ALGEBRA

M.Sc., MATHEMATICS First Year

Semester – I, Paper-I

Lesson Writers

Prof. V. Sambasiva Rao
(Retired Professor)
Department of Mathematics
University College of Sciences
Acharya Nagarjuna University

Dr. K. Siva Prasad
Department of Mathematics
University College of Sciences
Acharya Nagarjuna University

Dr. T. Srinivasa Rao
Department of Mathematics
Bapatla Engineering College
Bapatla

Dr. Noorbhasha Rafi
Department of Mathematics
Bapatla Engineering College
Bapatla

.

Editor:
Prof. R. Srinivasa Rao
Department of Mathematics
University College of Sciences
Acharya Nagarjuna University.

Director, I/c
Prof. V.VENKATESWARLU
MA., M.P.S., M.S.W., M.Phil., Ph.D.
CENTRE FOR DISTANCE EDUCATION
ACHARAYANAGARJUNAUNIVERSITY
NAGARJUNANAGAR – 522510
Ph:0863-2346222,2346208,
0863-2346259(Study Material)
Website: www.anucde.info
e-mail:anucdedirector@gmail.com

M.Sc., MATHEMATICS - ALGEBRA

First Edition 2025

No. of Copies :

This book is exclusively prepared for the use of students of M.SC.(Mathematics**)**
Centre for Distance Education, Acharya Nagarjuna University and this book is meant for limited Circulation only.

Published by:
Prof. V.VENKATESWARLU,
Director,I/C
Centre for Distance Education,
Acharya Nagarjuna University

Printed at:

FOREWORD

Since its establishment in 1976, Acharya Nagarjuna University has been forging ahead in the path of progress and dynamism, offering a variety of courses and research contributions. I am extremely happy that by gaining 'A^{+}' grade from the NAAC in the year 2024, Acharya Nagarjuna University is offering educational opportunities at the UG, PG levels apart from research degrees to students from over 221 affiliated colleges spread over the two districts of Guntur and Prakasam.

The University has also started the Centre for Distance Education in 2003-04 with the aim of taking higher education to the doorstep of all the sectors of the society. The centre will be a great help to those who cannot join in colleges, those who cannot afford the exorbitant fees as regular students, and even to housewives desirous of pursuing higher studies. Acharya Nagarjuna University has started offering B.Sc., B.A., B.B.A., and B.Com courses at the Degree level and M.A., M.Com., M.Sc., M.B.A., and L.L.M., courses at the PG level from the academic year 2003-2004 onwards.

To facilitate easier understanding by students studying through the distance mode, these self-instruction materials have been prepared by eminent and experienced teachers. The lessons have been drafted with great care and expertise in the stipulated time by these teachers. Constructive ideas and scholarly suggestions are welcome from students and teachers involved respectively. Such ideas will be incorporated for the greater efficacy of this distance mode of education. For clarification of doubts and feedback, weekly classes and contact classes will be arranged at the UG and PG levels respectively.

It is my aim that students getting higher education through the Centre for Distance Education should improve their qualification, have better employment opportunities and in turn be part of country's progress. It is my fond desire that in the years to come, the Centre for Distance Education will go from strength to strength in the form of new courses and by catering to larger number of people. My congratulations to all the Directors, Academic Coordinators, Editors and Lesson-writers of the Centre who have helped in these endeavors.

Prof. K.GangadharaRao

M.Tech.,Ph.D.,
Vice-Chancellor I/c
Acharya Nagarjuna University

M.Sc. – Mathematics Syllabus

SEMESTER-I

101MA24: ALGEBRA

Unit-I: Group theory: Definition of a Group - Some Examples of Groups - Some Preliminary Lemmas - Subgroups - A Counting Principle - Normal Subgroups and Quotient Groups - Homomorphisms– Automorphisms. (2.1 to 2.8 of the prescribed book [1]).

Unit-II: Group Theory Continued: Cayley's theorem - Permutation groups-Another counting principle - Sylow's theorem. (2.9 to 2.12 of the prescribed book [1]).

Unit-III: Direct products - finite abelian groups; Ring Theory: Definitions and Examples of Rings - some special classes of rings-Homomorphisms - Ideals and quotient Rings (2.13 to 2.14 and 3.1 to 3.4 of the prescribed book [l]).

Unit-IV: Ring Theory Continued: More Ideals and quotient Rings - The field of quotients of an Integral domain -Euclidean rings- A particular Euclidean ring-Polynomial Rings - Polynomials over the rational field. (3.5 to 3.10 of the Prescribed book [l]).

Unit-V: Polynomial Rings over Commutative Rings; Vector Spaces: Elementary Basic Concepts - Linear Independence and Bases - Dual spaces. (3.11 and 4.1 to 4.3 of the prescribed book [1]).

PRESCRIBED BOOK:

I.N. Herstein, ‘Topics in Algebra’, Second Edition, John Wiley & Sons, 1999.

REFERENCE BOOKS:

1) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.

2) Thomas W. Hungerford, ‘Algebra’, Springer- Verlag, New York, 1974.

3) Serge Lang, ‘Algebra’, Revised Third Edition, Springer-Verlag, New York, 2002.

CODE: 101MA24

M.Sc DEGREE EXAMINATION
First Semester
Mathematics::Paper I – ALGEBRA

MODEL QUESTION PAPER

Time : Three hours **Maximum : 70 marks**

Answer ONE question from each Unit. **(5 x 14 = 70)**

UNIT - I

1. (a) State and prove Lagrange's theorem on groups.
   (b) If G is a group and H,K are two subgroups of G then show that HK is a subgroup of G if and only if HK = KH

OR

2. (a) Let G be any group, g is a fixed element of G. Define ϕ: G→G by $\phi(x) = gxg^{-1}$. Then prove that ϕ is an isomorphism of G onto itself.
   (b) State and prove Cauchy's theorem for abelian groups.

UNIT – II

3. (a) State and prove Caylay's theorem.
   (b) If $O(G) = p^2$ where p is a prime number then prove that G is abelian.

OR

4. (a) If $O(G) = p^n$; where p is a prime number, then prove that $Z(G) \neq (e)$.
   (b) If p is a prime number and $p \mid O(G)$ then prove that G has an element of order p.

UNIT – III

5. (a) Let G be a group and suppose that G is the internal direct product of $N_1, N_2, \ldots, N_n$. Let $T = N_1 \times N_2 \times \ldots \times N_n$. Then prove that G and T are isomorphic.
   (b) If G and G' are isomorphic abelian groups, then prove that for every integer s, G(s) and G'(s) are isomorphic.

OR

6. (a) Prove that a finite integral domain is a field.
   (b) If U and V are ideals of R, let $U+V = \{u + v / u \in U, v \in V\}$ then prove that U+V is also an ideal of R.

UNIT – IV

7. (a) If R is a commutative ring with unit element and M is an ideal of R, the M is a maximal ideal of R if and only if R/M is a field.
   (b) If f(x) and g(x) are primitive polynomials then prove that f(x)g(x) is also a primitive polynomial.

OR

8. (a) Let R be a Euclidean ring and a, b $\in$ R. If b $\neq$ 0 is not a unit in R then prove that d(a) < d(ab).
   (b) State and prove Gauss lemma.

UNIT – V

9. (a) If R is a unique factorization domain then prove that R[x] is also a unique factorization domain.
   (b) If V is a finite dimensional vector space and W is a subspace of V, then prove that W is finite dimensional, dim W $\leq$ dim V and dim(V/W) $\leq$ dim V – dim W.

OR

10. (a) Prove that if V is a finite dimensional vector space over F then any two bases of V have the same number of elements.
    (b) Prove that if V and W are finite dimensional vector spaces of dimensions m and n respectively over F then Hom (V,W) is of dimension mn over F.

CONTENTS

LESSON – 0

PRELIMINARIES

OBJECTIVES:

The objectives of this lesson are to

- define the concept of a group and give certain examples.
- state and prove the Lagrange's theorem on subgroups of a finite group.
- define the cyclic group and their generators and give some examples of cyclic groups.

STRUCTURE :

0.1: INTRODUCTION:

In this lesson we study one of the most important algebraic concepts that of a group. A group is a nonempty set on which a law of composition is defined such that all elements have inverses. For example the set of all non-zero real numbers forms a group under multiplication and the set all real members forms a group under addition. The set of all invertible n x n matrices of real numbers is an important example in which the law of composition is matrix multiplication. Thus the concept of a group and the axioms which define it have a naturality about them.

0.2. GROUPS:

Let A and B be any two sets. Then $A \times B = \{(a, b) / a \in A, b \in B\}$ is called the cartesian product of A and B. For example,

Let $A = \{a_1, a_2, a_3\}$ $B = \{b_1, b_2\}$ then

$A \times B = \{(a_1, b_1), (a_2, b_1), (a_3, b_1), (a_1, b_2), (a_2, b_2), (a_3, b_2)\}$

Also that $A \times \phi = \phi = \phi \times B$.

Any subset of A x B is called a (binary) relation from A to B. For example, Let $R = \{(a_1, b_1), (a_2, b_1), (a_1, b_2)\}$. Then R is a relation from A to B. Any relation from A to itself is called a relation on A.

A relation R on A, where A is a non-empty set, is called an equivalence relation on A if R satisfies

1. reflexive : $(a , a) \in R \quad \forall\, a \in A$
2. symmetric: $(a, b) \in R \Rightarrow (b , a) \in R$
3. transitive : $(a , b) \in R$ and $(b, c) \in R \Rightarrow (a , c) \in R$

If R is an equivalence relation on A and $(a, b) \in R$, we say that a is equivalent to b under R and write $a \sim b$ or aRb: in this notation (1)-(3) become

$a \sim a$
$a \sim b \Rightarrow b \sim a$
$a \sim b$ and $b \sim c \Rightarrow a \sim c$

Let R(~) be an equivalence relation on A. If $a \in A$, the equivalence class of a (denoted $\bar{a}$) is the class of all those elements of A that are equivalent to a; that is, $\bar{a} = \{b \in A / b \sim a\}$. Note that any two equivalent classes are either identical or disjoint. Also note that for any $a \in A$, $\bar{a} \neq \phi$ since a ~ a. Also it is easy to verify that $A = \bigcup_{a \in A} \bar{a}$.

For any non empty set A, a mapping f: A x A $\rightarrow$A is called a binary operation on A. That is, for any two elements a and b in A, there is a unique element associated in A and that unique element will be denoted by f(a, b) or afb. Usually binary operations will be denoted by symbols like +, •, ◊, *, etc. If we say that * is a binary operation on A, this means that, for any element a and b, in this order, in A, there is another element denoted by a * b in A. For example The usual addition '+' and multiplication '•' on the set Z of integers, are binary operations on Z The composition '◊' of mappings on the set of mappings of a given set into itself, the set intersection or the set union on the set of subsets of a given set are familiar examples of binary operations.

0.2.1. Definition: A system (A, *), where A is a non empty set and * is a binary operation on A, is called a semigroup if a*(b*c) = (a*b) *c for all a, b, c ∈ A (associative law).

The set $\mathbb{R}$ of real numbers with usual addition '+' is a semigroup and $\mathbb{R}$ with usual multiplication '•' is a semigroup. But $\mathbb{R}$ with the binary operation defined by a * b = a – b is not a semigroup. (Since 2–(3–1) ≠ (2–3)–1. i.e, * is not associative)

0.2.2. Definition: Let (A, *) be a semigroup. An element e in A is called an identity element if a * e = a = e * a for all a ∈ A.

If a*e = a for all a∈A, then e is called a right identity and if e*a = a for all a ∈ A, then e is called a left identity. If e is a right identity and e^1 is a left identity in a semigroup (A, *), then $e^1 = e^1 * e = e$.

Therefore, it follows that a semigroup can have atmost one identity. A semigroup having identity is called a monoid. The real number 0 is the identity in ($\mathbb{R}$, +) and the real number 1 is the identity in ($\mathbb{R}$, •). If $\mathbb{R}^+$ denote the set of all positive real numbers, then ($\mathbb{R}^+$, +) is a semigroup without identity. So ($\mathbb{R}$, +)and ($\mathbb{R}$, •) are monoids but ($\mathbb{R}^+$, +) is not a monoid.

0.2.3. Definition: Let (A, *) be a semigroup with identity e. An element a in A is said to be invertible if there exists an element b in A such that a*b = e = b*a.

If a*b = e, then b is called a right inverse of a. If b*a = e, then b is called a left inverse of a.

