

Then as $x \neq 0$, either $a \neq 0$ or $b \neq 0$

thus $$d(a + ib) = a^2 + b^2 > 0$$

Let now $x, y \in \mathbf{Z}[i]$, s.t., $x \neq 0$, $y \neq 0$ and let $x = a + ib$, $y = c + id$.

Then
$$\begin{aligned} d(xy) &= d((a + ib)(c + id)) = d((ac - bd) + i(ad + bd)) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= d(x)\, d(y) \end{aligned} \quad \ldots(1)$$

Since $y \neq 0$, $d(y) \ge 1$ [$y \neq 0$ means c or d is non zero]

Thus $$d(xy) \ge d(x)$$

We now prove the last condition in the definition of a Euclidean domain.

Let $x, y \in \mathbf{Z}[i]$ be two members where x is an ordinary +ve integer n ($x = n + i0$) and $y = a + ib$

By Euclid's division algorithm,

$$a = un + r_1 \quad 0 \le r_1 < n$$
$$b = vn + r_2 \quad 0 \le r_2 < n$$

NOTES

Now either $r_1 \leq \frac{n}{2}$ or $r_1 > \frac{n}{2}$

if $r_1 > \frac{n}{2}$ then $-r_1 < -\frac{n}{2}$

$$\Rightarrow n - r_1 < n - \frac{n}{2} = \frac{n}{2}$$

Thus $a = un + r_1 = un + n - n + r_1$

$= n(u + 1) - (n - r_1)$

$= nq + k_1$ where $k_1 = -(n - r_1)$

$$| k_1 | = n - r_1 < \frac{n}{2}$$

Thus whether $r_1 \leq \frac{n}{2}$ or $\frac{n}{2} < r_1$

we can express

$$a = nq + k_1 \quad \text{where } | k_1 | \leq \frac{n}{2}$$

Similarly, $b = nq' + k_2$ where $| k_2 | \leq \frac{n}{2}$

i.e., $a + ib = n(q + iq') + (k_1 + ik_2)$

or $y = tn + r$ $[t = q + iq',\ r = k_1 + ik_2]$

where either $r = 0$ (k_1 & k_2 could be zero)

or $d(r) = d(k_1 + ik_2) = k_1^2 + k_2^2 \leq \frac{n^2}{4} + \frac{n^2}{4} < n^2 = d(n)$

Thus, under this particular case, the result is proved.

Let now $x, y \in \mathbf{Z}[i]$ be any two non zero members then $x\bar{x}$ is a +ve integer, say, n.

We apply the above result proved, to $y\bar{x}$ and n and find that

For $y\bar{x}$ and n, $\exists\ t, r \in \mathbf{Z}[i]$, s.t.,

$$y\bar{x} = tn + r$$

where either $r = 0$ or $d(r) < d(n)$

If $r = 0$ then $y\bar{x} = tn = tx\bar{x} \Rightarrow y = tx + 0$

If $d(r) < d(n)$ then $d(y\bar{x} - tn) < d(x\bar{x})$

$$\Rightarrow d(y\bar{x} - tx\bar{x}) < d(x)\ d(\bar{x}) \qquad \text{[using (1)]}$$

NOTES

$\Rightarrow d(\bar{x})\ d(y - tx) < d(x)\ d(\bar{x})$

$\Rightarrow d(y - tx) < d(x)\ \ [d(\bar{x}) > 0]$

Put $y - tx = r_o$ then $d(r_o) < d(x)$

So $y = tx + r_o$ where $d(r_o) < d(x)$

combining, we get

$y = tx + r_o$, where either $r_o = 0$ or $d(r_o) < d(x)$.

Hence the result is proved.

Problem 4: *Show that* $\boldsymbol{Z}[w] = \{a + bw \mid a, b \in \boldsymbol{Z}\}$ *is a Euclidean domain, where* $w = \frac{-1+\sqrt{3}i}{2}$ *and* $1 + w + w^2 = 0$.

Solution: Define $d(a + bw) = a^2 - ab + b^2 = |a + bw|^2$.

Now $d(a + bw) = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} > 0$, whenever $a + bw \neq 0$.

Let $0 \neq x, y \in \mathbf{Z}[w]$ and $x = a + wb$, $y = c + wd$. Then $d(xy) = d(x)\ d(y)$.

Consider $\frac{x}{y} = \frac{a+bw}{c+dw} = \frac{(a+bw)(c-dw)}{c^2 - cd + d^2}$

$= u + vw, \quad u, v \in \mathbf{Q}$

Choose, $r, s \in \mathbf{Z}$ such that $|r - u| \leq \frac{1}{2}$ and $|s - v| \leq \frac{1}{2}$.

Then $\frac{x}{y} = (r + sw) + t$, where $t = (u - r) + (v - s)w$.

Now $|t|^2 = (u - r)^2 - (u - r)(v - s) + (v - s)^2$

$\leq \frac{1}{4} - \frac{1}{4} + \frac{1}{4} < 1$

We can write

$x = (r + sw)y + ty$, where $r + sw \in \mathbf{Z}[w]$.

and $ty = x - (r + sw)y \in \mathbf{Z}[w]$

Also $d(ty) = |ty|^2 = |t|^2 |y|^2 = |t|^2 d(y) < d(y)$

Hence $\mathbf{Z}[w]$ is a Euclidean domain.

Theorem 8: *Let a, b be two non zero elements of a Euclidean domain R. If b is not a unit in R then* $d(a) < d(ab)$.

Proof: Let b be not a unit. Then for a, ab in $R\ \exists\ t, r \in R$ s.t.,

$a = tab + r$

where either $r = 0$ or $d(r) < d(ab)$

If $r = 0$, then $a = tab \Rightarrow a(1 - t\,b) = 0$

$\Rightarrow tb = 1$ or that b is a unit, which is not so.

Thus $r \neq 0$ and $d(r) < d(ab)$

Now $r = a - tab = a(1 - tb)$

Hence $d(a) \leq d(a(1 - tb)) = d(r) < d(ab)$.

Cor.: If a, b are non zero elements of a Euclidean domain R then $d(a) = d(ab)$ iff b is a unit.

If b is a unit then $\exists\ c$ s.t., $bc = 1$

Now $d(a) \leq d(ab) \leq d((ab)c) = d(a)$

$\Rightarrow d(a) = d(ab)$

Converse follows from above theorem.

Problem 5: *Show that an element x in a Euclidean domain is a unit if and only if* $d(x) = d(1)$.

Solution: Let $d(x) = d(1)$

Suppose x is not a unit, then by above theorem

$d(1) < d(1 \,.\, x)$ Taking $a = 1$, $b = x$

i.e., $d(1) < d(x)$

a contradiction

$\therefore\ x$ is a unit.

Conversely, let x be a unit in R, then $\exists\ y \in R$ s.t.,

$xy = 1$

Now $d(x) \leq d(xy)$ (by definition)

$\Rightarrow d(x) \leq d(1)$

Also $d(1) \leq d(1 \,.\, x)$

$\Rightarrow d(1) \leq d(x)$

Hence $d(x) = d(1)$.

Problem 6: *Show by an example that it is possible to find two elements a, b in a Euclidean domain such that* $d(a) = d(b)$ *but a, b are not associates.*

Solution: Consider $D = \{a + ib \mid a, b \in \mathbf{Z}\} = \mathbf{Z}[i]$, the ring of Gaussian integers

where $d(a + ib) = a^2 + b^2$

then D is a Euclidean domain.

Here $d(2 + i3) = 13 = d(2 - 3i)$

but $2 + 3i$ and $2 - 3i$, are not associates.

NOTES

Notice that units of D are $\pm 1, \pm i$ and thus an associate of $2 + 3i$ can be

$$(2 + 3i)1, (2 + 3i)(-1), (2 + 3i)i, (2 + 3i)(-i)$$

i.e., $\quad 2 + 3i, -2 - 3i, 2i - 3, 3 - 2i$

which are all different from $2 - 3i$.

Theorem 9: *Any two non zero elements a, b in a Euclidean domain R have a g.c.d. d and it is possible to write.*

$$d = \lambda a + \mu b \quad \textit{for some } \lambda, \mu \in R$$

Proof: Let $A = \{ra + sb \mid r, s \in R\}$

then A is an ideal of R as

$$0 = 0.\ a + 0.\ b \in A \ \Rightarrow A \neq \varphi$$

Let $\quad x, y \in A$

$\Rightarrow \quad x = r_1 a + s_1 b,\ \ y = r_2 a + s_2 b$

$r_1, r_2, s_1, s_2 \in R$

Thus $\quad x - y = (r_1 - r_2)a + (s_1 - s_2)b \in A$

Again $\ x \in A, r \in R, x = r_1 a + s_1 b$

$\Rightarrow \ rx = r(r_1 a + s_1 b) = (rr_1)a + (rs_1)b \in A$

showing that A is an ideal of R.

Since a Euclidean domain is a PID, A will be generated by some element, say, d.

We claim d = g.c.d.(a, b)

Now $d \in A \Rightarrow d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Again since $\quad a = 1.a + 0.\ b \in A$

$$b = 0\ .\ a + 1\ .\ b \in A$$

(Note R being a Euclidean domain has unity)

So $a \in A,\ A = (d) \Rightarrow\ a = \alpha d \quad$ for some $\alpha \in R$

$b \in A,\ A = (d) \Rightarrow\ b = \beta d \quad$ for some $\beta \in R$

$$\Rightarrow\ d \mid a \text{ and } d \mid b$$

Again, if $c \mid a$ and $c \mid b$

then $\quad c \mid \lambda a,\ \ c \mid \mu b$

$$\Rightarrow\ c \mid \lambda a + \mu b$$

i.e. $\quad c \mid d \ \Rightarrow\ d$ = g.c.d.(a, b).

Remarks: (*i*) The theorem clearly then holds in a PID, and the next result that we prove in a PID holds in a Euclidean domain.

(*ii*) Similarly one can show that any finite number of non-zero elements $a_1, a_2 ..., a_n$ in a Euclidean domain (PID) R have a g.c.d. which can be put in the form $\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n, \lambda_i \in R$.

Theorem 10: *Any two non zero elements a, b in a PID R have a least common multiple.*

Proof: Let $A = (a)$, $B = (b)$ be the ideals generated by a and b.

Then $A \cap B$ is an ideal of *PID R*. Suppose it is generated by l.

We show $l = \text{l.c.m.}(a, b)$

Now $A \cap B \subseteq A$, $A \cap B \subseteq B$

$l \in (l) \Rightarrow l \in (a) \Rightarrow l = au$ for some u

$l \in (l) \Rightarrow l \in (b) \Rightarrow l = bv$ for some v

$\Rightarrow a \mid l$ and $b \mid l$

Again, suppose $a \mid x$ and $b \mid x$

$\Rightarrow x = a\alpha,\ x = b\beta \quad \alpha, \beta \in R$

$\Rightarrow x \in (a), x \in (b)$

$\Rightarrow x \in A \cap B = (l)$

$\Rightarrow x = kl \ \Rightarrow l \mid x$

Hence $l = \text{l.c.m.}(a, b)$.

Definition: In an integral domain R with unity, a, b (non zero) are said to be *co-prime* or *relatively prime*, if g.c.d.(a, b) is a unit in R.

Problem 7: *Two elements a, b in an integral domain with unity are co-prime iff*

g.c.d.$(a, b) = 1$.

Solution: Let a, b be co-prime. By theorem 1 any associate of a g.c.d. is a g.c.d.

Since 1 is associate of any unit

1 will be an associate of $d = \text{g.c.d.}(a, b) = $ a unit

$\Rightarrow 1 = \text{g.c.d.}(a, b)$

Converse is obvious as 1 is a unit.

Prime and Irreducible Elements

Definitions: Let R be a commutative ring with unity. An element $p \in R$ is called a *prime element* if

(*i*) $p \neq 0$, p is not a unit.

(*ii*) For any $a, b \in R$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Let R be a commutative ring with unity. An element $p \in R$ is called an *irreducible element* if

(*i*) $p \neq 0$, p is not a unit.

(*ii*) whenever $p = ab$ then one of a or b must be a unit. (In other words, p has no proper factors.)

NOTES

Example 2: In the ring $< \mathbf{Z}, +, \cdot >$ of integers, every prime number is a prime element as well as irreducible element.

Example 3: Cosider the ring

$$\mathbf{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbf{Z}\}$$

under the operations defined by

$$(a + \sqrt{-5}b) + (c + \sqrt{-5}d) = (a + c) + \sqrt{-5}(b + d)$$

$$(a + \sqrt{-5}b) \,.\, (c + \sqrt{-5}d) = (ac - 5bd) + \sqrt{-5}(ad + bc)$$

(*i*) We show $\sqrt{-5}$ is a prime element.

$\sqrt{-5} \neq 0$, it is also not a unit as, if it were a unit then $\exists\ a + \sqrt{-5}b$, s.t.,

$$\sqrt{-5}(a + \sqrt{-5}b) = 1$$

$\Rightarrow \sqrt{-5} = 1 + 5b$, which is not possible as R.H.S. is an integer whereas L.H.S. is not an integer.

Suppose now $\sqrt{-5}$ divides $(a + \sqrt{-5}b)(c + \sqrt{-5}d)$,

then $\exists\ (x + \sqrt{-5}y)$ s.t.,

$$\sqrt{-5}(x + \sqrt{-5}y) = (a + \sqrt{-5}b)\ (c + \sqrt{-5}d)$$

which on comparison gives,

$$-5y = ac - 5bd$$

$$5(bd - y) = ac \Rightarrow 5 \mid ac$$

But 5 being a prime number

either $5 \mid a$ or $5 \mid c$.