If b is a right inverse of a and b^1 is a left inverse of the same element a that is, (a*b =e and b^1*a=e), then b = e*b = (b^1*a) *b = b^1* (a*b) = b^1*e = b^1. there exists unique b such that a*b = e = b*a = b^1 and hence a is invertible. This implies that if a is invertible, there exists unique b such that a*b = e = b*a and this unique b is called the inverse of a and is denotedby a^{-1}. For example, in the semigroup ($\mathbb{R}$, +), every element is invertible (for any $a \in \mathbb{R}$, –a is the inverse of a). In the semigroup ($\mathbb{R}$, •), 0 is not invertible and every non-zero element is

invertible. In the semigroup ($\mathbb{R}^+ \cup \{0\}$, +), the identity element 0 is the only invertible element. Note that the identity element if it exists, in any semigroup is invertible.

0.2.4. Definition: A system (A, $*$), where A is a non empty set and $*$ is a binary operation on A is called a group if it satisfies the following :

(i) $a*(b*c) = (a*b)*c$ for all $a, b, c \in A$.

(ii) There exists $e \in A$ such that $a*e = a = e*a$ for all $a \in A$.

(iii) To each $a \in A$, there exists $a^{-1} \in A$ such that $a*a^{-1} = e = a^{-1}*a$.

0.2.5. Examples:

(i) ($\mathbb{R}$, +), ($\mathbb{Q}$, +) and ($\mathbb{Z}$, +) are all groups, where + is the usual addition on the set $\mathbb{R}$ of real numbers, on the set $\mathbb{Q}$ of rational numbers and on the set $\mathbb{Z}$ of integers.

(ii) ($\mathbb{R}$, $\bullet$) is not a group, since 0 is not invertible. But if $\mathbb{R}^{|}$ is the set of nonzero real numbers, then ($\mathbb{R}^{|}$, $\bullet$) is a group.

(iii) Let X be any set and S(X) be the set of all bijections of X onto itself. Then (S(x), $\lozenge$) is a group, where $\lozenge$ is the composition of mappings.

(iv) For any set X, let M(X) be the set of all mappings of X into itself. Then (M(X), $\lozenge$) is a semigroup with identity (where the identity mapping is the identity element), but not a group (unless X is a single element set). An element $f \in M(X)$ has a right inverse if and only if f is a surjection(that is, onto map) and f has a left inverse if and only if f is an injection(that is one-one map).

(v) Let A be the set of all 2 x 2 matrices over the real numbers. Then (A, +) is a group, where + is the usual addition of matrices. If A is the set of all non-singularmatrices, then ($A^{|}$, $\bullet$) is a group, where $\bullet$ is the usual multiplication of matrices.

(vi) Let n be any positive integer and $Z_n = \{0, 1, 2, \ldots, n-1\}$. Define

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

Then (Z_n, $+_n$) is a subgroup, which is called the additive group of integers modulo n.

0.2.6. Theorem (Cancellation Laws): Let (G, $*$) be a group and $a, b, c \in G$. Then $a*b = a*c \Rightarrow b = c$ and $b*a = c*a \Rightarrow b = c$

Proof: Since $a \in G$ and G is a group, a^{-1} exists in G.
Consider $a*b = a*c \Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c)$
$\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c \Rightarrow e*b = e*c$, where e is the identity element in G.
$\Rightarrow b = c$
Similarly, by applying a^{-1} from right, we get that $b*a = c*a \Rightarrow b = c$.
The following two results are easy to prove and are left as exercises.

0.2.7. Theorem: Let (G, $*$) be a group. Then the following are true.

(i) The identity element in G is unique.

(ii) For any $a \in G$, the inverse of a in G is unique.

0.2.8. Theorem: Let (G, $*$) be a group and a, b $\in$ G. Then the following hold.

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

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

(3) $a*x = b$ has a unique solution in G.

(That is, there exists unique $x \in G$ such that $a*x = b$)

(4) $y*a = b$ has a unique solution in G.

(5) $a*b = e \Leftrightarrow b = a^{-1} \Leftrightarrow a = b^{-1}$

(6) $a*a = a \Leftrightarrow a = e$.

0.2.9. Definition: A group (G, $*$) is said to be an abelian (commutative) group if $a*b = b*a$ for all a, b $\in$ G.

Examples: (1) ($\mathbb{R}$, +), (Q, +) and ($\mathbb{Z}$, +) are abelian groups where + is the usual addition on the set $\mathbb{R}$ of real numbers, on the set of Q of rational numbers and on the set $\mathbb{Z}$ if integers.

(2) Let A be the set of all 2 x 2 non – singular matrices over the real numbers. Then(A, $\bullet$) is a non abelian group, where $\bullet$ is the usual multiplication of matrices.

0.3. SUBGROUPS:

If (G, $*$) is a group and a, b$\in$G, then we simply write ab for $a*b$. For simplicity, we supress the symbol $*$ which denotes the binary operation. Accordingly we simply say that G is a group, when there is no amiguility about the binary operation with which G is a group. If G is a group with respect to more than one binary operation then we mention the operation also.

0.3.1. Definition: Let G be a group. A nonempty subset H of G is called a subgroup of G if H is a group relative to the binary operation in G.

For any group G the singleton {e} and G itself are subgroups of G, called trivial subgroups. A subgroup H of G is said to be a proper subgroup if $H \neq \{e\}$, $H \neq G$. It is easy to see that the identity element of a subgroup of a group must be same as that of the group.

0.3.2. Theorem: Let G be a group. A non empty subset H of G is a subgroup of G if and only if for any a, b $\in$ H, ab $\in$ H and $a^{-1} \in H$.

Proof: Let H be a nonempty subset of G. If H is a subgroup of G, then obviously the implies condition is true. Conversely suppose that H satisfies for any a, b $\in$ H, ab $\in$ H and $a^{-1} \in H$. Then for any a $\in$ H, $a^{-1} \in H$. Hence, $e = aa^{-1} \in H \Rightarrow e \in H$.
Therefore H is a subgroup. Hence the result is true.

0.3.3. Theorem: Let G be a group. A nonempty subset H of G is a subgroup of G if and only if for any a, b $\in$ H, $ab^{-1} \in H$.

Proof: Let H be a non empty subset of G. If H is a subgroup of G, then obviously the implies condition is true. Conversely suppose that for any a, b $\in$ H, $ab^{-1} \in H$. Let a, b $\in$ H. Then by our supposition, $e = bb^{-1} \in H$. Hence $b^{-1} = ab^{-1} \in H$. Therefore, $ab = a(b^{-1})^{-1} \in H$. Hence H is a subgroup of G.

0.3.4. Theorem: Let H be a non-empty finite subset of a group G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof: Given that H is a non-empty finite subset of G. So write $H = \{a_1, a_2, \ldots, a_n\}$ for some positive integer n. Suppose H is a subgroup of G. Now we will show that for any $a, b \in H$, $ab \in H$.

Let $a, b \in H$. Then $aa^{-1} \in H$, $a \in H$ and $b \in H$.

$\Rightarrow e \in H$, $a \in H$ and $b \in H$.

$\Rightarrow b^{-1} = eb^{-1} \in H$ and $a \in H$.

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

So for any $a, b \in H$, we have $ab \in H$.

Conversely suppose that $ab \in H$ for any $a, b \in H$. Consider the set $Ha_1 = \{a_i a_1 / 1 \leq i \leq n\}$. By hypothesis, Ha_1 is a subset of H having the same number of elements as in H (for $a_i a_1 = a_j a_1 \Rightarrow a_i = a_j$ by 0.2.6). Therefore $Ha_1 = H$ and hence $a_1 \in H = Ha_1$; that is $a_1 = a_i a_1$ for some i. Now $ea_1 = a_1 = a_i a_1$ and hence $e = a_i \in H = Ha_1$, which again imples that $e = a_j a_i$ and hence $a_1^{-1} = a_j \in H$. Similarly $a_i^{-1} \in H$ for $2 \leq i \leq n$ therefore $a^{-1} \in H$ whenever $a \in H$. Now $e \in H$ and for any $a \in H$, we have $a^{-1} \in H$. Hence H is a subgroup of G.

The above theorem fails if H is infinite. For the set Z^+ of positive integers is a subset of the group (Z, +) satisfying the property that $a + ba^{-1} \in Z^+$ for $a, b \in Z^+$; but Z^+ is not a subgroup of (Z, +).

0.3.5. Theorem: Let G be a group. Then the intersection of any family of subgroups of G is again a subgroup of G. The union of a family of subgroups of G may not be a subgroup of G.

Proof: It is easy to verify that the intersection of any family of subgroups is again a subgroup. Regarding unions consider

$2Z = \{2a / a \in Z\}$ and $3Z = \{3a / a \in Z\}$

Then 2Z and 3Z are subgroups of the group (Z, +).But $3, 2 \in 2Z \cup 3Z$ and $3 - 2 \notin 2Z \cup 3Z$.

0.3.6. Self assessment Questions:

Let H and K be a subgroup of a group G. Then prove that

1. $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.
2. The product $HK = \{ab / a \in H \text{ and } b \in K\}$ is a subgroup of G if and only if HK = KH.

0.3.7. Definition: Let G be a group and X be a subset of G. Then the intersection of all subgroups of G containing X is the smallest subgroup of G containing X and is denoted by $\langle X \rangle$. If X consists only one element say a, then we write $\langle a \rangle$ for $\langle \{a\} \rangle$. $\langle X \rangle$ is called the subgroup generated by X : a is called a generator for $\langle a \rangle$ and X is called generating set for $\langle X \rangle$.

0.3.8. Theorem (1): For any nonempty subset X of a group G,

$\langle X \rangle = \{a_1 . a_2 \ldots\ldots a_n / \text{ for each i ; either } a_i \in X \text{ or } a_i^{-1} \in X; n \geq 1\}$

(2) For any element a of a group G, $\langle a \rangle = \{a^n / n \in Z\}$ where a^n is defined inductively by

$$a^n = \begin{cases} e \text{ if } n = 0 \\ a^{n-1}.a \text{ if } n > 0 \\ (a^{-1})^{-n} \text{ if } n < 0 \end{cases}$$

Proof: (1) Let A = { a_1. a_2..... a_n / for each i ; either $a_i \in X$ or $a_i^{-1} \in X$; $n \geq 1$}
It can be easily observed that $xy \in A$ whenever $x, y \in A$.
Also $(a_1. a_2..... a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}. . . . . a_2^{-1}a_1^{-1}$. Therefore A is a subgroup of G
Clearly $X \subseteq A$ and if H is any subgroup of G such that $X \subseteq H$, then $A \subseteq H$. Thus A is the smallest subgroup of G containing X and hence A = <X>.

(2) This follows from (1) and the definition of a^n for any $n \in Z$.
For $x \in \langle a \rangle \Leftrightarrow x = a_1 a_2..... a_n$, where for each i, $a_i \in \{a\}$ or $a_i^{-1} \in \{a\}$.
$\Leftrightarrow x = a^{\epsilon_1}, a^{\epsilon_2}, ..., a^{\epsilon_n}$ where each $\epsilon_i = \pm 1$.
$\Leftrightarrow x = a^m$, where $m = \epsilon_1 + \epsilon_2 + ... + \epsilon_n \in Z$.

0.4. LAGRANGE'S THEOREM:

In this section, we shall prove one of the most useful theorem due to Lagrange. If G is a finite group, then the number of elements in G is called the order of G and is denoted by O(G). The Lagrange's theorem states that, if H is a subgroup of a finite group G, then the order of H divides the order of G. Before going to the proof of this, first let us have the following.

0.4.1. Definition: Let H be a subgroup of a group G. For any $a \in G$, let $aH = \{ah / h \in H\}$ and $Ha = \{ha / h \in H\}$

aH is called the left coset of H corresponding to a in G and H is called the right coset of H corresponding to a in G.

0.4.2. Theorem: Let H be a subgroup of a group G. Then any two left (right) cosets of H in G are either equal or disjoint. If H is finite, then the number of elements in a left (right) coset of H is equal to O(H).

Proof: Let $a, b \in G$. Suppose $aH \cap bH \neq \phi$. Choose $x \in aH \cap bH$. Then $ah_1 = x = bh_2$ for some $h_1, h_2 \in H$.
Then $a^{-1}b = h_1 h_2^{-1} \in H$. Now $y \in aH \Rightarrow y = ah$ for some $h \in H$.
$\Rightarrow y = b(b^{-1}a)h \in bH$
This shows that $aH \subseteq bH$.
Now $y \in bH \Rightarrow y = bH$ for some $h \in H$.
$\Rightarrow y = a(a^{-1}b)h \in aH$.
This shows that $bH \subseteq aH$.
Thus $aH = bH$. That is, if aH and bH are not disjoint, then aH = bH. On the same lines, we can prove that Ha and Hb are either equal or disjoint. The mapping $h \rightarrow ah$ is a bijection of H onto aH and therefore when H is finite, aH is also finite and hence H and aH have the same number of elements. Similarly we can prove the theorem for right cosets also.

0.4.3. Theorem(Lagrange's theorem): Let H be a subgroup of a finite group G. Then O(H) divides O(G).

Proof: Each element $a \in G$ is in the corresponding left coset aH (Since $a = at\ e \in aH$). Therefore by theorem 0.4.2, the left cosets aH form a partition of G. That is any two left cosets of H in G are equal or disjoint and $G = \bigcup_{a \in G} aH$ Since G is finite, the number of left cosets of H in G is finite. So let $a_1H, a_2H, ..., a_nH$ be all the distinct left cosets of H in G.

Then $G = a_1H \cup a_2H \cup \ldots \cup a_nH$ and $(a_iH) \cap (a_jH) \neq \emptyset$ for $i \neq j$.

Therefore, $O(G) = \sum_{i=1}^{n} |a_iH| = \sum_{i=1}^{n} O(H) = n(OH)$, since $|a_iH| = O(H)$. Thus O(H) divides O(G) and $\frac{O(G)}{O(H)} = n$, the number of left cosets of H in G.

0.4.4. Corollary: If H is a subgroup of a finite group G, then the number of left cosets of H in G is equal to the number of right cosets of H in G and this number is equal to $\frac{O(G)}{O(H)}$.

Proof: In the proof of 0.4.3, n is the number of left cosets of H in G and $n = \frac{O(G)}{O(H)}$. The same argument is valid, if we consider right cosets.

0.4.5. Definition: Let H be a subgroup of a group G. Then the index of H in G is defined as the number of left(right) cosets of H in G and is denoted by [G:H] or $i_G(H)$ if it is finite. If G is a finite group, then $[G:H] = \frac{O(G)}{O(H)}$.

This definition may be extended to infinite groups. Let H be a subgroup of a group G (finite or infinite). If $\mathbb{R}$ is the set of distinct right cosets of H in G, and L is the set of distinct left cosets of H in G, then the cardinal number $\mathbb{R}$ of the set $\mathbb{R}$ is equal to the cardinal number $|\mathcal{L}|$ of the set $\mathcal{L}$; i.e, $|\mathbb{R}| = |\mathcal{L}|$, for the map $\mathbb{R} \to \mathcal{L}$ given by $Ha \to a^{-1}H$ is a bijection since Ha = Hb

$\Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H$.

The index of H in G, denoted by [G : H] is the cardinal number of the set of distinct left cosets of H in G. It is true that $|G| = [G:H]\ |H|$. The index of H in G may be finite with out G or H being finite. For, consider the group (Z, +) of integers. Let n be a positive integer and $H = nZ = \{na / a \in Z\}$. Then it is easy to verify that H, 1+H, 2+H, ..., (n–1)+H are all the distinct left cosets of H and hence H is of index n in Z.

0.4.6. Self Assessment question: Let $X = \{1, 2, 3\}$. Let S_3 be the group of all bijections on X; with the binary operation composition of mappings. Define $\phi : X \to X$ as $\phi(1) = 2$, $\phi(2) = 1$, $\phi(3) = 3$. Then $\phi^2 = I$, where I is the identity mapping on X. Prove that $H = \{I, \phi\}$ is a subgroup S_3. Compute all the left and right cosets of H in G and observe that, though their number is the same, they are different.

0.4.7. Theorem: Let H be a subgroup of a group G. For any a, b∈G, define a relation by $a \sim b \Leftrightarrow a^{-1}b \in H$. Then $\sim$ is an equivalence relation on G whose equivalence classes are precisely the left cosets of H in G.

Proof: Since H is a subgroup of G, H should contain the identity element of G. For any $a \in G$, we have $a^{-1}a = e$ and hence $a \sim a$. Therefore $\sim$ is reflexive.

$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H \Rightarrow b \sim a$. Therefore $\sim$ is symmetric.

Also $a \sim b$ and $b \sim c \Rightarrow a^{-1}b$ and $b^{-1}c \in H$

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

hence $\sim$ is transitive. Thus $\sim$ is an equivalence relation on G. Further, for any $a \in G$,

$a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH$

Hence aH is the equivalence class containing a with respect to the relation $\sim$.

0.4.8. Self assessment question: For any subgroup H of a group G, define a relation $\sim$ on G by $a \sim b \Leftrightarrow ab^{-1} \in H$.

Prove that $\sim$ is an equivalence relation on G whose equivalence classes are precisely the right cosets of H in G.

0.5. CYCLIC GROUPS:

For any element a in group G , we have constructed the subgroup $< a >$ generated by a in G (see 0.3.6). $< a >$ is called a cyclic subgroup of G.

0.5.1.Definition: A group G is called a cyclic group if there exists $a \in G$ such that $G = < a > = \{a^n / n \in Z\}$.

In this case, G is said to be generated by a and a is called a generator of G. If + is the binary operation on a group, it is conventional to write na for a^n: that is

$$na = \begin{cases} 0, \text{the } identity, if\ n = 0 \\ (n-1)a + a\ if\ n > 0 \\ (-n)(-a) if\ n < 0 \end{cases}$$

0.5.2. Examples:

(1) The group (Z, +) of integers is cyclic group, Since $Z = < 1 > = < -1 >$. Hence both 1 and -1 are generators for this cyclic group.

(2) For any positive integer n, consider the additive group Z_n of integers modulo n(see 0.2.5 (vi)). Recall that $Z_n = \{ 0, 1, 2, \ldots\ldots, n-1\}$.

Here the operation is addition modulo n, denoted by $+_n$. Note that $1 +_n 1 = 2$, $2 +_n 1 = 3$, ..., $(n-2) +_n 1 = n-1$ and $(n-1) +_n 1 = 0$, $0 +_n 1 = 1$,.....

By adding 1 to each element $0 \leq a < n-1$ in Z_n, we are getting the next element $a +_n 1$ in Z_n and by adding 1 to n-1 we get 0. This is the lesson for calling it a cyclic group. Z_n is a cyclic group generated by 1 whose order is n

0.5.3. Theorem: Let G be an infinite cyclic group. Then the following hold.

1) $x^n = e \Leftrightarrow x = e$ or $n = 0$, for any $x \in G$.
2) For any $x \in G$, $x^n = x^m \Leftrightarrow n = m$ or $x = e$.
3) There are exactly two generators for G.

Proof: Since G is a cyclic group, there exists $a \in G$ such that $G = < a > = \{ a^n / n \in Z\}$.

We shall first prove that $a^n \neq e$ for all $n \neq 0$. If possible suppose that $a^n = e$ for some $n \neq 0$.We can assume that n is positive (Since $a^n = e$ if and only if $a^{-n} = e$). Then by the division algorithm any integer m can be written as $m = nq + r$ for some q, $r \in Z$ write $0 \leq r < n$ and hence $a^m = a^{nq+r} = a^{nq}.a^r = (a^n)^q.(a^r) = e^q.a^r = a^r$.

This imples that $G = \{a^r / 0 \leq r < n\}$ which is a contradiction for the hypothesis that G is infinite.

Thus $a^n \neq e$ for all $n \neq 0$.

(1) If $x = e$ or $n = 0$, then clearly $x^n = e$.

Conversely, suppose $x \in G$ and $x^n = e$. We can write $x = a^m$ for some $m \in Z$. Now $a^{mn} = x^n = e$ and hence, by the above observation, $mn = 0$ so that $m=0$ or $n = 0$.Therefore $x = e$ or $n = 0$.

(2) This follows from (1) and from the fact that $x^n = x^m$ if and only if $x^{n-m} = e$.

(3) We have that a is a generator of G. Suppose b is another generator of G. Then $< a > = G = < b >$.

So that $a = b^n$ and $b = a^m$ for some integers m and n. Then $a^1 = a = b^n = (a^m)^n = a^{mn}$
and therefore by(2), $mn = 1$ which implies that $m = 1 = n$ or $m = -1 = n$.
From this it follows that $m = 1$ or -1 and hence $b = a$ or $b = a^{-1}$.Thus a and a^{-1} are the only generators of G. Also, note that $a \neq a^{-1}$ and $< a > = < a^{-1} >$. Thus G has exactly two generators.

0.5.4. Theorem: Let G be a finite cyclic group of order $n > 1$. Then the following hold.
(1) If a is a generator of G, then $G = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$ and n is the least positive integer such that $a^n = e$.
(2) For any generator a of G and for any integer m, $a^m = e \Leftrightarrow$ n divides m.
(3) The number of generators of G is equal to $\phi(n)$, the number of positive integers less than n and relatively prime to n.

Proof: (1) Let a be a generator of G. Then $a \neq e$ (Since $O(G) > 1$) and $G = < a > = \{a^m / m \in Z\}$.
Since G is finite and Z is infinite, we should have $a^m = a^t$ for some $m < t$. Then $a^{t-m} = e$ and $t-m$ is a positive integer. Let s be the smallest positive integer such that $a^s = e$. Then $a^i \neq a^j$ for all $0 \leq i \neq j \leq s-1$ and $G = \{e, a, a^2, \ldots\ldots, a^{s-1}\}$ (See the discussion in the beginning of the proof of 0.5.3). Since $O(G) = n$, it follows that $s = n$ and $G = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$.

(2) Let a be a generator of G. Then by(1), $a^n = e$ and hence $(a^n)^q = e$ for all integers q. This implies that $a^m = e$ whenever n divides m. On the other hand, suppose $a^m = e$. Then by the division algorithm, m can be written as $nq + r$ for some $q, r \in Z$ with $0 \leq r < n$. Now $e = a^m = a^{nq+r} = (a^n)^q a^r = a^r$. Since n is the last positive integer such that $a^n = e$ and since $a^r = e$ and $0 \leq r < n$, it follows that $r = 0$ and $m = nq$. Thus n divides m.

(3) We shall prove that for any $0 < r < n$, a^r is a generator of G if and only if r is relatively prime to n.
Let $0 < r < n$. Suppose a^r is a generator of G. Then $< a^r > = G = < a >$.
Hence $a = (a^r)^s$ for some integer s, so that $a^{rs-1} = e$. By (2) n divides $rs-1$ and therefore $nt = rs - 1$ for some integer t so that $rs - nt = 1$. From this it follows that r and n are relatively prime.
Conversely, suppose that r and n are relatively prime. Then there exist integers s and t such that $rs - nt = 1$ and hence $a = a^{rs-nt} = (a^r)^s(a^n)^{-t} = (a^r)^s$ which implies that $a \in < a^r >$.
Therefore $< a > \subseteq < a^r > \subseteq G = < a >$ and hence $G = < a^r >$. So that a^r is a generatorof G. Also note that $a^r \neq a^s$ for any $0 < r, s < n$. Thus the number of generators of G is equal to the number of positive integers less than n and relatively prime to n.

0.5.5. Definition: Let G be a group and $a \in G$. If there exists an integer $n \neq 0$ such that $a^n = e$, then we say that the order of a is finite. In this case, if m is the least positive integer such that $a^m = e$, then m is called the order of a , written O(a). If no such integer n exists, then a is said to be of infinite order.

0.5.6.Corollary: Let G be a group and $a \in G$. Then

(i) $a^n = e$ for integer $n \neq 0 \Leftrightarrow O(a)$ divides n.

(ii) $< a >$ is of order $m \Leftrightarrow O(a) = m$.

Proof: (i) follows from 0.5.4(2), while (ii) follows from 0.5.4(1)

0.6 MODEL EXAMINATION QUESTIONS:

0.6.1. Let $(G, *)$ be a group. Then the following are true.
(i) The identity element in G is unique.
(ii) For any $a \in G$, the inverse of a in G is unique.

0.6.2. Let G be a group. A nonempty subset H of G is a subgroup of G if and only if for any $a, b \in H$, $ab^{-1} \in H$.

0.6.3. Let H be a subgroup of a finite group G. Then O(H) divides O(G).

0.7 SUMMARY:

In this lesson we have introduced the concept of a group and certain examples of groups have been given. Also we have defined the subgroup of a group and some elementary properties of subgroups have been presented. Also we have introduced the concept of a coset of a subgroup and proved Lagrange's theorem. Further we have learnt the concept of a cyclic group and order of an element of a group and certain important properties of these have been proved.

0.8 TECHNICAL TERMS:

- Semi group
- Group
- Sub group
- Subgroup generated by a set
- Cosets of subgroups of a set
- Index of a subgroup
- Cyclic groups
- Order of an element of a group.

0.9 ANSWERS TO SELF ASSESSMENT QUESTIONS:

0.3.6. (1) Assume that $H \cup K$ is a subgroup of G. If possible suppose that $H \not\subset K$ and $K \not\subset H$. Then there exists elements $a \in H\text{-}K$ and $b \in K\text{-}H$. Now $a, b \in H \cup K$. By assumption, $ab \in H \cup K$. If $ab \in H$, then $b = a^{-1}ab \in H$; a contradiction. On the other hand if $ab \in K$, then $a = bb^{-1} \in K$, again a contradiction therefore either $H \subseteq K$ or $K \subseteq H$. Converse is trivial.