If $5 \mid a$ then $(\sqrt{-5})(\sqrt{-5}) \mid a$

$$\Rightarrow \sqrt{-5} \mid a$$

$$\Rightarrow \sqrt{-5} \mid a + b\sqrt{-5}$$

Similarly, if $5 \mid c$ then $\sqrt{-5} \mid c + \sqrt{-5}d$

Hence $\sqrt{-5}$ is a prime element.

(*ii*) We show further that 3 is an irreducible element which is not prime.

Suppose $3 = (a + \sqrt{-5}b)\ (c + \sqrt{-5}d)$, $a, b, c, d \in \mathbf{Z}$

Taking conjugates, we get

$$\overline{3} = (a - \sqrt{-5}b)(c - \sqrt{-5}d)$$

Thus $3.\overline{3} = (a^2 + 5b^2)(c^2 + 5d^2)$

i.e., $9 = (a^2 + 5b^2)(c^2 + 5d^2)$

$\Rightarrow$ $a^2 + 5b^2 = 1, 3$ or 9

Now $a^2 + 5b^2 = 3$ is not possible as $a, b \in \mathbf{Z}$

If $a^2 + 5b^2 = 1$ then $a = \pm 1$ and $b = 0$

If $a^2 + 5b^2 = 9$ then $a^2 + 5d^2 = 1$, giving $c = \pm 1$ and $d = 0$

Thus, if $a^2 + 5b^2 = 1$ then $a + \sqrt{-5}b = \pm 1 =$ unit

and if $a^2 + 5b^2 = 9$ then $c + \sqrt{-5}d = \pm 1 =$ unit

Hence 3 is an irreducible element of $\mathbf{Z}[\sqrt{-5}]$.

Now $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ and thus

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$$

We show it does not divide any one of these. Suppose $3 \mid (2 + \sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$

Then $(2 + \sqrt{-5}) = 3(a + \sqrt{-5}b)$ $a, b \in \mathbf{Z}$

$\Rightarrow 2 - \sqrt{-5} = 3(a - \sqrt{-5}b)$

$\Rightarrow 9 = 9(a^2 + 5b^2)$

$\Rightarrow 1 = a^2 + 5b^2 \Rightarrow a = \pm 1, b = 0$

$\Rightarrow 2 + \sqrt{-5} = \pm 3$ which is not possible

Thus $3 \nmid (2 + \sqrt{-5})$. Similarly $3 \nmid (2 - \sqrt{-5})$

Hence 3 is not a prime element of $\mathbf{Z}[\sqrt{-5}]$.

Theorem 11: *In a PID an element is prime if and only if it is irreducible.*

Proof: Let D be a PID and let $p \in D$ be a prime element. We need prove only that if $p = ab$, then a or b is a unit.

So let $p = ab$ then $p \mid ab$

$\Rightarrow$ $p \mid a$ or $p \mid b$ (p is prime)

If $p \mid a$ then $a = px$ for some x

So $p = ab = (px)b$

$\Rightarrow p(1 - xb) = 0$

$\Rightarrow 1 - xb = 0$ as $p \neq 0$

$\Rightarrow xb = 1$ $\Rightarrow b$ is a unit.

Similarly, if $p \mid b$ then a will be a unit.

NOTES

Conversely, let p be irreducible element and suppose $p \mid ab$. We show either $p \mid a$ or $p \mid b$.

If $p \mid a$, we have nothing to prove.

Suppose $p \nmid a$

Since p, a are elements of a PID they have a g.c.d., say, d.

We show d is a unit.

Now $d \mid p$ and $d \mid a$

$\Rightarrow \quad \exists\ u, v$ s.t., $p = du$, $a = dv$

If d is not a unit then as p is irreducible and $p = du$, u will be a unit

$\Rightarrow \quad u^{-1}$ exists

$\Rightarrow \quad pu^{-1} = d$

$\therefore \quad a = pu^{-1}v \Rightarrow p \mid a$ which is not so.

Thus d is a unit.

Again, we know that d can be expressed as

$$d = \lambda a + \mu p$$

which gives $dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p$

$$\Rightarrow\ b \,.\, 1 = \lambda d^{-1}ab + \mu d^{-1}bp$$

But $p \mid ab,\ p \mid \mu d^{-1}\ bp$

$\therefore \quad p \mid (ab\lambda d^{-1} + \mu d^{-1}bp)$

$\Rightarrow\ p \mid b$

Hence the result follows.

Cor.: In an integral domain with unity, every prime element is irreducible. The converse is not true.

Remark: Combining the results of Example 3 and the above theorem, we can say $\mathbf{Z}[\sqrt{-5}]$ is not a PID.

Example 4: Consider the ring $Z_6 = \{0, 1, 2, 3, 4, 5\}$ mod 6.

2 is a prime element in $\mathbf{Z}_6$ but is not irreducible.

2 is, of course, non zero, non unit.

Suppose $2 \mid a \otimes b$

Since $ab = 6q + a \otimes b$ for some q

and as $2 \mid 6q$, $2 \mid a \otimes b$, we find $2 \mid ab$

$$\Rightarrow\ 2 \mid a \quad \text{or} \quad 2 \mid b$$

$\Rightarrow\ 2 \mid a$ or $2 \mid b$ in $\mathbf{Z}_6$

Hence 2 is a prime element.

Again, as $2 \otimes 4 = 2$, where neither 2 nor 4 is a unit, we find 2 is not irreducible. (Note, $\mathbf{Z}_6$ is not an integral domain.)

Check Your Progress

1. Write two procedures of embedding one ring into another.
2. Give an example of a Euclidean ring.
3. What is a Principal ideal?
4. What is a Principal Ideal domain?

11.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. (i) Embedding of a ring in a ring with unity. (ii) Embedding of a domain in a field.
2. $<Z, +, .>$ Integral domain of integers is a Euclidean ring.
3. An ideal A which contains multiples of an element a_o, including a_o of R is called a *Principal Ideal* of R, generated by a_o. We denote this by $A = (a_o)$.
4. An integral domain R with unity is called a Principal Ideal Domain (PID) if every ideal of R is a principal ideal.

11.5 SUMMARY

- Every ring can be embedded in a ring with a unity.
- Let D be an integral domain with more than one element, than a field of quotients of D is a pair (F, σ) where F is a field and σ is a monomorphism of D into F such that every $z \in F$ is expressible as $\sigma(x)/\sigma(y)$ for some $x, y \in D$ with $y \neq 0$.
- An integral domain R is called a *Euclidean domain* (or a Euclidean ring) if for all $a \in R$, $a \neq 0$ there is defined a non –ve integer $d(a)$ s.t.,

  (i) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $d(a) \leq d(ab)$

  (*ii*) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $\exists$ t and r in R s.t., $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.
- Let R be a Euclidean domain and let A be an ideal of R, *then* $\exists$ $a_o \in A$ s.t., $A = \{a_o x \mid x \in R\}$. An ideal A which contains multiples of an element a_o, including a_o of R is called a *Principal Ideal* of R, generated by a_o. We denote this by $A = (a_o)$.

- An integral domain R with unity is called a Principal Ideal Domain (PID) if every ideal of R is a principal ideal.
- In an integral domain R with unity, a, b (non zero) are said to be *co-prime* or *relatively prime*, if g.c.d.(a, b) is a unit in R.

11.6 KEY WORDS

- **Embedding:** an embedding is one instance of some mathematical structure contained within another instance, such as a group that is a subgroup.
- **Domain:** domain of a function is the set of "input" or argument values for which the function is defined. That is, the function provides an "output" or value for each member of the domain.
- **Field:** a field is an algebraic structure with notions of addition, subtraction, multiplication, and division, satisfying certain axioms. The most commonly used fields are the field of real numbers, the field of complex numbers, and the field of rational numbers.

11.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Show that every field is a Euclidean ring.
2. Write a short note on Principal ideal Domain.
3. Prove that any two non-zero elements a, b in a *PID* R have a least common multiple.
4. Find all units of $Z[\sqrt{-3}]$.

Long Answer Questions

1. If $R = \{a + b\sqrt{3} \mid a, b \in Z\}$. Show that R is an integral domain with unity. Obtain its field of quotients.
2. Determine the fields of quotients of the integral domain of complex numbers $a + bi$ where $a, b \in Z$.
3. Give an example to show that non-isomorphic integral domain may have isomorphic fields of quotients.
4. Show that $Z[\sqrt{3}] = \{a + \sqrt{3b} \mid a, b \in Z\}$ is a Euclidean Ring.

11.8 FURTHER READINGS

Hungerford, Thomas W. 2003. *Algebra*. Berlin: Springer Science & Business Media.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Singh, Surjeet, Qazi Zameeruddin. 2005. *Modern Algebra*. NOIDA: Vikas Publishing House.

NOTES

NOTES

BLOCK - IV

EUCLIDEAN RING AND POLYNOMIAL RING

UNIT 12 A PARTICULAR EUCLIDEAN RING

Structure

12.0 INTRODUCTION

In this unit, you will know about a particular case of Euclidean domain. A Euclidean domain is an integral domain that can be endowed with a Euclidean function which allows a suitable generalization of the Euclidean division of the integers. The concept of polynomial rings is also discussed in this unit. A polynomial ring or polynomial algebra is a ring formed from the set of polynomials in one or more indeterminate with coefficients in another ring, often a field.

12.1 OBJECTIVES

After going through this unit, you will be able to:

- Know about a particular case of Euclidean ring
- Understand the concept of polynomial rings

12.2 A PARTICULAR EUCLIDEAN RING

Let $J[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. We call these the Gaussian integers. Our first objective is to exhibit $J[i]$ as a Euclidean ring. In order to do this we must first introduce a function $d(x)$ defined for every nonzero element in $J[i]$ which satisfies

1. $d(x)$ is a nonnegative integer for every $x \neq 0 \in J[i]$.

2. $d(x) \leq d(xy)$ for every $y \neq 0$ in $J[i]$.
3. Given , $\alpha, \beta \in J[i]$ there exist $q, r \in J[i]$ such that $\alpha = \alpha\beta + r$ where $r = 0$ or $d(r) < d(\beta)$.

NOTES

Put $d(a+bi) = |a+bi| = \sqrt{a^2+b^2}$.

Condition (1) is obvious. Condition (2) is also easy, since

$$d(\alpha\beta) = |\alpha\beta| = |\alpha||\beta| = |\alpha|d(\beta)$$

which is $\leq d(\beta)$, since $|\alpha| = \sqrt{a^2+b^2} \geq 1$, for a, b are integer numbers and $\alpha = 0$.

Condition (3) is more complicated. So let $\alpha = a + bi$ and $\beta = c + di \neq 0$. Then in $\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$ we get

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{ac-bd}{c^2+d^2} + \frac{ad+bc}{c^2+d^2}i = x + yi.$$

This is the exact quotient in $\mathbb{Q}[i]$, but what is the best we can do in $\mathbb{Z}[i]$? The nearest we can get is the number $k = m + ni$, where m is the integer nearest x, and n the integer nearest y.

Note that

$$|x-m| \leq \frac{1}{2} \quad \text{and} \quad |y-n| \leq \frac{1}{2}.$$

Now

$$\frac{\alpha}{\beta} = x + yi = m + ni + (x-m) + (y-n)i$$

and multiplying by β we get

$$\alpha = (m+ni)\beta + [(x-m) + (y-n)i]\beta.$$

Put as quotient $q = m + ni \in J[i]$. As reminder we then would have

$$r = [(x-m) + (y-n)i]\beta = \alpha - q\beta \in J[i].$$

We now compute

$$\begin{aligned} d(r) &= d([(x-m) + (y-n)i]\beta) \\ &= |[(x-m) + (y-n)i]\beta| \\ &= |[(x-m) + (y-n)i]||\beta| \\ &= \sqrt{(x-m)^2 + (y-n)^2}|\beta| \leq \frac{1}{\sqrt{2}}|\beta| < d(\beta) \end{aligned}$$

and see that condition (3) is satisfied.

NOTES

LEMMA 1: Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then p can be written as the sum of squares of two integers, that is, there exist integers a and b such that $p = a^2 + b^2$.

Proof: The ring of integers is a subring of $J[i]$. Suppose that the integer p is also a prime element of $J[i]$. Since

$$cp = x^2 + y^2 = (x + yi)(x - yi),$$

we have

$$p \mid (x + yi) \quad \text{or} \quad p \mid (x - yi) \quad \text{in} \quad J[i].$$

But if $p \mid (x + yi)$ then $x + yi = p(u + vi)$ which would say that $x = pu$ and $y = pv$ so that p also would divide $x - yi$. But then

$$p^2 \mid (x + yi)(x - yi) = cp$$

from which we would conclude that $p \mid c$ contrary to assumption. Similarly if $p \mid (x - yi)$. Thus p is not a prime element in $J[i]$. In consequence of this,

$$p = (a + bi)(g + di) \qquad ...(1)$$

where $a + bi$ and $g + di$ are in $J[i]$ and where neither $a + bi$ nor $g + di$ is a unit in $J[i]$. But this means that neither $a^2 + b^2 = 1$ nor $g^2 + d^2 = 1$. From (1) it follows that

$$p = (a + bi)(g + di)$$

Thus

$$p^2 = (a + bi)(g + di)(a - bi)(g - di) = (a^2 + b^2)(g^2 + d^2).$$

Therefore $(a^2 + b^2) \mid p^2$ so $a^2 + b^2 = 1$, p or p^2. But $a^2 + b^2 \neq = 1$ since $a + bi$ is not a unit in $J[i]$; $a^2 + b^2 \neq = p^2$, otherwise $g^2 + d^2 = 1$, contrary to the fact that $g + di$ is not a unit in $J[i]$. Thus the only feasibility left is that $a^2 + b^2 = p$.

LEMMA 2: If p is a prime number of the form $4n + 1$, then we can solve the congruence $x^2 \equiv -1 \bmod p$.