(2) Suppose HK = KH. HK is nonempty, since $e \in HK$. Let $a, b \in HK$. Then $a = h_1 k_1$, $b = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 y_1 h_2^{-1}$, where $y_1 = k_1 k_2^{-1} \in K$. Now $y_1 h_2^{-1} \in KH = HK$. Hence $y_1 h_2^{-1} = x_1 y_2$ for some $x_1 \in H$ and $y_2 \in K$. Therefore $ab^{-1} = h_1 x_1 y_2 = x_2 y_2$ where $x_2 = h_1 x_1 \in H$. Hence $ab^{-1} \in HK$. Thus HK is a subgroup. Conversely suppose that HK is a subgroup. Let $a \in KH$. Then $a = kh$ for some $k \in K$ and $h \in H$. Now $a^{-1} = h^{-1}k^{-1} \in HK \Rightarrow a \in HK$ (Since HK is a subgroup) This implies $KH \subseteq HK$. Next let $b \in HK$. Then $b^{-1} \in HK$. This implies $b^{-1} = xy$ for some $x \in H$, $y \in K \Rightarrow$

$b = y^{-1}x^{-1} \in KH$. Thus $HK \subseteq KH$. Hence $HK = KH$.

0.4.6. Given that $X = \{1, 2, 3\}$ and S_3 be the group of all bijections on X; with the binary operation composition of mappings.
Then $S_3 = \{I, \phi, \psi, \psi^2, \phi\psi, \psi\phi\}$ Where $\phi : X \to X$ defined by $\phi(1) = 2$, $\phi(2) = 1$, $\phi(3) = 3$ and $\psi(1) = 2$, $\psi(2) = 3$, $\psi(3) = 1$ and I is the identity mapping on X. Note that $\phi\psi = \psi^1\phi$, $\phi^2 = I$ and $\psi^3 = I$. First we show that $H = \{I, \phi\}$ is a subgroup of S_3 clearly I is the identity element in S_3 and hence in H also. Consider $\phi^2 = I \in H$ .Therefore H is a subgroup of S_3. Note that $H = \{I, \phi\}$, $H\psi = \{\psi, \phi\psi\}$, $H\psi^2 = \{\psi^2, \phi\psi^2\}$, are distinct right cosets of H in S_3 ($\because \phi\psi^2 = \psi\phi \in S_3$). And $H = \{I, \phi\}$, $\psi H = \{\psi, \psi\phi\}$, $\psi^2 H = \{\psi^2, \psi^2\phi\}$, are distinct left cosets of H in S_3 ($\because \phi\psi^2 = \phi\psi \in S_3$).

0.4.8. Proof is similar to that of 0.4.7.

0.10 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.V. Samba Siva Rao

LESSON -1

NORMAL SUBGROUPS AND QUOTIENT GROUPS

OBJECTIVES:

The objectives of this lesson are to

- define the concept of a normal subgroup of a group.
- prove some equivalent conditions to normal subgroups.
- prove the set of all right cosets of a normal subgroup is a group; which is called the quotient group.

STRUCTURE:

1.1: INTRODUCTION:

Normal subgroups are a special kind of subgroups and these facilitate the construction of quotient groups. In this lesson we shall introduce the concept of a normal subgroup of a group and prove some theorems related to normal subgroups. Also we show that the set of all right cosets of a normal subgroup of a group is a group.

1.2: NORMAL SUBGROUPS:

1.2.1. Definition: A subgroup N of a group G is said to be a normal subgroup of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Equivalently, N is a normal subgroup of G if and only if $gNg^{-1} \subseteq N$, for every $g \in G$, where $gNg^{-1} = \{gng^{-1} / n \in N\}$

Trivially the subgroups {e} and G itself are normal subgroup of G.

1.2.2. Example: In S_3, $N = \{I, \psi, \psi^2\}$ is normal subgroup of S_3 (For S_3, See 0.4.6)

1.2.3. Theorem: Let G be a group. A subgroup N of G is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.

Proof: Let N be a subgroup of G. Suppose that N is a normal subgroup of G. Then for $g \in G$, $gNg^{-1} \subseteq N$ and $g^{-1}N(g^{-1})^{-1} \subseteq N$ (Since $g^{-1} \in G$)
$\Rightarrow gNg^{-1} \subseteq N$ and $g^{-1}Ng \subseteq N$ for any $g \in G$.
Since $g^{-1}Ng \subseteq N$ for any $g \in G$, $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1} \subseteq N \Rightarrow N = gNg^{-1}$ for any $g \in G$.
Conversely suppose that $N = gNg^{-1}$ for any $g \in G$. Then $gNg^{-1} \subseteq N$ for any $g \in G$ and hence N is a normal subgroup of G.

1.2.4. Theorem: Let N be a subgroup of a group G. Then N is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

Proof: Given that N is a subgroup of a group G. Suppose N is a normal subgroup of G. Now we show that every left coset of N in G is a right coset of N in G. Let $g \in G$.Then gN is a left coset of N in G**.**
Now we show that gN = Ng.
Since N is a normal subgroup of G, $gNg^{-1} \subseteq N$ and $g^{-1}Ng \subseteq N$.
Let $x \in gN \Rightarrow x = gn$ for some $x \in N$.
Now $gng^{-1} \in gNg^{-1} \subseteq N \Rightarrow gng^{-1} \in N \Rightarrow gng^{-1}g \in Ng$.
$\Rightarrow gne \in Ng \Rightarrow gn \in Ng \Rightarrow x \in Ng$.
This shows that $gN \subseteq Ng$. Now let $y \in Ng \Rightarrow y = mg$ for some $m \in N$. Since $gNg^{-1} \subseteq N$, we have
$g^{-1}mg \in N \Rightarrow g^{-1}mg \in N \Rightarrow gg^{-1}mg \in gN \Rightarrow emg \in gN \Rightarrow mg \in gN \Rightarrow y \in gN$. This shows that $Ng \subseteq gN$ and hence gN = Ng.
Thus every left coset of N in G is a right coset of N in G
Conversely suppose that every left coset of N in G is a right coset of N in G. Now we will show that N is a normal subgroup of G. That is, for any $g \in G$, we will show that $gng^{-1} \in N \; \forall$ $n \in N$. Let $g \in G$.Then gN is a left coset of N in G. By our assumption, gN is a right coset of N in G. So gN = Nh for some $h \in G$. Now $g = ge \in gN \Rightarrow g \in Nh$.
But $g = eg \in Ng$. $\therefore g \in Nh \cap Ng \Rightarrow Nh \cap Ng \neq \phi$.
Since any two right cosets are either disjoint or equivalent and since $Nh \cap Ng \neq \phi$, we have Ng = Nh. $\therefore gN = Nh = Ng$.
Now for any $n \in N$, $gng^{-1} \in gNg^{-1} = Ngg^{-1} = N$
$\Rightarrow gng^{-1} \in N$ for all $n \in N \Rightarrow gNg^{-1} \subseteq N$.
Therefore, $gNg^{-1} \subseteq N \; \forall \; g \in G$ and hence N is a normal subgroup of G.

1.2.5. Self assessment question: A subgroup N of a group G is normal if and only if every right coset of N in G is a left coset of N in G.
Note that if G is abelian, then every subgroup of G is normal.

1.2.6. Problem: If G is a group and H is a subgroup of index 2 in G, prove that H is a normal subgroup of G.

Solution: Suppose G is a group and H is a subgroup of index 2 in G. Let $a \in G$, if $a \in H$, then clearly aH = Ha. Assume $a \notin H$. Since H is a subgroup of index 2, we have $G = H \cup aH$ and $H \cap aH = \phi$. Also $G = H \cup Ha$ and $H \cap aH = \phi$. Thus aH = Ha, $a \notin H$. Hence aH = Ha for all $a \in G$.Then by 1.2.4, H is a normal subgroup of G.

1.2.7. Problem: Show that the intersection of two normal subgroups of G is a normal subgroup of G.

Solution: Let H and K be two normal subgroups of a group G. Now we will show that $H \cap K$ is a normal subgroup of G.
Let $g \in G$. Let $h \in H \cap K$. Then $h \in H$ and $h \in K$. Since H and K are normal subgroups of G, we have $ghg^{-1} \in H$ and $ghg^{-1} \in K$. This implies $ghg^{-1} \in H \cap K$. Therefore $ghg^{-1} \in H \cap K$ for all $h \in H \cap K$ and for all $g \in G$. Hence $H \cap K$ is a normal subgroup of G.

1.2.8. Problem: If N is a normal subgroup of a group G and H is any subgroup of G, prove that NH is a subgroup of G.

Solution: Suppose N is a normal subgroup of a group G and H is any subgroup of G. Now we will show that NH is a subgroup of G.
Now NH = {nh / n ∈ N, h ∈ H}.
By 0.3.3, it is enough if we show that $xy^{-1} \in NH$ for any x , y ∈ NH.
Let x , y ∈ NH ⇒x = $n_1 h_1$, y = $n_2 h_2$ for some n_1, $n_2 \in N$ and h_1, $h_2 \in H$. Now $h_1h_2^{-1} \in H$ and $h_1h_2^{-1} \in G$ and $n_2^{-1} \in N$. Since N is a normal subgroup of G, $h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1} \in N$.
Consider $xy^{-1} = n_1h_1(n_2h_2)^{-1} = n_1h_1h_2^{-1}n_2^{-1} = n_1h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1}h_1h_2^{-1} \in NH$.
(Since $n_1h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1} \in N$ and $h_1h_2^{-1} \in H$). Therefore NH is a subgroup of G.

1.2.9. Problem: If H is a subgroup of a group G and N is a normal subgroup of G, show that H ∩ N is a normal subgroup of H.

Solution: Suppose H is a subgroup of G and N is a normal subgroup of G. Now we will show that H∩ N is a normal subgroup of H. Clearly H ∩ N is a subgroup of H. Let h ∈ H. Now for any x ∈ H∩N, consider $hxh^{-1} \in H$ (Since h, x ∈ H). Also $hxh^{-1} \in N$ (Since N is a normal subgroup of G and x ∈ N). Therefore $hxh^{-1} \in H \cap N$ and hence H∩ N is a normal subgroup of H.

1.2.10. Problem: Suppose that N and M are two normal subgroups of G and that N∩ M = (e). Show that for any n ∈ N and m ∈ M, mn = nm.

Solution: Suppose that N and M are two normal subgroups of a group G such that N∩M = (e). Let n∈N and m∈M. Consider $nmn^{-1}m^{-1} \in M$ (Since M is a normal subgroup of G) and $nmn^{-1}m^{-1} \in N$ (Since N is a normal subgroup of G). This implies that $nmn^{-1}m^{-1} \in N \cap M = (e)$ and so $nmn^{-1}m^{-1} = e$.
⇒ $nmn^{-1}e = m \Rightarrow nmn^{-1} = m \Rightarrow nmn^{-1}n = mn$
⇒ nme = mn ⇒ nm = mn.
Thus for any n∈N, m∈M we have mn = nm.

1.2.11. Theorem: A subgroup N of a group G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Proof: Let N be a subgroup of a group G. Suppose N is a normal subgroup of G. Let a, b ∈ G. Consider the right cosets Na and Nb. Since N is a normal subgroup of G**,** by 1.2.4, we have Na = aN. Now Na Nb = N(aN)b = N(Na)b = NNab = Nab (Since N is a subgroup of G, NN = N).
Therefore NaNb = Nab, which is right coset of N in G.
Conversely suppose that the product of two right cosets of N in G is again a right coset of N in G.
Now we show that N is a normal subgroup of G, that is $gNg^{-1} \subseteq N$ for any g ∈ G. Let g ∈ G. By our supposition, $NgNg^{-1}$ = Na for some a ∈ G.
Now $e = ege^{-1} \in NgNg^{-1} = Na \Rightarrow Ne = Na$.
⇒ N = Na. ⇒ $N = NgNg^{-1}$
Now $egNg^{-1} \subseteq NgNg^{-1} = N \Rightarrow gNg^{-1} \subseteq N$
So $gNg^{-1} \subseteq N$ for any g ∈ G and hence N is a normal subgroup of G.

1.3: QUOTIENT GROUPS:

Let N be a normal subgroup of a group G and let G/N denote the collection of all right cosets of N in G. We prove that G/N is a group in the following theorem. G/N is called the quotient group or a factor group of G by N.

1.3.1. Theorem: Let N be a normal subgroup of a group G. Then G/N is also a group.

Proof: Given that N is a normal subgroup of a group G. Consider $G/N = \{Na \mid a \in G\}$.
Define a binary operation $\bullet$ on G/N as follows.
Let $Na, Nb \in G/N$
Define $Na \bullet Nb = Nab$. Now we show that $(G/N, \bullet)$ is a group. First we show that $\bullet$ is well defined.
Let $Na, Nb, Na_1, Nb_1 \in G/N$ such that $Na = Nb$ and $Na_1 = Nb_1$. Then $ab^{-1} \in N$ and $a_1b_1^{-1} \in N$.
Now $a_1b_1^{-1} \in N$ and since N is a normal subgroup of G, $ba_1b_1^{-1}b^{-1} \in N$.
Consider $aa_1(bb_1)^{-1} = aa_1b^{-1}b^{-1}ab^{-1}(ba_1b_1^{-1}b^{-1}) \in N$ (Since $ab^{-1} \in N$ and $ba_1b_1^{-1}b^{-1} \in N$ and N is a subgroup of G).
This implies that $Naa_1 = Nbb_1 \Rightarrow Na \bullet Na_1 = Nb \bullet Nb_1$
So $\bullet$ is a well defined binary operation on G/N. Therefore for any $Na, Nb \in G/N$, $Na \bullet Nb \in G/N$.
Let $Na, Nb, Nc \in G/N$.
Consider $Na \bullet (Nb \bullet Nc) = Na \bullet (Nbc) = Na(bc) = N(ab) \bullet c = Nab \bullet Nc = (Na \bullet Nb) \bullet Nc$.
Therefore $Na \bullet (Nb \bullet Nc) = (Na \bullet Nb) \bullet Nc$ for any $Na, Nb, Nc \in G/N$ and $\bullet$ is associative on G/N. Let $Na \in G/N$. Now $Ne \in G/N$, where e is the identity element in G.
Consider $Na \bullet Ne = Nae = Na$ and $Ne \bullet Na = Nea = Na$.
Therefore Ne is the identity element in G/N.
Let $Na \in G/N$. Now $a^{-1} \in G$ and so $Na^{-1} \in G/N$.
Consider $Na \bullet Na^{-1} = Naa^{-1} = Ne$ and $Na^{-1} \bullet Na = Naa^{-1} = Ne$.
Therefore Na^{-1} is the inverse of N*a* in G/N. Hence $(G/N, \bullet)$ is a group.

1.3.2. Theorem: If G is a finite group and N is a normal subgroup of G, then O(G/N) = O(G)/O(N).

Proof: Suppose G is a finite group and N is a normal subgroup of G. By 0.4.4, the number of right cosets of N in G is equal to O(G)/O(N). Since G/N is the set of all right cosets of N in G, we have O(G/N) = O(G)/O(N).

1.4. MODEL EXAMINATION QUESTIONS:

1.4.1. Define the concept of a normal subgroup of a group. Show that a subgroup N of a group G is normal if and only if $gNg^{-1} = N$ for every $g \in G$.

1.4.2. Show that a subgroup N of a group G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

1.4.3. If G is a group and H is a subgroup of index 2 in G, show that H is a normal subgroup of G.

1.4.4. If N is a normal subgroup of a group G and H is any subgroup of G, prove that NH is a subgroup of G.

1.4.5. If H is a subgroup of a group G and N is a normal subgroup of G, show that $H \cap N$ is a normal subgroup of G.

1.4.6. Suppose N and M are two normal subgroups of a group G Such that $N \cap M = (e)$. Show that for any $n \in N$, $m \in M$, $mn = nm$.

1.4.7. Show that a subgroup N of a group G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

1.5 SUMMARY:

In this lesson we have introduced the concept of a normal subgroup of a group and proved some results related to normal subgroups. Also we consider the set of all right cosets of a normal subgroup of a group and we proved that it is a group, which is called the quotient group.

1.6 TECHNICAL TERMS:

- Normal subgroup
- Quotient group

1.7 ANSWERS TO SELF ASSESMENT QUESTIONS:

1.2.5 Given that N is a subgroup of a group G. Suppose N is a normal subgroup of G. Now we will show that every right coset of N in G is a left coset of N in G.

Let $g \in G$. Then Ng is a right coset of N in G. Now we show that Ng = gN. Since N is a normal subgroup of G, $gNg^{-1} \subseteq N$ and $g^{-1}Ng \subseteq N$.

Let $y \in Ng \Rightarrow y = mg$ for some $m \in N$.

Since $g^{-1}Ng \subseteq N$, we have $g^{-1}mg \in N \Rightarrow gg^{-1}mg \in gN$

$\Rightarrow emg \in gN \Rightarrow mg \in gN \Rightarrow y \in gN$.

This shows that $Ng \subseteq gN$.

Let $x \in gN \Rightarrow x = gn$ for some $n \in N$.

Now $gng^{-1} \in gNg^{-1} \subseteq N \Rightarrow gng^{-1} \in N \Rightarrow gng^{-1}g \in Ng$.

$\Rightarrow gne \in Ng \Rightarrow gn \in Ng \Rightarrow x \in Ng$.

This shows that $gN \subseteq Ng$ and hence Ng = gN. Thus every right coset of N in G is a left coset of N in G.

Conversely suppose that every right coset of N in G is a left coset of N in G. Now we will show that N is a normal subgroup of G. That is for every $g \in G$ we will show that $gng^{-1} \in N$ for all $n \in N$.

Let $g \in G$. Then Ng is a right coset of N in G. By our supposition Ng is a left coset of N in G. So Ng = hN for some $h \in G$.

Now $g = eg \in Ng \Rightarrow g \in hN$.

But $g = ge \in gN$. Therefore $g \in gN \cap hN \Rightarrow gN \cap hN \neq \phi$.

Since any two left cosets are either disjoint or equal and $gN \cap hN \neq \phi$, we have gN = hN. Therefore gN = Ng = hN.

Now for any $n \in N$, $gng^{-1} \in gNg^{-1} = Ngg^{-1} = Ne = N$.

$\Rightarrow gng^{-1} \in N$ for all $n \in N$.

So $gng^{-1} \in N$ for all $n \in N$ and for all $g \in G$ and hence N is a normal subgroup of G.

1.8 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer- Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.V. Samba Siva Rao

LESSON - 2

HOMOMORPHISMS

OBJECTIVES:

Objectives of this lesson are to

define the notion of a homomorphism of groups and give certain examples.
define the concept of the kernal of a homomorphism and prove certain elementary properties of homomorphism and their kernels.
define the notion of an isomorphism of groups and prove certain elementary properties of isomorphisms.
prove the fundamental theorem of homomorphisms. To prove the cauchy's and sylow's theorems for abelian groups.

STRUCTURE:

2.1: INTRODUCTION:

A relationship between groups G and G^1 is generally exhibited in terms of a structure related mapping f: $G \to G^1$ which are called homomorphisms. Such a mapping often gives us information about the structure of G^1 from known structural properties of G or information about the structure of G from known structural properties of G^1. The study of such structure related mappings from one algebraic structure to a similar algebraic structure is an important area in algebra. In this lesson, we shall introduce the concept of a homomorphism explicitly and study certain important elementary properties of homomorphisms.

2.2: DEFINITION AND EXAMPLES OF HOMOMORPHISMS:

2.2.1. Definition: Let $(G, \bullet)$ and $(G^1, *)$ be any two groups. A mapping f: $G \to G^1$ is called a homomorphism of groups if $f(a \bullet b) = f(a) * f(b)$ for all $a, b \in G$.

In other words, the image of the product $a \bullet b$ is equal to the product of the images f(a) and f(b) for any elements a and b in G.

2.2.2. Example: Let G be the group of all positive real numbers under the usual multiplication and G^1 be the group of all real numbers under the usual addition. Define f: $G \to G^1$ by $f(a) = \log_2 a$ for all $a \in G$.

Then $f(a.b) = \log_2(a.b) = \log_2 a + \log_2 b = f(a) + f(b)$ for all $a, b \in G$. Therefore f is a homomorphism of groups.

2.2.3. Example: Let G be the group of all real numbers under the usual addition and G^1 be the group of all non zero real numbers under usual multiplication.
Define f : G$\rightarrow$ G^1 by f(a) = 2^a for all a$\in$G.
Then f (a+b) = 2^{a+b}= $2^a.2^b$ = f(a) . f(b) for all a, b $\in$G and hence f is a homomorphism.

2.2.4. Example: Let (G, $\bullet$) and (G^1, $*$) be any groups.
Define : f : G $\rightarrow$ G^1 by f(a) = e^1 for all a$\in$G
where e^1 is the identity element in G^1
Then f(ab) = e^1 = $e^1 * e^1$ = f(a) $*$ f(b) for any a, b$\in$G and hence f is a homomorphism which is called the trivial homomorphism.

2.2.5. Example: Consider the group $\mathbb{Z}$ of all integers under the usual addition and let n be an arbitrarily fixed integer. Define f : $\mathbb{Z} \rightarrow \mathbb{Z}$ by f(a) = na for all a$\in \mathbb{Z}$. Then f is a homomorphism.

2.2.6. Example: Let G^1 = {1, –1} where 1.1 =1, (1)(–1) = –1, (–1)(1) = –1 and (–1) (–1) =1. Then G^1 is a group.

Define : f : $\mathbb{Z} \rightarrow G^1$ by

f(a) = $\begin{cases} 1 \text{ if a is even} \\ -1 \text{ if a is odd} \end{cases}$

Then f(a+b) = f(a) f(b) for all a, b$\in \mathbb{Z}$ and hence f is a homomorphism.

2.2.7. Self Assessment question:
Prove that the mapping f in 2.2.6 above is a homomorphism.

2.2.8. Example : Let n be any positive integer and $\mathbb{Z}_n$ be the addition group of integers modulo n. Define f : $\mathbb{Z} \rightarrow \mathbb{Z}_n$ by f(a) = r, where a = qn +r, $0 \leq r < n$. Note that r is the remainder obtained by dividing a with n. Then f is a homomorphism.

2.2.9. Self Assessment Question: Prove that f is a homomorphism in 2.2.8.

2.2.10. Example: For any group G, the map f: $G \rightarrow G$ defined by f(a) = a for all a$\in$G is a homomorphism called the identity homomorphism.

2.2.11. Example: Let G be the group of all 2 x 2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over the real numbers for which ad – bc $\neq$ 0. Then G is a group under the usual matrix multiplication. Let G^1 be the group of non-zero real numbers under the usual multiplication.
Define f : G $\rightarrow$ G^1 by

f$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$ = ad–bc, for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\in$ G. Then f is a homomorphism.

2.2.12. Example : Let (G, $\bullet$) be any group and let a$\in$G. Let $(\mathbb{Z}, +)$ be the group of all integers where + is the usual addition. Define f: $\mathbb{Z} \rightarrow$ G by f(n) = a^n for all n$\in \mathbb{Z}$, where a^n is defined inductively by

$$a^n = \begin{cases} e & \text{if } n = 0 \\ a^{n-1}.a & \text{if } n > 0 \\ (a^{-1})^{-n} & \text{if } n < 0 \end{cases}$$

Here a^{-1} is the inverse if a and e is the identity element in G. Then f is a homomorphism.

In the following theorem, certain important elementary properties of homomorphisms are derived.

2.2.13. Theorem: Let $f : G \to G^1$ be a homomorphism of groups. Then the following hold.

(i) $f(e) = e^1$, where e and e^1 are the identities in G and G^1 respectively

(ii) $f(a^{-1}) = f(a^{-1})$ for any $a \in G$

(iii) For any $a, b \in G$, $f(a) = f(b) \Leftrightarrow f(ab^{-1}) = e^1 \Leftrightarrow f(a^{-1}b) = e^1$

Proof: (i) Consider

$f(e)\, f(e) = f(e.e) = f(e) = e^1.\, f(e)$

and now, by the cancellation laws in G^1, we have $f(e) = e^1$.

(ii) For any $a \in G$, we have

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

This implies $f(a^{-1})$ is the inverse of f(a). Since the inverse of an element is unique, we have $f(a^{-1}) = f(a)^{-1}$.

(iii) For any $a, b \in G$.

$f(a) = f(b) \Leftrightarrow f(a)\, f(b^{-1}) = e^1$

$\Leftrightarrow f(a)\, f(b^{-1}) = e^1$

$\Leftrightarrow f(ab^{-1}) = e^1$

and $f(a) = f(b) \Leftrightarrow f(a)^{-1} f(b) = e^1$

$\Leftrightarrow f(a^{-1})\, f(b) = e^1$

$\Leftrightarrow f(a^{-1}b) = e^1$.

2.2.14. Theorem: Let N be a normal subgroup of a group G and G/N the quotient group. Define $f : G \to G/N$ by $f(a) = aN$ for any $a \in G$. Then f is a surjective (onto) homomorphism.

Proof: Given that N is a normal subgroup of a group G.