Proof: Let

$$x = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}.$$

Since $p - 1 = 4n$, in this product there are an even number of terms, therefore

$$x = (-1) \cdot (-2) \cdot (-3) \ldots \left(-\frac{p-1}{2}\right).$$

But $p - k \equiv -k \bmod p$, so that

$$\begin{aligned} x^2 &\equiv \left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)(-1) \cdot (-2) \cdot (-3) \ldots \left(-\frac{p-1}{2}\right) \\ &\equiv 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \ldots (p-1) \\ &\equiv (p-1)! \equiv -1 \mod p \end{aligned}$$

by Wilson's theorem.

NOTES

Theorem 1 (Fermat): If p is a prime number of the form $4n + 1$, then $p = a^2 + b^2$ for some integers a, b.

Proof: By Lemma 2 there exists an x such that $x^2 \equiv -1 \bmod p$. The x can be chosen so that $0 \le x \le p - 1$ since we only need to use the remainder of x on division by p. We can restrict the size of x even further, namely to satisfy $|x| \le p/2$. For if $x > p/2$, then $y = p \le x$ satisfies $y^2 \le 1 \bmod p$ but $|y| \le p/2$. Thus we may assume that we have an integer x such that $|x| \le p/2$ and $x^2 + 1$ is a multiple of p, say cp.

Now

$$cp = x^2 + 1 \le p^2/4 + 1 < p^2,$$

hence $c < p$ and so $p \chi c$. From this by Lemma 1 it follows that $p = a^2 + b^2$ for some integers

12.3 POLYNOMIAL RINGS

Consider any ring S and a subring R of S. Let $u \in S$ be such that $ru = ur$ for every $r \in R$. Let $R[u]$ denote the set of all elements of S of the form

$$a_0 + a_1u + a_2u^2 + a_nu^n,$$

where $a_i \in R$ for every $i = 0, 1, 2, ..., n$ and n is any positive interger. Using the fact that $au^k = u^ka$ for every $a \in R$ and every positive integer k, one can immediately see that $R[u]$ is non empty and closed under subtraction and multiplication. That is, $R[u]$ is a subring of S. Further if

$$a_0 + a_1u + a_2u^2 + ... + a_nu^n = 0$$

for $a_i \in R(i = 0,1,2,....,n)$ such that at least one of a_i is non-zero then we say that u is *algebraic* over R. However if for every choice of $a_0, a_1, a_2,...,a_n$ (of elements in R) $a_0 + a_1u + a_2u^n + ... + a_nu^n \ne 0$ whenever at least one of $a_i \ne 0$ $(i > 0)$ then u is said to be *transcendental* over R. For example let us consider R and Q. Now $\sqrt{2} \in \mathbf{R}$, by using the fact that $(\sqrt{2})^2 = 2 \in \mathbf{Q}$, we can see that each member of $\mathbf{Q}[\sqrt{2}]$ is of the type $a + b\sqrt{2},\ a, b \in \mathbf{Q}$. Further as $2 - 1(\sqrt{2})^2 = 0$, we see that $\sqrt{2}$ is algebraic over $\mathbf{Q}$. Consider π, we know that π is not an algebraic number i.e. it is not the root of any polynomial equation with coefficients as rational numbers. Thus π is transcendental over $\mathbf{Q}$.

Given any member

$$a_0 + a_1\pi + a_2\pi^2 + ... + a_n\pi^n \in \mathbf{Q}[\pi]$$

we get an infinite sequence $(a_0, a_1, a_2,....,....,a_n, 0, 0,....,...)$ of elements of $\mathbf{Q}$ in which all terms after nth stage are equal to zero. Conversely given any infinite sequence

$$(b_0, b_1, ..., ..., b_m, 0, 0, ..., ...)$$

of elements of **Q** in which all except finite number of terms are zero we can find a non-negative integer m such that $b_i = 0 \forall i \geq m+1$. this sequence determines an element

NOTES

$$b_0 + b_1\pi + b_2\pi^2 + ... + b_m\pi^m \in \mathbf{Q}[\pi].$$

Further notice that any two elements

$$c_0 + c_1\pi + c_2\pi^2 + ... \text{and } d_0 + d_1\pi + d_2\pi^2 + ...$$

with, $c_i, d_i \in \mathbf{Q}$, are equal if any only if $c_i = d_i \forall i,$ since otherwise we shall get π to be algebraic over **Q**. Thus each member $a_0 + a_1\pi + a_2\pi^2 + ... + a_n\pi^n$ is uniquely determined by the corresponding infinite sequence $(a_0, a_1, a_2, ..0, 0, ..., ...)$ of elements of **Q**. Again we turn to the general case of *R* and *S*. In that case if $u \in S$ is transcendental over *R* then each member $a_0 + a_1u + ... + a_iu^n$, $a_i \in R$ is uniquely determined by the infinite sequence $(a_0, a_1, a_2, ..., ..., a_n, 0, 0, ..., ...)$ of elements of **R**.

Let us take a look on the problem from different angle. Suppose *R* is a ring. For the sake of convenience let us suppose that R has unity $1(\neq 0)$. The problem is 'does there exist a ring *S* containing *R* such tat *S* contains an element *x* which commutes with every element of *R* and *x* is transcendental over *R*?' It is this problem we take up firstly in this section and give its answer in affirmative. We take clue from our earlier observation that if *x* is transcendentl over *R* then any member $a_0 + a_1x + a_2x_2 + ...+a_nx_n$ determines uniquely and is determined uniquely by the infinite sequence $(a_0, a_1, a_2, ..., ..., a_n, 0, 0, ..., ...)$ of elements of *R*. As we do not know for the time being, what this x will be—we prefer to define a polynomial over *R* as follows:

Definition: Any infinite sequence $(a_0, a_1, a_2, ..., ..., a_n, ..., ...)$ of elements of a ring R is said to a polynomial over *R* if all except finite number of its terms a_i are equal to zero.

In other words an infinite sequence $(a_0, a_1, a_2, ..., ..., a_n, ..., ...)$ of elements of a ring R is said to a polynomial over *R* is said to be a polynomial over *R* if there exists a non-negative integer n such that $a_i = 0 \forall i \geq n+1$.

Each member a_i of the polynomial $(a_0, a_1, a_2, ..., ...)$ is called its jth coefficient. Further a_0 is called the constant term and if *n* is the largert non-negative integer with $a_n \neq 0$ then a_n is called the leading coefficient of the polynomial.

Definition: *(Sum and product of two polynomials).*

Let $f = (a_0, a_1, a_2, ..., ...)$ and $g = (b_0, b_1, b_2, ..., ...)$ be any two polynomials over a ring *R* then their sum f + g and product fg are defined as under:

NOTES

$$f+g=(a_0+b_0,\ a_1+b_1, a_2+b_2,\ \ldots,\ldots$$
$$fg=(c_0+c_1,\ c_2,\ldots,\ldots) \quad \text{where } c_0=a_0b_0.$$
$$c_1=a_0b_1+a_1b_0,\ \ c_2=a_0b_2+a_1b_1+a_2b_0 \quad \text{and so on, in general}$$
$$c_k=a_0b_k+a_1b_{k-1}+\ldots+\ldots+\ldots+a_kb_0$$
$$=\sum_{i+j=k}a_ib_j \quad \text{for every } k\geq 0.$$

It remains to settle whether sum and product of two polynomials over R are polynomials over *R* or not. This is answered by the following more comprehensive theorem.

Theorem 2: The set T of all polynomials over a ring *R* is a ring under the addition and multiplication operation defined as follows:

$$\text{For all } f=(a_0,a_1,a_2,\ldots,\ldots), g=(b_0,b_1,b_2,\ldots,\ldots)\in T$$
$$f+g=(a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ldots,\ldots)$$
$$\text{and}\quad fg=(c_0,c_1,c_2,\ldots,\ldots)$$
$$\text{where}\quad c_k=\sum_{i+j=k}a_ib_j \ \text{ for every } k\leq 0.$$

Proof: Let a_n and b_m be coefficients of *f* and *g* respectively such that $a_i=0\vee i\geq n+1$ and $b_j=0\vee j\geq m+1$. If $s=max\ (m, n)$ then $a_t=b_t=0\vee s,$ so $a_t+b_t=0\vee t>s$, hence $f+g\in T$.

Again consider $k>m+n$, then if $i+j=k$ either $i>m$ or $j>n$ hence $a_ib_j=0$ for all *i* and *j* satisfying $i+j=k$ for $k>m+n$. This gives that $ck=0$ for all $k\geq m+n$, hence $fg\in T$.

Now as *R* is a ring it can be easily verified that $<T, +>$ is an Abelian group in which (0, 0, 0, ...,...) is the additive identity and for any $f=(a_0, a_1, a_2,...,...)\in T$, $f'=(-a_0,-a_1,-a_2,...,...)$ is the additive inverse of *f*. Clearly $f'\in T$. Finally item be easily checked that is distributive on left as well as on right over +. Hence $<T$, +,..> is a ring.

Theorem 3: Let T be a ring of polynomials over a ring *R* then $R'=\{(a,0,0,...,)\mid a\in R\}$ is a subring of T isomorphic to *R* under the mapping (*a*, 0, 0....,) $\rightarrow a$. Further if *R* has unity I then (1, 0, 0,...,...) is the unity of *T*.

Proof: Let $f: R\rightarrow T$ be defined by $f(a) = (a, 0, 0,....,...)\ \vee a\in R$. Then for all $a, b\in R$, $f(a+b) = (a+b, 0, 0,...,...) = (a, 0, 0,...,...) + (b, 0, 0,...,...) = f(a) + f(b)$ and $f(ab) = (ab, 0, 0,...,...) = (a, 0, 0,...,...)(b, 0, 0,...,...) = f(a)f(b)$. Also *f* is 1 – 1 since $f(a)=f(a)\Rightarrow(a,0,0,...,...)=(b,0,0,....,...)\Rightarrow a=b$.

NOTES

Hence $R \cong f(R) = R'$. This proves first part of the theorem.

Finally if R has unity 1 then $f(1) = (1, 0, 0,...,...) \in T$ and for all $(a_1, a_2, a_3,...,...) \in T$, $(a_1, a_2, a_3,...,...)$ $(1, 0, 0,...,...) = (a_1, a_2, a_3,...,...) = (1, 0, 0,...,...)$ $(a_1, a_2, a_3, ...,...)$. Hence $(1, 0, 0, ...,...)$ is the unity of T.

Remark: For each $a \in R$, let $\bar{a}$ denote the polynomial $(a, 0, 0,...,...)$. Further let R have unity 1 $(\neq 0)$.

Define $x = (0, 1, 0, 0,...,...)$ then $\bar{a}x = (a, 0, 0,...,...)(0, 1, 0, 0,...,...) = (0, a, 0, 0, ...,...) = (0, 1, 0, 0,...,...)$ $(a, 0, 0, ...,...) = x\ \bar{a}$ and so x commutes with every element of R' i.e. with every element of R if we identify each a with $\bar{a}$.

By applying the formula for multiplication of the polynomials one find that $x^2 = (0, 1, 0, 0, ...,...)$, $x^3 = (0, 0, 0, 1, 0, 0,....,.....)$. and so on, in general $x^n = (0, 0, 0,.....,.....,0, 1, 0,....,....)$ with 1 at $(n+1)$ the place. Further for any $a \in R$, $\bar{a}\ x^n = (0, 0, 0, ...,... a, 0,....,....)$. with a at $(n+1)$ the place.

Let $f = (a_0, a_1, a_2, ...,...)$ be any polynomial over R. As there exists a non-negative integer n such that $a_i = 0 \vee i \geq n+1$ we see that $= (a_0, a_1, a_2, ...,...., a_n, 0, 0, ...,....) = (a_0, 0, 0,....,...) + (0, \underbrace{a_1}_{(n+1)\text{th place}}, 0, 0,....,....) + (0, 0, \alpha a_2, 0,..,...) + ... +$

$.... + ... + (0, 0, ..., 0, a_n, 0, ...,...)\ \bar{a}_1 + \bar{a}_2 x^2 + ... + \bar{a}_n x^n$.

Further $f = 0$ if and only if $a_i = 0 \vee i$ gives $\bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + ... + \bar{a}_n x^n = 0$ if and only if each $a_i = 0$. As $R \cong R'$ under the mapping $a \to \bar{a}$ we identify R with R' and each $a \in R$ with the ploynomial $\bar{a}$. Then we get that R is a subring of T. Now $x \in T$ is such that $ax = xa \vee \in R$. Every member of T is of the form

$$f = a_0 + a_1 x + a_2 x^2 + ... + ... + a_n x^n$$

and $f = 0$ only when each $a_i = 0$. Consequently x is transcendental over R and $T = R[x]$. Thus we have found a ring T containing R such that T is a ring of polynomials in an element x over R and x is transcendental over R. We show that such ring T is unique to within isomorphism. For this we have.

Theorem 4: Let R be any, S and S' two overrings of R. Suppose that there exist $u \in S, u' \in S'$ such that u and u' commute with every element of R. Then $R[u] \cong R[u']$ under the mapping $f: R[u] \to R[u']$ defined by $f(a_0 + a_1 u + a_2 u^2 + ...) = a_0 + a_1 u' + a_2 (u')^2 + ...$ whenever u and u' are transcendental over R.

Proof: Firstly we show that f is well-defined.

$$a_0 + a_1 u + a_2 u^2 + ... = b_0 + b_1 u + b_2 u^2 + ...$$

then $(a_0 - b_0) + (a_1 - b_1)u + (a_2 - b_2)u^2 + ... = 0$

$\Rightarrow \quad a_0 = b_0,\ a_1 = b_1, a_2 = b_2, \ldots..$ as u is transcendental over R.