Then $G/N = \{aN / a \in G\}$. Recall that the binary operation in G/N is defined as $aN.bN = (ab)N$ for any $a, b \in G$ and hence $f(a.b) = (ab)N = aN.bN = f(a).f(b)$. Therefore f is a homomorphism.

Let $aN \in G/N$. Then $a \in G$. Now $f(a) = aN$ and hence f is onto. Thus f is a surjective homomorphism.

2.2.15. Self assessment question: If $f : G \to H$ and $g : H \to K$ are homomorphisms of groups, prove that $gof : G \to K$ is also a homomorphism.

2.3: THE KERNEL OF A HOMOMORPHISM:

The identity element of G to that of G^1. There in 2.2.13(i) Theorem we have learnt that any homomorphism of G into G^1 carries may be several elements in G which are carried to the identity element G^1. The collection of such elements in G is called the kernel of that

homomorphism and this plays an important role in the study of the homomorphisms of groups.

2.3.1. Definition: Let $f: G \to G^1$ be a homomorphism of groups and e^1 be the identity element of G^1. The Kernel of f is defined as the set Ker $f = \{a \in G / f(a) = e^1\}$

2.3.2. Self Assessment question: Determine the kernels of each of the homomorphisms given in examples 2.2.2 to 2.2.12.

2.3.3. Theorem : The kernel of any homomorphism $f: G \to G^1$ is a normal subgroup of G.
Proof : Let $f: G \to G^1$ be a homomorphism of groups and $k = \text{Ker } f = \{a \in G / f(a) = e^1\}$. where e and e^1 are the identity elements in G and G^1 respectively. By 2.2.13(i)theorem, $f(e) = e^1$ and $e \in K$, so that K is a nonempty subset of G.
Now $a, b \in K \Rightarrow f(a) = e^1$ and $f(b) = e^1$
$\Rightarrow f(ab^{-1}) = e^1$ (by 2.2.13 (iii))
$\Rightarrow ab^{-1} \in K$.
Therefore K is a subgroup of G.
Also $a \in K$ and $x \in G \Rightarrow f(xax^{-1}) = f(x)\ f(a) f(x^{-1})$
$= f(x)e^1 f(x)^{-1} = e^1 \Rightarrow xax^{-1} \in K$
Thus K is a normal subgroup of G.

2.3.4. Note: A converse of 2.3.3 can be started as follows: Any normal subgroup of G is the Kernel of some homomorphism of G into a suitable group G^1. This statement is also true; for, let N be a normal subgroup of a group G and consider the quotient group G/N and define $f: G \to G/N$ by $f(a) = aN$ for any $a \in G$ (see 2.2.14).
Then f is a homomorphism and Ker $f = \{a \in G / f(a) = N\} = \{a \in G / aN = N\} = N$.

Note that N is the identity element of the quotient group G/N. Before taking up the next important property of the Kernels of homomorphisms. Let us recall that, for any mapping $f: A \to B$ and $b \in B$, an element $a \in A$ is called an inverse image of b under f if $f(a) = b$. There may be several (or not even one) inverse images of b. However, if f is a surjection of A onto B, then any $b \in B$ has at least inverse image in A under f. In the following we describe an important property of Kernels of surjective homomorphisms.

2.3.5. Theorem: Let f be a homomorphism of G onto G^1 (i.e, $f: G \to G^1$ is a surjective homomorphism) and $y \in G^1$. Let K be the Kernel of f. Then the set of all inverse images of y in G under f is equal to the coset aK, where a is any inverse image of y.

Proof : Given that f is a homomorphism of G onto G^1 and $y \in G^1$. Let a be an inverse image of y in G under f; i.e, $a \in G$ such that $f(a) = y$. Then for any $x \in G$, $x \in ak \Leftrightarrow x = ak$ for some $k \in K$.
$\Leftrightarrow a^{-1}x = k \in K \Leftrightarrow f(a^{-1}x) = e^1$
$\Leftrightarrow f(a^{-1})f(x) = e^1 \Leftrightarrow f(a)^{-1} f(x) = e^1$
$\Leftrightarrow f(x) = f(a) = y$ (by 2.2.13 (iii))
Thus $ak = \{x \in G / f(x) = y\}$.

2.4: ISOMORPHISMS:

Consider the group $G = \{1, -1\}$ under the usual multiplication and the group $\mathbb{Z}_2 = \{0, 1\}$ under the addition modulo 2. These two groups look like similar, except for the labeling or naming of the elements. The identity in G is 1 while in $\mathbb{Z}_2$ it is 0. Also the other element –1 in

G has the property that (–1)(–1) = 1 while the element 1 in $\mathbb{Z}_2$ has a similar property that 1+1 = 0. In other words, there is a bijection f : G $\to$ $\mathbb{Z}_2$ which is a homomorphism too, such an f is defined by f(1) =0 (which is a necessary property of homomorphisms) and f(–1) =1. Let us formalise this idea in the following.

2.4.1. Definition: A homomorphism f : G $\to$ G^1 is called an isomorphism if f is a bijection (that is, f is both one-one and onto). Two groups G and G^1 are said to be isomorphic and is expressed as $G \cong G^1$ if these is an isomorphism f : G $\to$ G^1.

2.4.2. Theorem: A homomorphism f : G $\to$ G^1 is an injection if and only if Ker f = {e}, where e is the identity in G.

Proof: Let f : G $\to$ G^1 be a homomorphism of groups. Suppose that f is an injection.
Recall that Ker f = $\{a \in G / f(a) = e^1\}$
Since it is always true that $f(e) = e^1$, we have e $\in$ Kerf. On the other hand, a $\in$ Kerf $\Rightarrow$ $f(a)=e^1 = f(e)$
$\Rightarrow$ a =e (since f is one - one)
Thus Ker f ={e}
Conversely suppose that ker f = {e}. Then, for any elements a and b in G, f(a) = f(b)
$\Rightarrow f(ab^{-1}) = e^1$ (by 2.2.13(iii))
$\Rightarrow ab^{-1} \in$Ker f = {e} $\Rightarrow$ $ab^{-1} = e \Rightarrow$ a = b.
Thus f is an injection.

Injective homomorphisms are usually called monomorphisms and surjective homomorphisms are called epimorphisms. An isomorphism is both a monomorphism and an epimorphism. A homomorphism f: G $\to$ G^1 is an isomorphism if and only if Kerf = {e} and every element of G^1 has an (unique) inverse image in G.

2.4.3. Theorem: (i) The inverse of an isomorphism is also an isomorphism
(ii) If f: G $\to$ H and g: H $\to$ K are isomorphisms, then so is gof.

Proof: (i) Let f : G$\to$ H be an isomorphism. Then f is a bijective homomorphism.
Since f is a bijection, the inverse map f^{-1} : H $\to$ G exists such that fof^{-1} and $f^{-1}$of are identity mappings of H and G respectively. Also f^{-1} is clearly a bijection.
Further, for any x, y$\in$H, we have
$f(f^{-1}(xy)) = xy = f(f^{-1}x).f(f^{-1}y) = f(f^{-1}(x).f^{-1}(y))$ and since f is an injection,
we have $f^{-1}(x.y) = f^{-1}(x).f^{-1}(y)$
Thus f^{-1} : H$\to$G is a homomorphism also and f^{-1} is an isomorphism.

(ii) Follows from the facts that the composition of two bijections (homomorphisms) is also a bijection (homomorphism respectively).

2.4.4. Self Assessment Question: Let G, H and K be groups. Then prove that the following

(i) $G \cong G$
(ii) $G \cong H \Rightarrow H \cong G$
(iii) $G \cong H$ *and* $H \cong K \Rightarrow G \cong K$

2.5: THE FUNDAMENTAL THEOREM OF HOMOMORPHISMS:

We shall prove a very crucial and fundamental theorem which states that any

homomorphic image of a group G is isomorphic to a quotient of G. In theorem 2.2.14, we have already proved that any quotient G/N of a group G is a homomorphic image of G. We prove a converse of this in the following.

2.5.1. Theorem (Fundamental theorem of Homomorphisms): Let f: $G \to G^1$ be a surjective homomorphism of groups. Then $G/\ker f \cong G^1$.

Proof : Given that f: $G \to G^1$ is a surjective homomorphism of groups. Let K = Ker f. We have already proved that K is a normal subgroup of G (see 2.3.3). Now define g: $G/K \to G^1$ by g(aK) = f(a).
for any $aK \in G/K$ with $a \in G$.
Let us recall that, for different elements a and b, aK and bK may be equal. On the face of it, g(aK) looks like depending on a. We shall first prove that g(aK) depends on the coset aK but note on the element a.
For any $a, b \in G$, aK = bK
$\Leftrightarrow ab^{-1} \in K = \ker f$
$\Leftrightarrow$ f(a) = f(b) (by 2.2.13 (iii))
This proves that g is well defined and g is an injection also.
Further for any $a, b \in G$,
g(ak.bk) = g((ab) K) = f(ab) = f(a).f(b) = g(aK).g(bK)
and hence g is a homomorphism and g is an injection also.
Now, we will show that g is onto
Let $x \in G^1$. Since f is surjective, x = f(a) for some $a \in G$.
Now $aK \in G/K$ and g(aK) = f(a) = x
Therefore g is surjective (onto).
Thus g is an isomorphism of G/K onto G^1 and $G/K \cong G^1$.

The above theorem is actually an important tool in the development of the structure theory of groups. Before going to certain applications of the fundamental theorem of homomorphisms, let us prove the following.

2.5.2. Theorem: Let $f : G \to G^1$ be a surjective homomorphism of groups with Kernel K.

(i) If H^1 is a subgroup of G^1 and $H = f^{-1}(H^1) = \{a \in G / f(a) \in H^1\}$, then H is a subgroup of G containing K.
(ii) The correspondence $H^1 \to f^{-1}(H^1)$ is a one-to-one correspondence between the subgroups of G^1 and the subgroups of G containing K.
(iii) H^1 is a normal subgroup of G^1 if and only if $f^{-1}(H^1)$ is a normal subgroup of G.

Proof: Given that $f : G \to G^1$ is a surjective homomorphism of groups, with kernel K.
(i) Let H^1 is a subgroup of G^1 and $H = f^{-1}(H^1) = \{a \in G / f(a) \in H^1\}$
For any $a \in K$, we have $f(a) = e^1 \in H^1$ and hence $a \in H$.
Therefore $K \subseteq H$ and in particular $H \neq \phi$
Also $a, b \in H \Rightarrow f(a), f(b) \in H^1$
$\Rightarrow f(a).f(b)^{-1} \in H^1$ (Since H^1 is a subgroup of G^1)
$\Rightarrow f(a).f(b^{-1}) \in H^1 \Rightarrow f(ab^{-1}) \in H^1 \Rightarrow ab^{-1} \in H$
Thus H is a subgroup of G containing K.

(ii) Let S^1 and T^1 be subgroups of G^1 such that $f^{-1}(S^1) \subseteq f^{-1}(T^1)$
Then $x \in S^1 \Rightarrow f(a) = x$ for some $a \in G$ (since f is onto)

$\Rightarrow a \in f^{-1}(S^1) \subseteq f^{-1}(T^1) \Rightarrow f(a) \in T^1 \Rightarrow x \in T^1$
Therefore, $S^1 \subseteq T^1$. Thus $S^1 = T^1$ whenever $f^{-1}(S^1) = f^{-1}(T^1)$, which implies that the correspondence $H^1 \mapsto f^{-1}(H^1)$, is one-one.
To prove that this is onto also, let S be a subgroup of G containing K. Put $H^1 = \{f(a)/a \in S\}$.
Then clearly H^1 is a subgroup of G^1 and $S \subseteq f^{-1}(H^1)$
Further, $b \in f^{-1}(H^1) \Rightarrow f(b) \in H^1 \Rightarrow f(b) = f(a)$ for some $a \in S$.
$\Rightarrow f(ba^{-1}) = e^1$ and $a \in S$
$\Rightarrow ba^{-1} \in \text{Ker } f = K \subseteq S$ and $a \in S$
$\Rightarrow b = (ba^{-1})\, a \in S$
Therefore, $f^{-1}(H^1) \subseteq S$ and hence $f^{-1}(H^1) = S$
Thus $H^1 \mapsto f^{-1}(H^1)$ is a one-to-one correspondence between the subgroups of G^1 and the subgroups of G containing K.

(iii) Suppose H^1 is a normal subgroup of G^1.Then $xyx^{-1} \in H^1$ for all $y \in H^1$ and $x \in G^1$.
Now, for any $b \in G$ and $a \in f^{-1}(H^1)$, we have $f(a) \in H^1$ and $f(b) \in G^1$ and hence $f(bab^{-1}) = f(b)$ $f(a)f(b^{-1}) = f(b)f(a)f(b)^{-1} \in H^1$
So that $bab^{-1} \in f^{-1}(H^1)$
Thus $f^{-1}(H^1)$ is a normal subgroup of G.