This in turn implies $a_0 + a_1u' + a_2(u'^2) + ... = b_0 + b_1u' + b_2(u'^2) + ...$ hence $f(a_0 + a_1u' + a_2u^2 + ...) = f(b_0 + b_1u + b_2u^2 + ...)$.

Consequently f is well-defined.

Now let $a_1 + a_1u + a_2u^2 + ..., b_0 + b_1u + b_2u^2 + ... \in R[u]$

Then $f[(a_0 + a_1u + a_2u^2 + ...) + (b_0 + b_1u + b_2u^2 + ...)]$

$$= f[(a_0 + b_0) + (a_1 + b_1)u + (a_2 + b_1u + b_2u^2 + ...)]$$
$$= (a_0 + b_0) + (a_1 + b_1)u' + (a_2 + b_2)(u') + ...]$$
$$= [a_0 + a_1u' + a_2(u')^2 + ...] + [b_0 + b_1u' + b_2(u')^2 + ...]$$
$$= f(a_0 + a_1u + a_2u^2 + ...)(b_0 + b_1u + b_2u^2 + ...]$$

Further $f[(a_0 + a_1u + a_2u^2 + ...)(b_0 + b_1u + b_2u^2 + ...)]$

$$= f[a_0b_0 + (a_0b_1 + a_1b_0)u + (a_0b_2 + a_1b_1 + a_2b_0)u^2 + ...]$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)u' + (a_0b_2 + a_1b_1 + a_2b_0) \quad (u')^2$$
$$= [a_0 + a_1u' + a_2(u')^2 + ...][b_0 + b_1u' + b_2(u')^2 + ...]$$
$$= f(a_0 + a_1u + a_2u^2 + ...) f(b_0 + b_1u + b_2u^2 + ...)$$

Thus f is a homomorphism.

Again $f(a_0 + a_1u + a_2u^2 + ...) = f(b_0 + b_1u + b_2u^2 + ...)$

$$\Rightarrow \quad a_0 + a_1(u')^2 + a_2(u') + \ldots = b_0 + b_1u' + b_2(u')^2 +$$
$$\Rightarrow \quad (a_0 - b_0) + (a_1 - b_1)u' + (a_2 - b_2) \quad (u')^2 + \ldots = 0$$
$$\Rightarrow \quad a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \ldots, \quad \text{as } u' \text{ is transcendental over } R.$$
$$\Rightarrow \quad a_0 + a_1u + a_2u^2 + \ldots = b_0 + b_1u + b_2u^2 + \ldots$$

This gives f is 1 – 1.

Finally each elements of $R[u']$ is of the type $a_0 + a_1u' + a_2(u')^2 + \ldots$ with $a_0, a_1, a_2, \ldots \in R$, which is clearly equal to $f(a_0 + a_1u + a_2u^2 + ...)$.

Hence f is onto.

Consequently $R[u] \cong R[u']$.

Let us return to R and T mentioned earlier. We call $x = (0, 1, 0, 0,...,...)$ an indeterminate over R. Now if R has no unity then R can be embedded in a ring S with unity $1(\neq 0)$. Then $T \subseteq S[x]$ with $x = (0, 1, 0, 0,...,...) \in S[x]$ but $x \notin T$. However each member of T is still of the form $a_0 + a_1x + a_2x^2 + ... + a_nx^n,\ a_i \in R$.

Still we denote T by $R[x]$. In this case it must be emphasized that $x \notin R[x]$.

NOTES

NOTES

Check Your Progress

1. Give an example of a Euclidean ring.
2. What is the definition of a polynomial over a ring?

12.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. $J[i] = \{a + bi \mid a, b \in Z\}$.
2. Any infinite sequence $(a_0, a_1, a_2, \ldots a_n, a_{n+1} \ldots)$ of elements of a ring R is said to be a polynomial over R if all except finite number of its terms a_i are equal to zero.

12.5 SUMMARY

- Gaussian integers $J[i] = \{a + bi \mid a, b \in Z\}$ is a Euclidean ring.
- If p is a prime number of the form $4n + 1$, then $p = a^2 + b^2$ for some integers a, b.
- Let $f(x) = a_o + a_1x + a_2x^2 + \ldots + a_mx^m$ be any non-zero polynomial in $R[x]$. We say $f(x)$ has *degree m* if $a_m \neq 0$ and $a_i = 0$ for all $i > m$, and write deg $f(x) = m$.

12.6 KEY WORDS

- **Polynomial:** an expression of more than two algebraic terms, especially the sum of several terms that contain different powers of the same variable(s).
- **Degree:** The degree of a polynomial is the highest degree of its monomials with non-zero coefficients.
- **Zero polynomial:** The zero polynomial is the additive identity of the additive group of polynomials. The degree of the zero polynomial is undefined.

12.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. If R and S be two isomorphic rings. Show that $R[x]$ and $S[x]$ are also isomorphic.

2. Show that R is an integral domain iff $R[x]$ is an integral domain, where $R[x]$ is the ring of polynomial of a ring R.

Long Answer Questions

1. State and prove Fermat's theorem.
2. Show that set of all polynomials with even co-efficients is a prime ideal in $\mathbf{Z}[x]$.
3. Let R be a ring. Verify that the set S of all those polynomials in $R[x]$ which have constant term zero, form a subring of $R[x]$.

12.8 FURTHER READINGS

Hungerford, Thomas W. 2003. *Algebra*. Berlin: Springer Science & Business Media.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Singh, Surjeet, Qazi Zameeruddin. 2005. *Modern Algebra*. NOIDA: Vikas Publishing House.

NOTES

UNIT 13 POLYNOMIALS OVER THE RATIONAL FIELD

Structure

13.0 INTRODUCTION

In this unit, you will know about polynomials over the rational field. In abstract algebra, the field of rationals of an integral domain is the smallest field in which it can be embedded. This unit also introduces you to the Unique Factorization Method, which is a very important concept in ring theory.

13.1 OBJECTIVES

After going through this unit, you will be able to:

- Discuss polynomials over the rational field
- Know about Unique Factorization Method
- Solve related problems

13.2 POLYNOMIALS OVER THE RATIONAL FIELD

A rational field consists of the fractions a/b, where a and b are integers and $b \neq 0$. The additive inverse of such a fraction is equal to "a/b and the multiplicative inverse, provided that $a \neq 0$ is equal to b/a. The field axioms such as the laws of distributivity, commutativity and associativity reduce to standard properties of rational numbers.

Equations of the form $a_m x^m + a_{m-1} x^{m-1} + \ldots\ldots + a_1 x + a_0 = 0$, where m is a positive integer and the a's are elements of the rational field are called polynomial equations in x.

Let F be a rational field. If $a_m, a_{m-1}, \ldots, a_1, a_0 \in F$, then any expression of the form,

$$a_m x^m + a_{m-1}x^{m-1} + \ldots. + a_1 x + a_0$$

is called a **polynomial over *F*** in the **indeterminate** x with coefficients $a_m, a_{m-1}, \ldots, a_0$. The set of all polynomials with coefficients in F is denoted by $F[x]$. If n is the largest nonnegative integer such that $a_n \neq 0$, then we say that the polynomial,

$$f(x) = a_n x^n + \ldots + a_0$$

has **degree** n, written as $\deg(f(x)) = n$ and a_n is called the leading coefficient of $f(x)$.

NOTES

13.3 UNIQUE FACTORIZATION DOMAINS

Definition: Let R be an integral domain with unity then R is called a unique factorization domain (UFD) if

(*i*) every non-zero, non-unit element a of R can be expressed as a product of finite number of irreducible elements of R and

(*ii*) if $a = p_1 p_2 \ldots. p_m$

$a = q_1 q_2 \ldots. q_n$

where p_i and q_j are irreducible in R then $m = n$ and each p_i is an associate of some q_j.

(It would, of course, be possible to write q_is in such a manner that each p_i will be an associate of q_i.)

For example, the ring $< \mathbf{Z}, +, \cdot >$ of integers is a UFD. We know it is an integral domain with unity. If $n \in \mathbf{Z}$ be any non-zero, non-unit element (i.e., $n \neq 0, \pm 1$) of $\mathbf{Z}$ then if $n > 0$, we can write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots. p_m^{\alpha_m} \text{ where } p_i \text{ are primes}$$

$$\Rightarrow n = (p_1 p_1 \ldots. p_1)(p_2 p_2 \ldots. p_2) \ldots. (p_r p_r \ldots. p_r)$$

or that n is a product of prime (and thus irreducible) elements of $\mathbf{Z}$. Again this representation of n is unique (by fundamental theorem of arithmetic).

In case $n < 0$, let $n = (-m)$ where $m > 0$ then we can express m as product of primes (therefore, irreducibles) in $\mathbf{Z}$

say, $m = q_1 q_2 \ldots. q_k$

then $(-m) = n = (-q_1)(q_2) \ldots. (q_k)$

A field $< F, +, \cdot >$ is always a UFD as it contains no non-zero, non-unit elements.

$\mathbf{Z}[\sqrt{-5}]$ is an integral domain which is not a UFD.

$46 \in \mathbf{Z}[\sqrt{-5}]$ is a non-unit, non-zero element and we can express it as product of irreducibles in two ways:

$$46 = 2 \cdot 23$$

$$46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$$

But 2 is not an associate of $1+3\sqrt{-5}$ or $1-3\sqrt{-5}$. Hence $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

NOTES

Note: That is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$ and thus by using next theorem, $\mathbf{Z}[\sqrt{-5}]$ cannot be a UFD.

Theorem 1: In a UFD R an element is prime iff it is irreducible.

Proof : Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible.

Conversely, let $a \in R$ be irreducible. Then a is non-zero, non-unit. Let $a \mid bc$ then $bc = ak$ for some k.

Case 1: b is a unit

then $c = akb^{-1} = a\ (kb^{-1}) \Rightarrow a \mid c$.

Case 2: c is a unit then similarly, $a \mid b$.

Case 3: b, c are non-units

If k is a unit, then $bc = ak$

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

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit. Thus, ck^{-1} is a unit.

But that implies c is a unit, which is again not true. Hence, k is not a unit.

We can thus express

$$b = p_1p_2 \ldots\ldots p_m.$$
$$c = q_1q_2 \ldots\ldots q_n$$
$$k = r_1r_2 \ldots\ldots r_t$$

as product of irreducibles (by definition of UFD).

So $bc = ak$ becomes

$$p_1p_2 \ldots\ldots p_m\ q_1q_2 \ldots\ldots q_n = ar_1\ r_2 \ldots\ldots r_t = x \text{ (say)}$$

Then x is an element having two representations as product of irreducible elements. By definition of UFD each element in one representation is an associate of some element in the other.

$\Rightarrow$ a is an associate of some p_i or some q_j

$\Rightarrow$ $ua = p_i$ or $ua = q_j$ for some unit u

$\Rightarrow$ $a \mid p_i$ or $a \mid q_j$

$\Rightarrow$ $a \mid b$ or $a \mid c$ $\qquad (p_i \mid b,\ q_j \mid c)$

$\Rightarrow$ a is prime element.

NOTES

Theorem 2: If R is an integral domain with unity in which every non-zero, non-unit element is a finite product of irreducible elements and every irreducible element is prime, then R is a UFD.

Proof: To show that R is a UFD we need prove that if $a \in R$ be a non-zero, non-unit element and

$$a = p_1 p_2 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$$

where p_i and q_j are irreducible elements then $m = n$ and each p_i is an associate of some q_j.

We use induction on n.

Let $n = 1$, then $a = p_1 p_2 \ldots\ldots p_m = q_1$ and as q_1 is irreducible some p_i is a unit. But each p_i being irreducible cannot be a unit. Thus $m = 1$.

$\therefore$ $a = p_1 = q_1$ or that the result is true for $n = 1$. Let it be true for $n - 1$.

Let now $a = p_1 p_2 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$

Then $p_1 p_2 \ldots\ldots p_m = q_1 (q_2 \ldots\ldots q_n)$

$\Rightarrow$ $q_1 \mid p_1 p_2 \ldots\ldots p_m$

Since q_1 is irreducible, it is prime (given)

$\Rightarrow q_1 \mid p_i$ for some i

Without loss of generality, we can take $i = 1$

then $\Rightarrow q_1 \mid p_1 \Rightarrow p_1 = q_1 u_1$

But p_1 irreducible $\Rightarrow q_1$ or u_1 is a unit.

As q_1 is not a unit (being irrducible), u_1 will be a unit and thus p_1, q_1 are associates.

Now $(q_1 u_1) p_2 p_3 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$

or $(u_1 p_2) p_3 \ldots\ldots p_m = q_2 q_3 \ldots\ldots q_n$

$\Rightarrow p_2' p_3 \ldots\ldots p_m = q_2 q_3 \ldots\ldots q_n$, $p_2' = u_1 p_2$ is irreducible.

R.H.S. contains $n - 1$ elements and result being true for $n - 1$, we find $m - 1 = n - 1 \Rightarrow m = n$.

Also, just as we showed that q_1 is an associate or p_1, we can show that q_2 is an associate of p_2, by considering $p_1 p_2 \ldots\ldots p_m = q_2 (q_1 q_3 \ldots\ldots q_n)$

Thus, q_i will be an associate of p_i.

Hence R is a UFD.

Since it has already been proved that in a UFD every irreducible element is prime, hence proved.

Theorem 3: An integral domain R with unity is a UFD if and only if every non-zero, non-unit element is a finite product of irreducible elements and every irreducible element is prime.

A second definition of a UFD and is used to solve various UFD based problems.

NOTES

Theorem 4: An integral domain R with unity is a UFD iff every non-zero, non-unit element is finite product of primes.

Proof: If R is a UFD then every non-zero, non-unit element is a finite product of irreducibles (by definition) and also every irreducible element is prime, hence the result follows.

Conversely, let $a \in R$ be a non-zero, non-unit element. Then $a = p_1 p_2 \ldots p_n$, where p_i are prime elements $\forall\ i$. Since R is an integral domain, prime elements are irreducible and so each p_i is irreducible. We now show that every irreducible element of R is a prime element. Let $x \in R$ be any irreducible element. Then $x \neq 0$, non-unit. Thus $x = q_1 q_2 \ldots q_m$ where q_i are prime. Suppose $m > 1$. Since x is irreducible, either q_1 or $(q_2 q_3 \ldots q_m)$ is a unit. But q_1 is prime and thus cannot be a unit. So $(q_2 q_3 \ldots q_m)$ is a unit which implies q_2 is a unit but that is not true as q_2 is a prime. Hence $m = 1$ or that x is prime. By theorem 2 then, R is a UFD. Summing up the preceding results, we have proved.

Theorem 5: If R is an integral domain with unity then the following are equivalent:

(*i*) R is a UFD.

(*ii*) Every non-zero, non-unit element of R is a finite product of irreducible elements and every irreducible element is prime.

(*iii*) Every non-zero, non-unit element of R is finite product of prime elements.

Theorem 6: In a UFD R any two non-zero elements have a g.c.d.

Proof : Let a, b be any two non-zero elements of R.

Suppose one of them (say a) is a unit then $aa^{-1} = 1$

$\therefore \quad b = (aa^{-1})b = a(a^{-1}\ b) \Rightarrow a \mid b$

Also $\quad a \quad = 1.\ a \Rightarrow a \mid a$

Now if $c \mid a$ and $c \mid b$ then as it means $c \mid a$

we get $\quad a = \text{g.c.d.}(a, b)$.

Similarly, if b is a unit, $b = \text{g.c.d.}(a, b)$.

Let now a and b be non-units. Since R is a UFD we can express

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$$

as product of irreducibles (note it is possible to express both a, b as product of same irreducibles by suitably choosing the powers).

Let $\quad s_i = \min(\alpha_i, \beta_i)$

we show $\quad d = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$ is g.c.d.(a, b)

Now $\quad a = (p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n})(p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots p_n^{\alpha_n - s_n})$

$$= d\,(p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots p_n^{\alpha_n - s_n})$$

$$\Rightarrow d \mid a$$

NOTES

Similarly $d \mid b$

Let now $c \mid a$ and $c \mid b$

If c is a unit, $d = (cc^{-1})d \Rightarrow c \mid d$

If c is not a unit, we can write

$$c = p_1^{r_1} p_2^{r_2} \ldots\ldots p_n^{r_n}$$

Since $c \mid a$, $r_i \leq \underline{\alpha_i}$ for all i

$c \mid b$, $r_i \leq \beta_i$ for all i

$\Rightarrow$ $r_i \leq \min(\alpha_i, \beta_i) = s_i$ for all i

Thus $d = p_1^{s_1} p_2^{s_2} \ldots\ldots p_n^{s_n} = (p_1^{r_1} p_2^{r_2} \ldots\ldots p_n^{r_n})(p_1^{s_1 - r_1} \ldots\ldots p_n^{s_n - r_n})$

$\Rightarrow$ $c \mid d$

Hence $d = \text{g.c.d.}(a, b)$

which proves our result.

As seen earlier, if d_1 and d_2 are two g.c.d.s of a, b then d_1 and d_2 are associates.

Theorem 7: Any two non-zero elements in a UFD have an l.c.m.

Theorem 8: A PID R is a UFD.

Proof: Let $a \in R$ be any non-zero, non-unit element. If a is irreducible then as $a = a$, we can express a as finite product of irreducibles. If a is not irreducible then, a is divisible by some irreducible element p_1.

$$p_1 \mid a \Rightarrow a = a_1 p_1 \text{ for some } a_1$$

If a_1 is irreducible you can express a as a product of finite number of irreducible elements.

Suppose a_1 is not irreducible.

Then a_1 is a non-zero, non-unit element as $a_1 = 0 \Rightarrow a = 0$, which is not so. Again if a_1 is a unit then as $a = a_1 p_1$, we find a and p_1 are associates and so a is irreducible as p_1 is irreducible. But a_1 is not irreducible.

Thus, $\exists$ an irreducible element p_2 such that $p_2 \mid a_1$

$\Rightarrow$ $a_1 = p_2 a_2$ for some a_2

If a_2 is irreducible, then

$$a = a_1 p_1 = p_2 p_1 a_2$$

Hence, proved if a_2 is not irreducible, we continue like this.

Consider the ideals (a), (a_1), (a_2), ...

Then $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots\ldots$

as $x \in (a) \Rightarrow x = ar = p_1 a_1 r \in (a_1)$ etc.

Thus, we get an ascending chain of ideals, which must terminate after a finite number of steps. Hence, you will get some irreducible element a_n so that

$$a = p_1 p_2 \ldots\ldots p_n a_n$$

i.e., a is expressed as a product of finite number of irreducible elements.

We need show now that if a has more than two such representations then the number of elements is same in both and each element in one representation is an associate of an element in the other.

NOTES

Let $$a = p_1 p_2 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$$

and proceed exactly as in theorem 1 and our result is proved.

Theorem 9: If $f(x)$ be a non-zero polynomial in $R[x]$ where R is a UFD, then $f(x) = df_1(x)$ where f_1 is primitive and $d = c(f)$.

Proof: Let $f(x) = a_o + a_1 x + \ldots\ldots + a_n x^n$

and let $c(f) = d = \text{g.c.d.}(a_o, a_1, \ldots\ldots a_n)$

Then $d \mid a_i$ for all i

$\Rightarrow$ $a_i = du_i$ for some u_i

$f(x) = du_o + du_1 x + \ldots\ldots + du_n x^n$

$= d(u_o + u_1 x + \ldots\ldots + u_n x^n) = df_1(x)$ where $f_1(x)$ will be primitive.

Note: If $t = \text{g.c.d.}(u_o, u_1, \ldots\ldots, u_n)$

then $t \mid u_i \; \forall \; i \Rightarrow td \mid du_i \; \forall \; i$

$\Rightarrow$ $td \mid a_i \; \forall \; i$ and thus $td \mid d$

$\Rightarrow$ $t \mid 1$ or that t is a unit.

Theorem 10: (Gauss' Lemma): Let R be a *UFD*, then in $R[x]$ the product of two primitive polynomials is a primitive polynomial.

Proof: Let $f(x) = a_o + a_1 x + \ldots\ldots + a_m x^m$

$g(x) = b_o + b_1 x + \ldots\ldots + b_n x^n$

be two primitive polynomials in $R[x]$, then $f(x)$ and $g(x)$ are non-zero (by definition). Thus

$$f(x)g(x) = c_o + c_1 x + c_2 x^2 + \ldots\ldots \text{ is also non-zero.}$$

Let $$d = \text{g.c.d.}(c_o, c_1, c_2, \ldots\ldots)$$

We show d is a unit. Suppose it is not, then there exists an irreducible element p such that, $p|d$.

[Recall that in a UFD, a non-unit element a can be expressed as a product of irreducibles, $a = p_1 p_2 \ldots\ldots p_n \Rightarrow p_1 \mid a$]

Thus $p \mid d \Rightarrow p \mid c_i$ for all i ...(1)

Now, if $p \mid a_i$ for all i then $p \mid \text{g.c.d.}(a_o, a_1, \ldots\ldots, a_m)$, which is a unit, say, u.

Now, $p \mid u \Rightarrow u = pk \Rightarrow 1 = p(ku^{-1})$

$\Rightarrow p$ is a unit,

NOTES

which is not true as p is irreducible.

$\therefore$ $p \nmid a_i$ for some i

Let i be such least +ve integer, then

$p \mid a_o, p \mid a_1, \ldots, p \mid a_{i-1}, p \nmid a_i$

Similarly $\exists$ some integer j, such that,

$p \mid b_o, p \mid b_1, \ldots, p \mid b_{j-1}, p \nmid b_j$

Now $c_{i+j} = (a_o b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \ldots + a_{i+j} b_o)$

Since $p \mid c_{i+j}$ by (1) and also

$p \mid (a_o b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1})$,

$p \mid (a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0)$

we find $p \mid a_i b_j$, but p being irreducible in a UFD is prime

$\Rightarrow p \mid a_i$ or $p \mid b_j$, a contradiction. Hence the result.

Corollary: If R is a UFD and $f(x), g(x) \in R[x]$, then

$c(f(g)) = c(f)\, c(g)$ (upto units)

Since we can write $f(x) = df_1(x)$, $d = c(f)$

$g(x) = d'g_1(x)$, $d' = c(g)$

$f(x)g(x) = dd'f_1(x)\ g_1(x)$

where f_1, g_1 being primite give $f_1 g_1$ to be primitive

$c(f_1 g_1) = 1$ (or a unit)

$\therefore$ $c(fg) = dd' = c(f)\, c(g)$

Converse of Gauss' Lemma is also true.

Theorem 11: If R is an integral domain with unity, then units of R and $R[x]$ are same.

Proof: Let a_o be a unit of R.

Then $\exists\ b_o \in R$ such that, $a_o b_o = 1$

Let $f(x) = a_o + 0.x + 0.x^2 + \ldots$

$g(x) = b_o + 0.x + 0.x^2 + \ldots$

then $f(x)g(x) = a_o b_o + 0.x + 0.x^2 + \ldots$

$= 1 = 1 + 0.x + 0.x^2 + \ldots$

$\Rightarrow f(x)$ is a unit in $R[x]$

i.e., a_o is a unit in $R[x]$.

Conversely, let $f(x)$ be any unit of $R[x]$

Then $\exists\ g(x) \in R[x]$ such that,

$f(x)g(x) = 1\ (= 1 + 0.x + 0.x^2 + \ldots)$

$\Rightarrow$ deg (fg) = deg 1

NOTES

$\Rightarrow$ deg f + deg g = 0

$\Rightarrow$ deg f = deg g = 0

$\Rightarrow$ f and g are constant polynomials

i.e., $f(x) = a_o + 0x + 0x^2 + ...$ $a_o \in R$

$g(x) = b_o + 0x + 0x^2 + ...$ $b_o \in R$

Since $fg = a_o b_o = 1$

we find, $a_o = f(x)$ is a unit of R

Hence the result.

Example 1: Show that $2x + 1$ is a unit in $\mathbf{Z}_4[x]$.

Solution: Since $(2x + 1)(2x + 1) = 0x^2 + 0x + 1 = 1$

$[4 = 0$ in $\mathbf{Z}_4]$

we find $2x + 1$ is a unit in $\mathbf{Z}_4[x]$.

Note: Notice $2x + 1$ is a non constant polynomial and, therefore, does not belong to $\mathbf{Z}_4$ and thus cannot be a unit in $\mathbf{Z}_4$. But then $\mathbf{Z}_4$ is not an integral domain. In fact, 1 and 3 are units of $\mathbf{Z}_4$. $[3 \otimes 3 = 1]$.

Theorem 12: If R is an integral domain with unity and a is an irreducible element of R then a is irreducible element of $R[x]$.

Proof: Suppose a is not irreducible element of $R[x]$ then $\exists\, p(x), q(x) \in R[x]$ such that, $a = p(x)\, q(x)$

where $p(x)$ and $q(x)$ are non-units.

Now $a = pq$

$\Rightarrow$ deg a = deg p + deg q

$\Rightarrow$ 0 = deg p + deg q

$\Rightarrow$ deg p = deg q = 0

$\Rightarrow$ p, q are constant polynomials $\Rightarrow p, q \in R$

Thus $a = pq$, $p, q \in R$ and p, q are non-units [units of R and $R[x]$ are same], a contradiction to the fact that a is irreducible in R.

Hence the result follows.

Definition: Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree (i.e., of deg ≥ 1) is said to be an *irreducible polynomial* over R if it cannot be expressed as product of two polynomials of positive degree.

In other words, if whenever $f(x) = g(x)h(x)$,

then deg $g = 0$ or deg $h = 0$

A polynomial of positive degree, which is not irreducible is called *reducible* over R.

NOTES

Example 2: Show that $\frac{\mathbf{Q}[x]}{I}$ where $I = < x^2 - 5x + 6 >$ is not a field.

Solution: Since $x^2 - 5x + 6 = (x-2)(x-3)$ we find it is not irreducible polynomial over **Q.**

Thus $I = < x^2 - 5x + 6 >$ is not a maximal ideal of $\mathbf{Q}[x]$ and hence $\frac{\mathbf{Q}[x]}{I}$ is not a field.

Example 3: Show that $f(x) = x^3 - 9$ is reducible in $\mathbf{Z}_{11}$.

Solution: Since $4 \otimes 4 \otimes 4 = 9$ in $\mathbf{Z}_{11}$, we find $(x - 4)$ is a factor of $x^3 - 9$. By actual division we find

$$x^3 - 9 = (x - 4)\ (x^2 + 4x + 5) \text{ in } \mathbf{Z}_{11}.$$

Hence $x^3 - 9$ is reducible.

Example 5: Show that the polynomial $x^2 + x + 2$ is irreducible over $F = \{0, 1, 2\}$ mod 3. Use it to construct a field of 9 elements.

Solution: Let $f(x) = x^2 + x + 2$. If it is reducible over F, we should be able to find some $\alpha \in F$ such that, $f(\alpha) = 0$.

But for no $\alpha \in F, f(\alpha) = 0$. [For example, for $\alpha = 1$, $1^2 + 1 + 2 = 1 \neq 0$ etc.]

Thus $f(x)$ is irreducible polynomial over F and as F is a field, $f(x)$ is irreducible element of $F[x]$. Hence $< f(x) >$ is a maximal ideal of $F[x]$ proving thereby that $\frac{F[x]}{< f(x) >}$ is a field.