Conversely suppose that $f^{-1}(H^1)$ is a normal subgroup of G, where H^1 is a subgroup of G^1. Let $y \in H^1$ and $x \in G^1$. Since f is onto, we can choose a and b in G such that $y = f(a)$ and $x = f(b)$. Then $a \in f^{-1}(H^1)$ and $b \in G$. Since $f^{-1}(H^1)$ is a normal subgroup of G, we have $bab^{-1} \in f^{-1}(H^1)$ and therefore $f(bab^{-1}) \in H^1$
Now $xyx^{-1} = f(b)f(a)f(b)^{-1} = f(bab^{-1}) \in H^1$.
Thus H^1 is a normal sub group of G^1.

2.5.3. Theorem: Let $f : G \to G^1$ be a surjective homomorphism with kernel K. Let N^1 be a normal subgroup of G^1 and $N = f^{-1}(N^1)$.
Then $G/N \cong G^1/N^1$ and equivalently $G/N \cong (G/K)/(N/K)$.

Proof: Given that $f: G \to G^1$ be a surjective homomorphism with kernel K and N^1 is a normal subgroup of G^1 and $N = f^{-1}(N^1)$.
Define $g : G \to G^1/N^1$ by $g(a) = f(a)N^1$ for all $a \in G$.
Then, for any $a, b \in G$, we have $g(ab) = f(ab)N^1 = f(a)\, f(b)\, N^1$ (since f is a homomorphism)
$= f(a)\, N^1 .\, f(b)\, N^1$
$= g(a)\, g(b)$
Therefore g is a homomorphism.Now we show that g is onto.
Let $x \in G^1/N^1 \Rightarrow x = zN^1$ for some $z \in G^1$
Since $z \in G^1$ and since f is onto, $z = f(a)$ for some $a \in G$.
Now $x = zN^1 = f(a)N^1 = g(a)$
Therefore g is onto hence $g : G \to G^1/N^1$ is a surjective homomorphism. By the fundamental theorem of homomorphisms (2.5.1),
$G/\ker g \cong G^1/N^1$
But $\text{Ker}g = \{a \in G / g(a) = N^1, \text{the identity in } G^1/N^1\}$
$= \{a \in G / f(a)N^1 = N^1\}$
$= \{a \in G / f(a) \in N^1\}$
$= f^{-1}(N^1)$
$= N$

Thus we have $G/N \cong G^1/ N^1$
Also, if we restrict f to N, then it becomes a surjective homomorphism of N onto N^1 whose kernel is K again and hence by the fundamental theorem of homomorphisms (2.5.1).
$N^1 \cong N/K$ and $G^1 \cong G/K$
Thus $G/N \cong G^1/ N^1 \cong (G/K)/(N/K)$.

2.5.4. Self Assessment Question: Let N and K be normal subgroup of a group G such that $K \subseteq N$. Then prove that N/K is a normal subgroup of G/K and that $(G/K)/(N/K) \cong G/N$.

2.5.5. Self Assessment question: Let N be a normal subgroup of a group G and K be any subgroup of G. Then prove that KN is a subgroup of G, $K \cap N$ is a normal subgroup of K and $K/ K \cap N \cong KN/N$.

2.6: CAUCHY'S THEOREM AND SYLOW'S THEOREM:

In the previous section, we have learnt that the homomorphic images of a given group G coincide (upto isomorphism) with the quotient G/N of G, where N is a normal subgroup of G. A group is said to be simple if it has no nontrivial homomorphic images or equivalently, if it has no nontrivial normal subgroups. When we construct the quotient group G/N, where N is a normal subgroup of G, knowing the structure of G/N help us in knowing the structure of G upto N". We can ascertain certain information about G by looking at those of a quotient of G. Those ideas are applied in proving the following two theorems. In fact, later we prove those results in a much more several set up and in easier way. However, the proofs of these two results are important on their own in view of the use of several group theoritic concepts and illustrations in proving these.

2.6.1. Theorem (Cauchy's Theorem for abelian groups): Let G be a finite abelian group and p is a prime number such that p divides O(G). Then G has an element a such that $a \neq e$ and $a^p = e$.

Proof: We shall use induction on O(G). Since p divides O(G), we have $p \leq O(G)$. If O(G) = p, then we can take any element $a \neq e$ in G, for, by Lagrange's theorem, O(a) = p and hence $a^p = e$. Next suppose that O(G) > p and assume that the theorem is true for all abelian groups of order less than O(G). Choose an element $b \neq e$ in G. Let n be the order of b; that is, n is the least positive integer such that $b^n = e$. We shall distinguish two cases.

Case (i) : Suppose p divides n. Then $b^{n/p} \neq e$ and $(b^{n/p})^p = e$ and hence $b^{n/p}$ is the required element a.

Case (ii): Suppose p does not divide n. Let H be the subgroup generated by b in G. Then O(H) = n > 1. Since G is an abelian group, H is a normal subgroup of G and hence we can consider the quotient group G/H. Also, we have
O(G) = O(H). O(G/H) = n.O(G/H).
Since p divides order of G and p does not divide n, it follows that p divides O(G/H). Also G/H is a group of order less than O(G)
(Since n > 1 and O(G/H) = O(G)/n). Therefore, by the induction hypothesis, these exists a non-identity element X in G/H such that $X^p = H$, the identity element in G/H. $X \in G/H$ implies that X = xH for some $x \in G$. Then $X^{o(x)} = (xH)^{o(x)} = x^{o(x)}$. H = H.Since O(X) = p in G/H, we get that p divides O(x). Now, as in case (i), $x^{O(x)/p}$ is the required element a in G.

2.6.2. Theorem (Sylow's theorem for abelian groups):

Let G be a finite abelian group, p a prime number and r a non-negitive integer such that p^r divides O(G) and p^{r+1} does not divide O(G). Then G has a subgroup of order p^r.

Proof: Given that G is a finite abelian group, p a prime number and r a non- negative integer such that p^r divides O(G) and p^{r+1} does not divide O(G).
If r =0, then p^r=1 and {e} is the subgroup of order p^r. Suppose r > 0. Then p divides O(G) and hence by the Cauchy's theorem (2.6.1), there exists an element $a \neq e$ in G such that $a^p = e$.

Now, consider H = $\{x \in G / x^{p^n} = e \text{ for some } n \in \mathbb{Z}^+\}$.
Then H has at least two elements, namely e and a. We shall prove that H is a subgroup of G.

Let x, y∈H. Then $x^{p^n} = e$ and $y^{p^n} = e$ for some n, m∈ $\mathbb{Z}^+$.

$\Rightarrow \left(xy^{-1}\right)^{p^{n+m}}$

$\Rightarrow x^{p^{n+m}} \left(y^{p^{n+m}}\right)^{-1} = e \Rightarrow xy^{-1} \in H$.

Therefore H is a subgroup of G. Next, we shall prove that p is the only prime dividing O(H). If q is a prime number dividing O(H) and $q \neq p$, then again by 2.6.1, there exists $x \neq e$ in H such that $x^q = e$. Since x∈H, $x^{p^n} = e$ for some n $\in \mathbb{Z}^+$. Since $q \neq p$, q and p^n are relatively prime and hence these exist integers t and s such that $tq + sp^n = 1$ and now consider

$x = x^1 = x^{tq + sp^n} = \left(x^q\right)^t . \left(x^{p^n}\right)^s = e$, which is a contradiction, since by our choice $x \neq e$.

Therefore no prime other than p divides O(H). This implies that $o(H) = p^m$ for some $m \geq 0$.

Since O(H) divides O(G) (by the Lagrange's theorem) and since p^{r+1} does not divide O(G), it follows that $0 \leq m \leq r$.
Since a∈H and $a \neq e$, O(H) > 1 and hence m > 0.
Finally we prove that m = r and conclude that H is the required subgroup of G. On the contrary, suppose m < r. Consider the quotient group G/H (note that, since G is abelian, H is a normal subgroup of G).
Then p^r divides $O(G) = O(G/H)\, O(H) = O(G/H).p^m$; so that p^{r-m} divides o(G/H) and r – m > 0. Thus p divides O(G/H). Again by the Cauchy's theorem 2.6.1, there exists an element xH in G/H such that. $xH \neq H$ and $(xH)^p = H$.

Then $x^pH = H$, and hence $x^p \in H$ so that $\left(x^p\right)^{p^n}$ = e for some n and therefore $x^{p^n+1} = e$ which implies that x∈H and xH = H, which is a contradiction to the choice of x. Thus m = r and $O(H) = p^r$

Later, we extend both the above theorems for arbitrary finite groups. However, if G is a finite abelian group. Then the subgroup H described in theorem 2.6.2 is unique. This is proved in the following.

2.6.3. Theorem: Let G be a finite abelian group, p a prime and r a non-negative integer such that p^r divides O(G) and p^{r+1} does not divide O(G). Then G has a unique subgroup of order p^r.

Proof : The theorem is trivial for r = 0. Therefore, we can suppose that r > 0. We have

proved the existence of a subgroup of order p^r in the Sylow's theorem (2.6.2).
So we shall now prove the uniqueness. Let H and K be any subgroups of order p^r in G. Since G is abelian, HK=KH and hence HK is a subgroup of G. Also

$$O(HK) = \frac{O(H)O(K)}{O(H \cap K)} = \frac{p^r p^r}{O(H \cap K)}$$

Therefore $O(HK) = p^s$ for some positive integer s. By the Lagrange's theorem, p^s divides O(G). Since $H \subseteq HK$, $p^r = O(H) \leq O(HK) = p^s$ and hence $r \leq s$. But since p^{r+1} does not divide O(G), s can not be strictly greater than r. That is r = s which implies that O(H) = O(HK) and hence H = HK. This yields that $k \subseteq H$. Since H and K are of the same order, we get that H = K.

The above theorem fails for non abelian groups, that is, if G is a finite non abelian group such that $p^r | O(G)$ and $p^{r+1} \nmid O(G)$ then G may possess more than one subgroups of order p^r. The following illustrates this.

2.6.4. Example: Consider the group S_3, the symmetric group of degree 3. Then S_3 is a non abelian group of order 3! = 6. Take p = 2 and r = 1. Then $p^r | O(S_3)$ and $p^{r+1} \nmid O(S_3)$. For any transposition σ in S_3, $\{id, \sigma\}$ is a subgroup of order p^r in S_3. There are three distinct transpositions in S_3, namely (1, 2), (2, 3) and (3, 1) and hence these are three distinct subgroups each of order 2, in S_3

2.6.5. Self Assessment Question: How many subgroups are there in S_3, each of order 3?

Later, we shall prove that any two subgroups H and K of order p^r, where p^{r+1} does not divide O(G), must be conjugate to each other, in the sense that $H = aKa^{-1}$ for some $a \in G$, even though they may not be equal

2.6.6. Self Assessment Question: Prove that any two subgroups of order 2 in S_3 are conjugate to each other .

2.7. MODEL EXAMINATION QUESTIONS:

2.7.1. Define the concepts of a homomorphism of groups and its Kernel. Prove that a homomorphism $f : G \to G^1$ is injective if and only if Ker f = {e}

2.7.2. State and prove the Fundamental theorem of homomorphisms.

2.7.3. State and prove the Cauchy's theorem for finite abelian groups.

2.7.4. State and prove the Sylow's theorem for finite abelian groups.

2.7.5. If G is a finite abelian group, p is a prime number and r is a non negitive integer. such that $p^r | O(G)$ and $p^{r+1} \nmid O(G)$, then prove that there can be atmost one subgroup of order p^r in G. Is this true for non abelian groups ? Justify your answer.

2.8 SUMMARY:

In this lesson, we have learnt the concepts of a homomorphism, isomorphism and Kernel of a homomorphism and proved certain important properties of these. We have proved three very important theorems, namely, the fundamental theorem of homomorphisms, Cauchy's theorem for finite abelian groups and Sylow's theorem for finite abelian groups.

2.9 TECHNICAL TERMS:

- Homomorphism.
- Isomorphism. (bijective homomorphism)
- Monomorphism. (injective homomorphism)
- Epimorphism. (surjective homomorphism)
- Kernel of a homomorphism.
- Homomorphic image.
- Fundamental theorem of homomorphism.
- Cauchy's Theorem.
- Sylow's Theorem.

2.10 ANSWERS TO SELF ASSESSMENT QUESTIONS:

2.2.3. The identity in G^1 is 1 and hence

$\ker f = \{a \in G / f(a) = 1\}$

$= \{a \in \mathbb{R} / 2^a = 1\}$

$= \{0\}$

2.2.4. Every element of G is mapped to e^1 and hence ker f = G

2.2.5. $f : \mathbb{Z} \to \mathbb{Z}$ is defined as f(a) = na
for any $a \in \mathbb{Z}$. If n = 0, then f is the trivial homomorphism and ker f = $\mathbb{Z}$.
If $n \neq 0$, then ker f = $\{a \in \mathbb{Z} / na = 0\} = \{0\}$.