Any element of this field is of the type

$$p(x) + < f(x) >, \text{ where } p(x) \in F[x].$$

Since $F[x]$ is a Euclidean domain,

for $f(x), p(x) \in F[x], \exists\ t(x), r(x)$ such that,

$$p(x) = f(x)\,t(x) + r(x), \text{ where either}$$

$$r(x) = 0 \text{ or } \deg r(x) < \deg f(x) = 2$$

In either case $r(x)$ is of the type $ax + b, \quad a, b \in F$

So $\quad p(x) - r(x) = f(x)\ t(x) \in < f(x) >$

i.e., $\quad p - r \in I$, where $I = < f(x) >$

$\Rightarrow\ p - r + I = I$

i.e., $\quad p + I = r + I = ax + b + < f(x) >$

Hence any member $p + < f(x) >$ of $\frac{F[x]}{< f(x) >}$ is of the type $ax + b + < f(x) >$.

Thus $\quad \frac{F[x]}{< f(x) >} = \{ax + b + < f(x) > \mid a, b \in F\}$

NOTES

Since $a \in F = \{0, 1, 2\}$ can be chosen in three ways and for each choice of a, b can be selected in three ways, we find the number of elements of $\frac{F[x]}{< f(x) >}$ will be $3 \times 3 = 9$. Thus $\frac{F[x]}{< f(x) >}$ is the required field of nine elements.

Eisenstein's Criterion

Theorem 13: (Eisenstein's criterion): Let $f(x) = a_o + a_1x + a_2x^2 + ... + a_nx^n$ be a polynomial with integer coefficients (i.e., $f(x) \in \mathbf{Z}[x]$). Suppose that for some prime number p,

$$p \mid a_o,\ p \mid a_1,\ p \mid a_2\ ...,\ p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_o$$

then $f(x)$ is irreducible polynomial over $\mathbf{Q}$, the ring of rationals.

We first prove.

Lemma: If $f(x) \in \mathbf{Z}[x]$ is primitive and $f(x)$ is irreducible over $\mathbf{Z}$ then f is irreducible over $\mathbf{Q}$.

Proof: Suppose f is not irreducible over $\mathbf{Q}$, then we can write $f = gh$, $g, h \in \mathbf{Q}[x]$ with deg g, deg $h > 0$

Then $g(x) \in \mathbf{Q}[x] \Rightarrow g = \frac{1}{\alpha} g_1(x)$ where $g_1(x) \in \mathbf{Z}[x]$

$h(x) \in \mathbf{Q}[x] \Rightarrow h = \frac{1}{\beta} h_1(x)$ where $h_1(x) \in \mathbf{Z}[x]$

(For instance, if $g(x) = \frac{2}{3}x^2 + \frac{1}{2}x + 1 \in \mathbf{Q}[x]$ then $g(x) = \frac{1}{6}(4x^2 + 3x + 6)$, where then $g_1(x) = 4x^2 + 3x + 6 \in \mathbf{Z}[x]$).

Again $g_1(x) \in \mathbf{Z}[x] \Rightarrow g_1 = dg_1^*$ where g_1^* is primitive

$h_1(x) \in \mathbf{Z}[x] \Rightarrow h_1 = d'h_1^*$ where h_1^* is primitive

Thus $f = gh = \frac{1}{\alpha\beta} dd' g_1^* h_1^*$

$\Rightarrow \alpha\beta f = dd' g_1^* h_1^*$

$\Rightarrow c(\alpha\beta f) = c(dd' g_1^* h_1^*)$

Since f is primitive polynomial in $\mathbf{Z}[x]$, its content is a unit in $\mathbf{Z}$ and as units in $\mathbf{Z}$ are 1 or – 1 $c(f) = \pm 1$. Similarly, $c(g_1^*)$, $c(h_1^*)$ can be ± 1.

Equating the contents on both sides, we get

$$\pm\alpha\beta = \pm dd'$$

i.e., $\alpha\beta = \pm dd'$

and, hence, the equation $\alpha\beta f = dd' g_1^* h_1^*$ reduces to $f = \pm g_1^* h_1^*$

Now, deg $(\pm g_1^*)$ = deg g_1^* = deg dg_1^* = deg g_1

$$= \deg \frac{1}{\alpha} g_1 = \deg g > 0$$

NOTES

Similarly, $\deg(h_1^*) > 0$.

Thus, we can write $f = \pm g_1^* h_1^*$ where $\pm g_1^*, h_1^*$ are polynomials in $\mathbf{Z}[x]$ and have positive degree

$\Rightarrow$ f is reducible over $\mathbf{Z}$, a contradiction

hence, the lemma is proved.

We now come to the proof of the main theorem.

We show f is irreducible over $\mathbf{Z}$.

Suppose it is not irreducible over $\mathbf{Z}$, then $\exists\ g, h \in \mathbf{Z}[x]$ such that, $f = gh$

with $\deg g, \deg h > 0$

Let $g(x) = b_o + b_1 x + \ldots\ldots + b_s x^s$

$h(x) = c_o + c_1 x + \ldots\ldots + c_t x^t$

then $g(x)\ h(x) = b_o c_o + (b_1 c_o + b_o c_1)x + \ldots\ldots$

So $f = gh$

$\Rightarrow\ a_o + a_1 x + \ldots\ldots = b_o c_o + (b_1 c_o + b_o c_1)\ x + \ldots$

$\Rightarrow\ a_o = b_o c_o$

Now $p \mid a_o \Rightarrow p \mid b_o c_o \Rightarrow p \mid b_o$ or $p \mid c_o$ as p is prime

Suppose $p \mid b_0$ then $p \nmid c_0$ as $p^2 \nmid a_o$

$[p \mid b_0, p \mid c_0 \Rightarrow p^2 \mid b_0 c_0 \Rightarrow p^2 \mid a_0]$

Again, p cannot divide all of $b_0, b_1, b_2, \ldots\ldots, b_s$ as if it does then p divides each term of the type

$b_0 c_0,\ b_1 c_0 + b_0 c_1,\ \ldots\ldots$

i.e., p divides all of $a_0, a_1, \ldots\ldots, a_n$

But $p \nmid a_n$

Let k be the smallest integer such that $p \nmid b_k$, $k \le s < n$

So $p \mid b_0, p \mid b_1, \ldots\ldots, p \mid b_{k-1}, p \nmid b_k$

Now $a_k = b_k c_0 + b_{k-1} c_1 + \ldots\ldots + b_o c_k$

$p \mid a_k$ by given condition as $k < n$

Also $p \mid (b_{k-1} c_1 + b_{k-2} c_2 + \ldots\ldots + b_0 c_k)$

$\Rightarrow\ p \mid b_k c_0 \Rightarrow p \mid b_k$ or $p \mid c_0$

both leading to a contradiction. Hence $f(x)$ is irreducible over $\mathbf{Z}$.

If $f(x)$ is primitive, it will be irreducible over $\mathbf{Q}$ by lemma. If $f(x)$ is not primitive we can write $f = d f_1$ where f_1 is primitive and $d = c(f)$

Then f irreducible over $\mathbf{Z} \Rightarrow d f_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow\ f_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow\ f_1$ is irreducible over $\mathbf{Q}$ (as f_1 is primitive)

$\Rightarrow\ d f_1$ is irreducible over $\mathbf{Q}$

$\Rightarrow\ f$ is irreducible over $\mathbf{Q}$

NOTES

Hence, the theorem is proved.

Note: Since $f(x) = g(x)h(x) \Leftrightarrow f(x+1) = g(x+1)\ h(x+1)$

We find $f(x)$ will be reducible (irreducible) iff $f(x+1)$ is reducible (irreducible). In fact one can take any integer in place of 1.

The polynomial $f(x) = x^3 - x + 1$ is irreducible over **Q**, as suppose it is reducible then it has a root in **Q**.

Let $\frac{m}{n}$ [m, n integers, $n \neq 0$, $(m, n) = 1$] be a root.

Then $\frac{m^3}{n^3} - \frac{m}{m} + 1 = 0$

$\Rightarrow m^3 - mn^2 + n^3 = 0$

$\Rightarrow m^3 = n^2\ (m - n)$

$\Rightarrow n^2 \mid m^3 \Rightarrow n \mid m^3.\ 1 \Rightarrow n \mid 1$ as $(m, n) = 1$

$\Rightarrow n = \pm 1$

$\Rightarrow \frac{m}{n} = \pm m$

or that $m^3 - m + 1 = 0$

$\Rightarrow m\ (m^2 - 1) = -1$

$\Rightarrow m \mid 1$ or that $m = \pm 1$

$\Rightarrow \frac{m}{n} = \pm 1$ which gives

$1 - 1 + 1 = 0$, which is not possible.

Hence, $x^3 - x + 1$ is not reducible over **Q**.

13.4 RELATED PROBLEMS

Problems 1: For any prime p show that the

poly, $x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$ is irreducible over Q.

Let $f(x) = x^{p-1} + x^{p-2} + 2 \ldots + x^2 + x + 1$

$$= \frac{x^{p-1}}{x-1} \text{ (sum of a GP)}$$

Now

$$f(x+1) = \frac{(x+1)^p - 1}{(x-1) - 1} = x^p + p^p c_1 x^{p-1} + \cdots$$

NOTES

$$\frac{+^{p}c_{p}x^{p-2}+\cdots+^{p}c_{p}-1}{x}$$

$$= \frac{x^{p}+^{p}c_{1}x^{p-1}+\cdots+^{p}c_{p-1}x}{x}$$

$$= x^{b-1}+^{p}c_{1}x^{p-2}+\cdots+^{p}c_{p-1}$$

Since p is *a* prime no. $p/^{p}c_{p}$ for all

$1 \le r \le p-1$

Also $^{p}c_{p-1}$ *or* $p^2 +^{p}c_{p-1.}$

Hence by eisentein criterian f(x+1)

Problems 2: The polynomial $x^2 - 4x + 2$ is irreducible over **Q**, as if we take $p = 2$, then $p \mid 4$, $p \mid 2$, $p \nmid 1$, $p^2 \nmid 2$.

Again, consider the polynomial $x^2 + 1 = f(x)$.

Since there is no prime p which divides 1, we cannot apply the Eisenstein's criterion to $f(x)$.

Consider $f(x + 1) = (x + 1)^2 + 1$

$= x^2 + 2x + 2$ ($a_o = 2$, $a_1 = 2$, $a_2 = 1$)

Take $p = 2$, then $p \mid 2$, $p \nmid 1$, $p^2 \nmid 2$

Hence $f(x + 1)$ is irreducible.

$\Rightarrow f(x)$ is irreducible (by using the preceding remarks)

Again, let $f(x) = x^3 + x^2 - 2x - 1$

Since there is no prime that divides 1, we cannot apply the criterion here.

Consider $f(x + 1) = (x + 1)^3 + (x + 1)^2 - 2(x + 1) - 1$

$= x^3 + 4x^2 + 3x - 1$

We have the same situation. Let us consider

$f(x - 1) = (x - 1)^3 + (x - 1)^2 - 2(x - 1) - 1$

$= x^3 - 2x^2 - x - 1$

Again it is not possible to apply the criterion.

Consider $f(x + 2) = x^3 + 7x^2 + 14x + 7$

then $p = 7$ will do as here $a_0 = 7$, $a_1 = 14$, $a_2 = 7$, $a_3 = 1$ and $7 \mid 7$, $7 \mid 14$, $7 \mid 7$, $7 \nmid 1$, $7^2 \nmid 7$.

Thus, by criterion $f(x + 2)$ and therefore, $f(x)$ is irreducible.

Note: One may note that Eisenstein's criterion is not necessary for irreducibility of a polynomial as you have seen there does not exist any prime p such that $p \mid 1$ (although the polynomial could be irreducible). $x^3 - x + 1$ is irreducible over **Q**, but Eisenstein's criterion is not applicable.

NOTES

Check Your Progress

1. Is $F[x]$ *a* Euclidean domain when F is a field?
2. Is $Z[x]$ *a* PID?
3. What is an irreducible polynomial?

13.5 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. Yes $F[x]$ is a Euclidean domain when F is a field.
2. No, $Z[x]$ is not a PID as Z is not a field.
3. Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree is said to be an irreducible polynomial over R if it cannot be expressed as product of two polynomials of positive degree.

13.6 SUMMARY

- Let F be a rational field. If $a_m, a_{m-1}, \ldots, a_1, a_0 \in F$, then any expression of the form, $a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ is called a **polynomial over *F*** in the **indeterminate** x with coefficients $a_m, a_{m-1}, \ldots, a_0$. The set of all polynomials with coefficients in F is denoted by $F[x]$.
- Let R be an integral domain with unity then R is called a unique factorization domain (UFD) if (i) every non-zero, non-unit element a of R can be expressed as a product of finite number of irreducible elements of R and (*ii*) if $a = p_1 p_2 \ldots p_m$; $a = q_1 q_2 \ldots q_n$ where p_i and q_j are irreducible in R then $m = n$ and each p_i is an associate of some q_j..
- Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree is said to be an irreducible polynomial over R if it cannot be expressed as product of two polynomials of positive degree. A polynomial of positive degree, which is not irreducible is called reducible over R.

13.7 KEY WORDS

- **Polynomial:** an expression of more than two algebraic terms, especially the sum of several terms that contain different powers of the same variable(s).
- **Degree:** The degree of a polynomial is the highest degree of its monomials with non-zero coefficients.
- **Zero polynomial:** The zero polynomial is the additive identity of the additive

group of polynomials. The degree of the zero polynomial is undefined.

- **Rational field:** The field of rationals is the set of rational numbers, which form a field. This field is commonly denoted Q.
- **Ring:** A ring is one of the fundamental algebraic structures used in abstract algebra. It consists of a set equipped with two binary operations that generalize the arithmetic operations of addition and multiplication.

NOTES

13.8 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Show that an integral domain R with unity is a field iff $R[x]$ is a PID.
2. Write a short note on polynomials over the rational field.
3. Explain in briefly the concept of UFD?

Long Answer Questions

1. Show that if F is a field, then $F[x]$ is a Euclidean ring.
2. Show that if is an integral domain with unity, then units of R and are same.
3. Explain Eisenstein's criterion.

13.9 FURTHER READINGS

Hungerford, Thomas W. 2003. *Algebra*. Berlin: Springer Science & Business Media.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Singh, Surjeet, Qazi Zameeruddin. 2005. *Modern Algebra*. NOIDA: Vikas Publishing House.

NOTES

UNIT 14 POLYNOMIAL RINGS OVER COMMUTATIVE RINGS

Structure

14.0 INTRODUCTION

In this unit, you will know about polynomial rings over the commutative rings. Polynomial rings occur in many parts of mathematics, and the study of their properties was among the main motivations for the development of commutative algebra and ring theory.

14.1 OBJECTIVES

After going through this unit, you will be able to:

- Discuss polynomial rings over commutative rings
- Solve related problems

14.2 POLYNOMIAL RINGS OVER COMMUTATIVE RINGS

Theorem 1: Let $R[x]$ be the ring of polynomials over a ring R then

(*i*) R is commutative iff $R[x]$ is commutative.

(*ii*) R has unity iff $R[x]$ has unity.

Proof: (*i*) If $R[x]$ is commutative then any subring of $R[x]$ is commutative and as R is isomprphic to a subring of $R[x]$, R will be commutative.

NOTES

Conversely, if R is commutative

and $f(x) = a_o + a_1x + a_2x^2 + ... + a_mx^m$

$g(x) = b_o + b_1x + b_2x^2 + ... + b_nx^n$

be two members of $R[x]$, then by definition of product

$$f(x)g(x) = a_ob_o + (a_1b_o + a_ob_1)x + ...$$
$$= b_oa_o + (b_1a_o + b_oa_1)x + ...$$
$$= g(x)f(x).$$

(*ii*) If R has unity 1 then the polynomial

$e(x) = 1 + 0x + 0x^2 + ...$ is unity of $R[x]$ as $f(x)e(x)$ will be $f(x)$ for any polynomial $f(x)$.

Conversely, let $R[x]$ have unity.

Define a map $\theta : R[x] \to R$, such that,

$$\theta(f(x))) = \theta(a_o + a_1x + .. + a_mx^m) = a_o$$

then θ is an onto homomorphism.

Thus, R is a homomorphic image of $R[x]$ and hence has unity, as homomorphic image of a ring with unity is a ring with unity. It fact, $\theta(e(x))$ will be unity of R where $e(x)$ is unity of $R[x]$.

Theorem 2: Let $R[x]$ be the ring of polynomial of a ring R and suppose

$$f(x) = a_o + a_1x + ... + a_mx^m$$
$$g(x) = b_o + b_1x + ... + b_nx^n$$

are two non-zero polynomials of degree m and n respectively, then

(*i*) If $f(x) + g(x) \neq 0$, $\deg(f(x) + g(x)) \leq max(m, n)$

(*ii*) If $f(x)\ g(x) \neq 0$, $\deg(f(x)\ g(x)) \leq m + n$

(*iii*) If R is an integral domain, $\deg(f(x)\ g(x)) = m + n$

(*iv*) R is an integral domain iff $R[x]$ is an integral domain.

(*v*) If F is a field, $F[x]$ is not a field.

Proof: (*i*) By definition,

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_t + b_t)x^t$$

where $t = \max(m, n)$.

Now $a_k + b_k = 0$ for all $k > t$ as $a_k = 0$, $b_k = 0$

thus degree of $f(x) + g(x)$ is less than or equal to $t = \max(m, n)$. Notice it is possible to have $\deg(f(x) + g(x)) < \max(m, n)$. Consider the ring $\mathbf{Z}$ of integers.

Let $f(x) = 1 + 2x - 2x^2$

$g(x) = 2 + 3x + 2x^2$

be two members of $\mathbf{Z}[x]$,

then $f(x) + g(x) = (1 + 2) + (2x + 3x) + (-2x^2 + 2x^2)$

$= 3 + 5x$

NOTES

Thus deg $(f(x) + g(x)) = 1$ whereas deg $f(x) = 2 =$ deg $g(x)$

(*ii*) Let $f(x)\ g(x) = c_0 + c_1x + c_2x^2 + ...$

where $c_k = (a_kb_0 + a_{k-1}\ b_1 + ... + a_0b_k)$.

Here $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + ... + a_mb_n\ \ ..... + a_{m+n}b_0$

$= a_mb_n$

as all other terms would be zero. ($a_{m+i} = 0$, $b_{n+j} = 0$ for all $i, j > 0$).

Again, $c_{m+n+t} = 0$ for all t > 0 and

thus deg$(f(x)\ g(x)) \leq m + n$ (a_mb_n can be zero even if $a_m \neq 0\ b_n \neq 0$)

We show that it is possible that deg $(f(x)\ g(x)) < m + n$.

Consider the ring $R = \{0, 1, 2, 3, 4, 5\}$ modulo 6

Take $f(x) = 1 + 2x^3$

$g(x) = 2 + x + 3x^2$

two polynomials in $R[x]$ of degree 3 and 2, respectively.

Here $f(x)g(x) = 2 + x + 3x^2 + 4x^3 + 2x^4$

which is of degree $4 < 5$.

Notice, here R is not an integral domain.

(*iii*) If R is an integral domain then as $a_m \neq 0$, $b_n \neq 0$, therefore, $a_mb_n \neq 0$ and hence $c_{m+n} = a_mb_n \neq 0$ showing that deg $(f(x)g(x)) = m + n$.

(*iv*) If $R[x]$ is an integral domain then since R is isomorphic to a subring of $R[x]$, R will also be an integral domain.

Conversely, suppose R is an integral domain.

Let $f(x)$, $g(x)$ be any two non-zero members of $R[x]$ such that,

$f(x)g(x) = 0$

where $f(x) = a_o + a_1x + ... + a_mx^m$

$g(x) = b_o + b_1x + ... + b_nx^n$

Now both $f(x)$ and $g(x)$ cannot be constant polynomials as then $a_o \neq 0$, $b_o \neq 0$ (so $c_o = a_ob_o \neq 0$)

$\therefore \quad f(x)g(x) \neq 0$

Since at least one of $f(x)$, $g(x)$ is non constant polynomial, its degree is ≥ 1.

R being an integral domain

deg $(f(x)g(x)) =$ deg $f(x) +$ deg $g(x) \geq 1$

NOTES

which is a contradiction as it implies then $c_k \neq 0$ for some $k > 0$

whereas $f(x)g(x) = 0$.

Hence $f(x)g(x) = 0 \Rightarrow f(x) = 0$ or $g(x) = 0$

$\Rightarrow$ $R[x]$ is an integral domain.

(v) Let F be a field, then since F is commutative, has unity, by previous results we find $F[x]$ will be a commutative ring with unity. In fact F being an integral domain, $F[x]$ will also be an integral domain. We show, not all non-zero elements of $F[x]$ have multiplicative inverse. Consider the non-zero polynomial

$$f(x) = 0 + 1x + 0x^2 + 0x^3 + \ldots \; (= a_o + a_1x + a_2x^2 + \ldots\ldots)$$

Suppose $g(x) = b_o + b_1x + b_2x^2 + \ldots$ is its multiplicative inverse

then $f(x)g(x) = c_o + c_1x + c_2x^2 + \ldots$

should be unity $e(x) = 1 + 0x + 0x^2 + \ldots$ of $F[x]$

$\Rightarrow$ $c_o = 1$, $c_i = 0$ for all $i > 0$

where $c_o = a_ob_o = 0 \,.\, b_o = 0 \neq 1$.

Hence no $g(x)$ can be multiplicative inverse of $f(x) = x$.

Showing that $F[x]$ is not a field.

If R is a ring, we get $R[x]$ the corresponding ring of polynomials. Since $R[x]$ is a ring, we can similarly get $R[x, y]$ the corresponding ring of polynomials of $R[x]$ and the process can be extended. If F is a field then $F[x]$ is a ring with unity and similarly $F[x, y]$ will be a ring with unity. We shall use it a little later when we come to factorisation domains.

Example 1: Let R and S be two isomorphic rings. Show that $R[x]$ and $S[x]$ are also isomorphic.

Solution: Let $\phi : R \to S$ be the given isomorphism.

Define a mapping

$f : R[x] \to S[x]$, such that,

$$f(a_o + a_1x + \ldots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n.$$

It should now be a routine exercise for the reader to show that this f is an isomorphism.

Theorem 3: If F is a field, then $F[x]$ is a Euclidean domain.

Proof: We have seen that $F[x]$ is an integral domain with unity.

For any $f(x) \in F[x]$, $f(x) \neq 0$, define

$d(f(x)) = \deg f(x)$ which is non – ve integer

Since, for any $f(x)$, $g(x) \in F[x]$, $f(x)$, $g(x) \neq 0$

$\deg (f(x)\, g(x)) = \deg f(x) + \deg g(x)$

we get $\deg (f(x)) \leq \deg (f(x)g(x))$, as $\deg (g(x)) \geq 0$

$\therefore \quad d(f(x)) \leq d(f(x)g(x))$

Lastly, we show for any non-zero $f(x), g(x)$ in $F[x]$, $\exists\ t(x)$ and $r(x)$ in $F[x]$ such that

NOTES

$$f(x) = t(x)g(x) + r(x)$$

where either $r(x)$ is zero or $\deg r(x) < \deg g(x)$

If $\deg f(x) < \deg g(x)$ then $f(x) = 0$. $g(x) + f(x)$ gives the result.

Assume now the result is true for all (non-zero) polynomials in $F[x]$ of deg. less than $\deg f(x)$.

Let $f(x) = a_0 + a_1 + \ldots + a_m x_m$

$g(x) = b_0 + b_1 x + \ldots + b_n x_n$

Suppose $\deg f(x) \geq \deg g(x)$

Define $f_1(x) = f(x) - a_m b_n^{-1}\ x^{m-n}\ g(x)$ then coefficient of x^m in $f_1(x)$ is $a_m - a_m b_n^{-1}.\ b_n = a_m - a_m = 0$

either $f_1(x) = 0$ (zero polynomial) or $\deg f_1(x) < m$

If $f_1(x) = 0$, then

$$0 = f(x) - a_m b_n^{-1} x^{m-n}\ g(x)$$

gives $f(x) = a_m b_n^{-1} x^{m-n}\ g(x) + 0$

So by taking $t(x) = a_m b_n^{-1} x^{m-n}$ and $r(x) = 0$ we get the required result.

Suppose $f_1(x) \neq 0$,

then $\deg f_1(x) < m$

i.e., $\deg f_1(x) < \deg f(x)$

By induction hypothesis

$$f_1(x) = t_1(x)\ g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore \quad f(x) - a_m b_n^{-1}\ x^{m-n}\ g(x) = t_1(x)\ g(x) + r(x)$

or $f(x) = [a_m b_n^{-1}\ x^{m-n} + t_1(x)]\ g(x) + r(x)$

$= t(x)g(x) + r(x)$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

and hence $F[x]$ is a Euclidean domain (and also, therefore, a PID).

Notes:

1. Thus $\mathbf{Q}[x]$ is a Euclidean domain which is not a field.
2. One can show that the above defined $t(x)$ and $r(x)$ are unique.
   Suppose $f(x) = t(x)\ g(x) + r(x)$ where either $r(x) = 0$ or $\deg r < \deg g$

and $f(x) = t'(x)\, g(x) + r'(x)$ where either $r'(x) = 0$ or deg $r' <$ deg g

then $t(x)\, g(x) + r(x) = t'(x)\, g(x) + r(x)$

$\Rightarrow$ $g(t - t') = r' - r$ ...(1)

Suppose $t(x) \neq t'(x)$ then $t - t' \neq 0$ and thus has degree ≥ 0

(1) $\Rightarrow$ deg $(g(t - t'))$ = deg $(r' - r)$

$\Rightarrow$ deg g +deg $(t - t')$ = deg $(r' - r)$ ...(2)

Also since $g(t-t')$ has positive degree $(\geq n)$, $r' - r$ cannot be zero, otherwise $g(t - t')$ would be a constant polynomial, so its degree cannot be $\geq n$.

$r' - r$ cannot be zero $\Rightarrow$ both r and r' cannot be zero together.

Now L.H.S. of (2) is greater than or equal to deg g

whereas R.H.S. of (2) is $\leq$ max (deg r', deg r) $<$ deg g

as if both r, r' are non-zero then deg $r <$ deg g

deg $r' <$ deg g

$\Rightarrow$ max (deg r, deg r') $<$ deg g

If one of r, r' is zero, the other has deg less than deg g. In any case R.H.S. $<$ deg g,

which is a contradiction.

Thus $t - t' = 0 \Rightarrow t = t'$

$\therefore$ (1) $\Rightarrow$ $r = r'$.

Hence the uniqueness is established.

If F is a field then $F[x]$ being a Euclidean domain will be a PID.

Theorem 4: If F is a field, every ideal in $F[x]$ is principal.

Example 2: Let $R = \{0, 1)$ mod 2, then $R[x]$ is an infinite integral domain. If $f(x) \in R[x]$ be any member and if,

$$f(x) = a_o + a_1 x + ... + a_m x^m \text{ then we have}$$

$$\begin{aligned} 2\, f(x) &= f(x) + f(x) \\ &= (a_o \oplus a_o) + (a_1 \oplus a_1)\, x + ... + (a_m \oplus a_m)\, x^m \\ &= 0 + 0.x + 0.x^2 + ... \\ &= O(x), \text{ zero of } R[x] \end{aligned}$$

Thus $2f(x) = 0\ \forall f \in R[x]$, showing that $R[x]$ is of finite characteristic (although it is infinite). Note also that ch R = ch $R[x]$.

Example 3: Let R be a commutative ring with unity. Let A be an ideal of R. Show that

$$\frac{R[x]}{A[x]} \cong \frac{R}{A}[x].$$

Hence or otherwise prove or disprove

A is prime ideal of $R \Rightarrow A[x]$ is prime ideal of $R[x]$.

NOTES

Solution: Define a mapping

$$\theta : R[x] \to \frac{R}{A}[x] \text{ such that,}$$

$$\theta(f(x)) = \theta(a_o + a_1x + ... + a_nx^n)$$
$$= (a_o + A) + (a_1 + A)\,x + ... + (a_n + A)x^n$$

then θ is clearly well defined.

If $f(x) = a_o + a_1x + a_2x^2 + ...$

$g(x) = b_o + b_1x + b_2x^2 + ...$

$f(x)g(x) = c_o + c_1x + c_2x^2 + ...$

then $\theta(f(x) + g(x)) = \theta((a_o + b_o) + (a_1 + b_1)\,x + ...)$

$= [(a_o + b_o) + A] + [(a_1 + b_1) + A]\,x + ...$

$= (a_o + A) + (b_o + A) + (a_1 + A)x + (b_1 + A)\,x + ...$

$= ((a_o + A) + (a_1 + A)x + ...) + ((b_o + A) + (b_1 + A)x + ...)$

$= \theta(f(x)) + \theta(g(x))$

$\theta(f(x)g(x)) = \theta(c_o + c_1x + c_2x^2 + ...)$

$= (c_o + A) + (c_1 + A)x + ...$

$= (a_ob_o + A) + (a_1b_o + a_ob_1 + A)x + ...$

$= (a_o + A)\,(b_o + A) + [(a_1b_o + A) + (a_ob_1 + A)]x + ...$

$= (a_o + A)\,(b_o + A) +$
$[(a_1 + A)\,(b_o + A) + (a_o + A)\,(b_1 + A)]x + ...$

Also $\theta(f(x))\ \theta(g(x)) = [(a_o + A) + (a_1 + A)x + ...]\ [(b_o + A) + ...]$

$= (a_o + A)\,(b_o + A) + [(a_1 + A)\,(b_o + A) + (a_o + A)\,(b_1 + A)]x + ...$

$\Rightarrow$ θ is a homorphism.

That θ is onto is evident from the definition of θ and hence by fundamental theorem,

$$\frac{R[x]}{\text{Ker}\,\theta} \cong \frac{R}{A}[x].$$

Now $f(x) \in \text{Ker}\ \theta \Leftrightarrow \theta(f(x)) = (0 + A) + (0 + A)\,x + ...$

$\Leftrightarrow$ $(a_0 + A) + (a_1 + A)\,x + ... = (0 + A) + (0 + A)\,x + ...$

$\Leftrightarrow$ $a_i + A = A$ for all i

$\Leftrightarrow$ $a_i \in A$ for all i

$\Leftrightarrow$ $f(x) \in A[x]$

Hence $\dfrac{R[x]}{A[x]} \cong \dfrac{R}{A}[x]$

Finally, let A be a prime ideal of R.

Then $\frac{R}{A}$ is an integral domain.

$\Rightarrow \frac{R}{A}[x]$ is an integral domain

$\Rightarrow \frac{R[x]}{A[x]}$ is an integral domal, because of the isomorphism

$\Rightarrow A[x]$ is a prime ideal of $R[x]$.

Note: It is clear if A is an ideal of a ring R then $A[x]$ is an ideal of $R[x]$ (Kernels are ideals).

Theorem 5: Let R be a commutative ring with unity such that $R[x]$ is a *PID,* then R is a field.

Proof: By previous theorem, $\frac{R[x]}{< x >} \cong R$.

We claim $< x >$ is a maximal ideal of $R[x]$.

Suppose I is any ideal such that $< x > \subseteq I \subseteq R[x]$.

Since $R[x]$ is a PID, $I = < f(x) >$ for some $f(x) = a_0 + a_1x + ... + a_nx_n$

Now $x \in < x > \subseteq I = < f(x) >$

$\Rightarrow x = f(x)g(x)$ for some $g(x) \in R[x]$

which implies either $f(x) = x$, $g(x) = 1$. (unity of $R[x]$)

or $f(x) = \alpha x$, $g(x) = \alpha^{-1}$, $\alpha \in R$

or $f(x) = 1$, $g(x) = x$

(Second case being conditional to the existence of α^{-1})

If $f(x) = x$, $I = < f(x) > \Rightarrow I = < x >$

if $f(x) = \alpha x$, $I = < f(x) > \Rightarrow I = < \alpha x > = < x >$

if $f(x) = 1$, $I = < f(x) > \Rightarrow I = < 1 > = R[x]$

Hence, $< x >$ is a maximal ideal.

$\therefore \frac{R[x]}{< x >}$ is a field.

Hence, R is a field.

Example 4: Let R be a commutative ring with unity and $< x >$ be a prime ideal of $R[x]$. Show that R must be an integral domain.

Solution: Let $a, b \in R$ be such that $ab = 0$

Then the polynomials

$(0 + 1x + 0x^2 + ...) + (a + 0x + 0x^2 + ...)$ and

$(0 + 1x + 0x^2 + ...) + (b + 0x + 0x^2 + ...)$ belong to $R[x]$

$\Rightarrow x + a, x + b \in R[x]$

NOTES

$\Rightarrow (x + a)(x + b) \in R[x]$

$\Rightarrow x^2 + x(a + b) + ab \in R[x]$

Since $ab = 0$, $x^2 + x(a + b) = x[x + a + b] \in \langle x \rangle$

thus $(x + a)(x + b) \in \langle x \rangle$

$\Rightarrow (x + a) \in \langle x \rangle$ or $(x + b) \in \langle x \rangle$ as $\langle x \rangle$ is prime ideal

Now $(x + a) \in \langle x \rangle \Rightarrow x + a = xf(x)$ for some $f(x) \in R[x]$

$= x(a_0 + a_1x + ...)$

$\Rightarrow a = 0$

Similarly if $(x + b) \in \langle x \rangle$ then $b = 0$.

Hence, R is an integral domain.

Example 5: Show that the ideal

$A = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbf{Z}[x]\}$ of $\mathbf{Z}[x]$ is not a principal ideal.

Solution: Suppose A is a principal ideal generated by $k(x)$, $k(x) \in \mathbf{Z}[x]$

Since $x = x(1 + 0x + 0x^2 + ...) + 2(0 + 0x^2 + ...) \in A = \langle k(x) \rangle$

$x = k(x)\, h(x)$

Also $2 \in \langle k(x) \rangle \Rightarrow 2 = k(x)t(x)$ ...(1)

Thus $xk(x)t(x) = 2k(x)h(x)$

$\Rightarrow 2h(x) = xt(x)$

$\Rightarrow$ each coefficient of $t(x)$ is an even integer.

i.e., $t(x) = 2r(x)$ for some $r(x) \in \mathbf{Z}[x]$

$\Rightarrow 2 = 2k(x)r(x)$

$\Rightarrow r(x)k(x) = 1$

$\Rightarrow 1 \in \langle k(x) \rangle$

$\Rightarrow \langle k(x) \rangle = \mathbf{Z}[x]$ [ideal with unity]

$\Rightarrow A = \mathbf{Z}[x]$

which is not true as A is proper ideal of $\mathbf{Z}[x]$.

Note: Example 5 shows us that $\mathbf{Z}[x]$ is not a PID.

Example 6: Show that the above ideal A is maximal ideal in $\mathbf{Z}[x]$.

Solution: Let I be an ideal such that $A \subset I \subseteq \mathbf{Z}[x]$.

Since $A \neq I$, $\exists$ $h(x) \in I$, such that, $h(x) \notin A$.

Let $h(x) = b_o + b_1x + b_2x^2 + ... + b_mx^m$

then b_o is odd as if b_o is even then $h(x) \in A$.

$h(x) = 2k + b_1x + b_2x^2 + ... + b_mx^m = g(x) + xf(x)$ type

Thus $h(x) = (2a + 1) + b_1x + b_2x^2 + ... + b_mx^m$

$h(x) = g(x) + 1$

$\Rightarrow \quad 1 = h(x) - g(x)$

$\Rightarrow \quad 1 \in I$ as $h(x) \in I$, $g(x) \in A \subseteq I$

$\Rightarrow \quad I = \mathbf{Z}[x]$

$\Rightarrow$ A is maximal.

Note: We also use the notation $(2, x)$ for the ideal A.

NOTES

14.3 SUPPLEMENTARY PROBLEMS

Problems 1. Show that $\frac{Z_3(x)}{I}$ where $I = <x^2 + x + 1>$ is not a integral domain.

Ans. $(x + 2) + I \in \frac{Z_3(x)}{I}$

and $[(x + 2) + I]^2 = (x + 2)^2 + I = (x^2 + 1 \,.\, x + 1) + I$

$= I =$ zero of $\frac{Z_3(x)}{I}$

but $(x + 2) + I$ is not a zero of $\frac{Z_3(x)}{I}$

$\frac{Z_3(x)}{I}$ is not an Integral Domain.

Problems 2. Show that $f(x) = 8x^3 + 6x + 1 \in z(x)$ is primitive where as $g(x) = = 8x^3 + 6x + 2 \in z(x)$ is not primitive.

Ans. Consider $c(f) = g.c.d.\ (8, 6, 1) = 1$

$c(f) = g.c.d.\ (8, 6, 2) = 2$

Also $g(x) = 2(4x^3 + 3x + 1) = 2g(x)$

where $c(g) = 1$

Here $g(x) = 2g(x)$ where $g(x)$ is primitive

Problems 3. Show that $\frac{Q(x)}{I}$ where $I = <x^2 - 5x + 6>$ is not a field.

A. Since $x^2 - 5x + 6 = (x - z)\,(x - 3)$, we find it is not ... irreducible polynomial over Q.

Thus $I = <x^2 - 5x + 6>$ is not a maximal ideal of $Q(x)$ and hence $\frac{Q(x)}{I}$ is not a field.

NOTES

Problems 4. Show that $z_5(x)$ is a UFD.

Sol. Since 5 is prime, z_5 is a field

UFO $\Rightarrow z_5$ is a UFD

Diff. $\Rightarrow z_5(x)$ is a UFD

Problems 5. $z\left[\sqrt{-5}\right]$ is in Integral domain which is not a UFD.

Ans. $46 \in z\left[\sqrt{5}\right]$ is a non unit, non zero element. We can express it as product of two irreducible in two ways.

$46 = 2.23$

$46 = (1+3\sqrt{-5})(1-\sqrt{-5})$

But 2 is not an associate of $1+3\sqrt{-5}$ or $1-3\sqrt{-5}$. Hence $z(F5)$ is not UFD.

Problems 6. Show that $2x + 1$ is a unit in $z_4(x)$

Sol. Since $(2x + 1)(2x + 1) = 0x^2 + 0x + 1 = 1$

$[4 = 0$ in $z_4]$

We find $2x + 1$ is a unit in $z_4(x)$

Problems 7. Show that the polynomial $f(x) = x^2 - 2x - 15$ is both primitive as well as irreducible over z.

Ans. Consider

$$c(f) = gcd\ (1, 2, -15) = 1$$

also $x^2 - 2x - 15 = (x - 5)(x + 3)$

However, the polynomial $x^2 - 2$ is primitive as well as irreducible over z.

Check Your Progress

1. What is a commutative ring?
2. What is a polynomial ring?

14.4 ANSWERS TO CHECK YOUR PROGRESS QUESTIONS

1. A commutative ring is a ring in which the multiplication operation is commutative.
2. A polynomial ring formed from the set of polynomials in one or more indeterminates with coefficients in another ring, often a field.

NOTES

14.5 SUMMARY

- Let $R[x]$ be the ring of polynomials over a ring R then R is commutative iff $R[x]$ is commutative and R has unity iff $R[x]$ has unity.
- **L**et R be a commutative ring with unity such that $R[x]$is a PID, then R is a field.

14.6 KEY WORDS

- **Polynomial:** an expression of more than two algebraic terms, especially the sum of several terms that contain different powers of the same variable(s).
- **Degree:** The degree of a polynomial is the highest degree of its monomials with non-zero coefficients.
- **Zero polynomial:** The zero polynomial is the additive identity of the additive group of polynomials. The degree of the zero polynomial is undefined.
- **Ring:** A ring is one of the fundamental algebraic structures used in abstract algebra. It consists of a set equipped with two binary operations that generalize the arithmetic operations of addition and multiplication.
- **Commutative ring:** A commutative ring is a ring in which the multiplication operation is commutative.
- **Polynomial ring**: A polynomial ring formed from the set of polynomials in one or more indeterminates with coefficients in another ring, often a field.

14.7 SELF ASSESSMENT QUESTIONS AND EXERCISES

Short Answer Questions

1. Write a short note on polynomial rings.
2. Show that if F is a field, every ideal in $F[x]$ is principal.

Long Answer Questions

1. If R is a commutative ring, show that ch R[x] is same as ch R.
2. Let R be a commutative ring with unity and $< x >$ be a prime ideal of $R[x]$. Show that R must be an integral domain.

NOTES

14.8 FURTHER READINGS

Hungerford, Thomas W. 2003. *Algebra*. Berlin: Springer Science & Business Media.

Khanna, V.K, S.K Bhamri. *A Course in Abstract Algebra*. NOIDA: Vikas Publishing House.

Singh, Surjeet, Qazi Zameeruddin. 2005. *Modern Algebra*. NOIDA: Vikas Publishing House.