2.2.6. ker f = $\{a \in \mathbb{Z} / f(a) = 1\}$

= {a∈ $\mathbb{Z}$ /a is even} = The set of even integers.

2.2.7: Let a, b∈ $\mathbb{Z}$. We have prove that f(a+b) = f(a) f(b). If a and b are both even, then so is a+b and f(a+b) =1, f(a)=1=f(b). If both a and b are odd then a+b is even and
f(a+b) = 1 = (–1)(–1) = f(a).f(b)
Similar argument can be made when one of a and b is even and the other is odd.

2.2.8. 0 is the identity in Z_n and hence
ker f = {a∈ $\mathbb{Z}$ /a = qn for some q∈ $\mathbb{Z}$ } = nZ.

2.2.9: Let a, b∈ $\mathbb{Z}$. Write $a = q_1n + r_1$ and $b = q_2n + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1 < n$ and $0 \leq r_2 < n$. Then $f(a) = r_1$ and $f(b) = r_2$. Also we have $0 \leq r_1 + r_2 < 2n$. We shall distinguish two cases
Case (i): Suppose $r_1 + r_2 < n$.
Then $a+b = (q_1 + q_2)n + (r_1 + r_2)$ and
$f(a+b) = r_1 + r_2 = r_1 +_n r_2 = f(a) +_n f(b)$ where $+_n$ is the addition modulo n.

Case (ii) : Suppose $r_1 + r_2 \geq n$. Then
$a+b = (q_1 + q_2 + 1)n + (r_1 + r_2 - n)$ and $0 \leq r_1 + r_2 - n < n$ and hence $f(a+b) = r_1 + r_2 - n$
$= r_1 +_n r_2 = f(a) +_n f(b)$
Thus f is a homomorphism.

2.2.10. Ker f = {e}

2.2.11. Ker f = $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} / ad - bc = 1\right\}$

2.2.12. ker f = $\{n \in \mathbb{Z} / a^n = e\} = \{0\}$ if a is of infinite order; that is $a^n \neq e$ for all $n \neq 0$ and ker f = $n\mathbb{Z}$, if a is of order n; that is n is the smallest positive integer such that $a^n = e$.

2.2.15: For any a, b ∈ G,
gof(ab) = g(f(ab))
= g(f(a)f(b)) (since f is a homomorphism)
= g(f(a) g(f(b)) (since g is a homomorphism)
= (gof) (a) (gof) (b)
Therefore, gof is a homomorphism.

2.3.2: (2.2.2) The identity in G^1 is 0 and hence
Ker f = $\{a \in G / f(a) = 0\}$
= $\{a \in \mathbb{R} / a > 0$ and $\log_2 a = 0\} = \{1\}$
Therefore, ker f = {1}

2.4.4. (i) The identity mapping of G onto G is an isomorphism and hence $G \cong G$
(ii) If $G \cong H$, then there exists an isomorphism $f: G \to H$ and, in this case, $f^{-1}: H \to G$ is an isomorphism (2.4.3(i)) and hence $H \cong G$.
(iii) This follows from 2.4.3(ii)

2.5.4. Let $f: G \to G/K$ be defined by f(a) = aK for any $a \in G$. Then f(N) = N/K which is a normal subgroup of G/K and by 2.5.3 theorem, $G/N \cong (G/K)/(N/K)$.

2.5.5. Since N is a normal subgroup G, NK = KN and hence KN is a subgroup of G. If $x \in K$ and $a \in K \cap N$ then $xax^{-1} \in K \cap N$ and hence $K \cap N$ is a normal subgroup of K. Define $f: K \to KN/N$ by f(a) = aN. Then f is an epimorphism and ker f = $K \cap N$ and by 2.5.1 Theorem, K/Ker f ≅ KN/N. Hence $K/K \cap N \cong KN/N$.

2.6.5. Let α be the 3 -cycle (123) in S_3. Then α^2 = (1 3 2) and α^3 = id .$\{id, \alpha, \alpha^2\}$ is the only subgroup of order 3 in S_3.

2.6.6. There are three subgroups , each of order 2 in S_3 and these are
$H_1 = \{id, (1,2)\}$; $H_2 = \{id, (2,3)\}$ and $H_3 = \{id, (3,1)\}$.
Let $\beta = (1,2)$, $\gamma = (2,3)$ and $\delta = (3,1)$, Then $\gamma H_1 \gamma^{-1} = H_3$,
$\beta H_2 \beta^{-1} = H_3$ and $\delta H_1 \delta^{-1} = H_2$.

2.11 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer- Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.V.Samba Siva Rao

LESSON - 3

AUTOMORPHISMS

OBJECTIVES:

Objectives of this lesson are to

- define the notion of an automorphism and give certain examples.
- prove that the set of all automorphisms of a group G is it self a group under the composition of mappings.
- define the concept of an inner automorphism and prove that the group of inner automorphisms of a group G is isomorphic to the quotient group G/ $\mathbb{Z}(G)$, where $\mathbb{Z}(G)$ is the centre of G.
- determine all the automorphisms of a given cyclic group.

STRUCTURE:

3.1: INTRODUCTION:

In the previous lesson, we have learnt the concepts of a homomorphism and a bijective homomorphism, which is called an isomorphism. When an isomorphism is from a group G onto itself, it is called an automorphism of G. Automorphisms play an important role in the structure theory of groups. For any group G, the automorphisms of G form a group under the composition of mappings. On several occations, the structure of the group of automorphisms of G reveals that of the group G itself. In particular, when G is an infinite cyclic group, then there are eaxctly two automorphisms and when G is a finite cyclic group of order n, then there are exactly $\phi(n)$ number of automorphisms of G which is also equal to the number of generators of G. In this lesson, we shall have a detailed discussion on these topics.

3.2: THE GROUP OF AUTOMORPHISMS:

Isomorphisms of a group G onto itself are called automorphisms. In the following theorem we shall prove that the automorphisms of a given group form a group again. First, let us have the formal definition of an automorphism.

3.2.1. Definition : Let G be a group. Any bijective homomorphism of G onto G itself is called an automorphism of G. The set of all automorphisms of G will be denoted by Aut(G).

Note that the homomorphism given in example 2.2.5 is injective but not surjective and that given in example 2.2.8 is surjective but not injective. This says that surjective (onto) and injectivity (one-one) are both necessary for a homomorphism to become an

isomorphism or an automorphism.

3.2.2. Theorem: Let G be a group. Then the set Aut(G) of all automorphisms of G forms a group under the composition of mappings.

Proof : Let f, g $\in$ Aut(G). Then f and g are automorphisms of G and so f and g are isomorphism of G. Hence fog is an isomorphism and fog is an automorphism of G. Thus, the composition of mappings is a binary operation on the set Aut(G). Clearly, we have fo(goh) = (fog)oh for all f, g, h $\in$ Aut(G). Also, the identity mapping i_G, defined by i_G (a) = a for all a $\in$ G, is an automorphism of G and hence $i_G \in$ Aut(G) and for any f $\in$ Aut(G). $i_G \, o \, f = f = fo \, i_G$. Therefore i_G is the identity element of Aut(G). Further, for any f $\in$ Aut(G), f being a bijection, its inverse f^{-1} exists and f^{-1} is also an automorphism (2.2.3(1)). Since $fof^{-1} = i_G = f^{-1}of$, it follows that f^{-1} is the inverse of f in Aut(G). Thus Aut(G) is a group under the composition of mappings.

Every element of a group G has an inverse in G and hence $a \mapsto a^{-1}$ can be treated as a function of G into G. If $a^{-1} = b^{-1}$ for any a, b $\in$ G, then $a = (a^{-1})^{-1} = (b^{-1})^{-1} = b$ and for any y $\in$ G, $y^{-1} \in$ G and $(y^{-1})^{-1} = y$. That is the mapping $a \mapsto a^{-1}$ is a homomorphism and hence an automorphism of G**.**

3.2.3. Self Assessment Question: Prove that the following are equivalent for any group G.

(i) G is abelian

(ii) The mapping f : G $\to$ G, defined by f(a) = a^{-1} for any a $\in$ G is an automorphism of G

(iii) $(ab)^{-1} = a^{-1}b^{-1}$ for any a, b $\in$ G
(iv) $(ab)^2 = a^2b^2$ for any a, b $\in$ G

(v) There exist three consecutive integers n such that $(ab)^n = a^nb^n$ for all a, b $\in$ G

3.2.4. Theorem: Let G be a group and a $\in$ G. Let f be an automorphism of G. Then o(f(a)) = o(a).

Proof : Let f be an automorphism of G and a$\in$G. If a is of order zero. Then $a^n \neq e$ for any positive integer n and hence $f(a)^n = f(a^n) \neq f(e) = e$. (Since f is an automorphism and $a^n \neq e$)
So that f(a) is also of order zero. Now, suppose o(a) > o and let o(a) = n. Then n is the least positive integer such that $a^n = e$.
We have $f(a)^n = f(a^n) = f(e) = e$
And, for any positive integer m < n, $a^m \neq e$ and hence $f(a)^m = f(a^m) \neq f(e) = e$ (since f is an automorphism) Thus n is the least positive integer such that $f(a)^n = e$. Therefore, O(f(a)) = O(a).

3.2.5. Self Assessment question: If f : G $\to$ G$^{\prime}$ is an isomorphism of groups and a $\in$ G, then prove that the orders of a and f(a) in G and G$^{\prime}$ respectively are same.

3.3: INNER AUTOMORPHISMS:

In this section we shall introduce a special type of automorphisms known as inner automorphisms. With each element a in a group G, we shall associate an automorphism of G as defined in the following.

3.3.1. Theorem: Let G be a group and a $\in$ G. Define $f_a : G \to G$ by $f_a(x) = axa^{-1}$ for any x $\in$ G. Then f_a is an automorphism of G.

Proof: Let G be a group and a $\in$ G.
Define f_a: G$\to$ G as $f_a(x) = axa^{-1}$ for any x$\in$G.
Now we show that f_a is an automorphism of G.
For any x, y$\in$G, we have $f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)\, f_a(y)$.
And hence f_a is a homomorphism.
Also, $f_a(x) = f_a(y) \Rightarrow axa^{-1} \Rightarrow aya^{-1} \Rightarrow x = y$ (By the cancellation laws).
Therefore f_a is one-one. Finally to prove that f_a is a surjection. Let us take y$\in$G.
Then $a^{-1}ya \in G$ and $f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$. Therefore f_a is a surjection also.
Thus f_a is an isomorphism of G onto G; that is, f_a is an automorphism of G.

Note that the automorphism defined in the above theorem is called an inner automorphism of G and we denote the set of all inner automorphisms of G by I(G).

3.3.2. Definition: For any group G, the centre of G is defined as the set $\mathbb{Z}$ (G) = {a $\in$ G / ax = xa for all x$\in$G}.

3.3.3. Self Assessment Question: Prove that the centre $\mathbb{Z}$(G) of a group G is a normal subgroup of G.

3.3.4. Theorem: For any group G, the set I(G) of inner automorphisms of G is a group under the composition of mappings and $G/\mathbb{Z}(G) \cong I(G)$ where $\mathbb{Z}$(G) is the centre of G.

Proof: Let G be a group and Aut(G) be the set of all automorphisms of G. We know that Aut(G) is a group under the composition of mappings (see 3.2.2). We shall prove that the set I(G) of all inner automorphisms of G is a subgroup of Aut(G). For any a $\in$ G, we have $f_a \in$ I(G).
If $f_a, f_b \in$ I(G) with a, b $\in$ G, then $(f_a \circ f_b)(x) = f_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$
$f_e(x) = exe^{-1} = x = id(x)$
Hence $f_a \circ f_b = f_{ab}$ and f_e = id, the identity map.
Therefore $f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e = f_{a^{-1}a} = f_{a^{-1}} \circ f_a$ and hence $f_a^{-1} = f_{a^{-1}}$.
Now $f_a \circ f_b^{-1} = f_a \circ f_{b^{-1}} = f_{ab^{-1}} \in I(G)$.
Thus I(G) is a subgroup of Aut(G)
Now, let us define $\alpha : G \to I(G)$ by $\alpha(a) = f_a$ for any a$\in$G.
Then $\alpha(ab) = f_{ab} = f_a \circ f_b = \alpha(a)\,\alpha(b)$ for any a, b$\in$G. Therefore α is a homomorphism. Also, clearly α is a surjection (since any element of I(G) is of the from f_a for some a$\in$G)
Now by the fundamental theorem of homomorphisms (2.5.1),
we have $G/\mathrm{Ker}\,\alpha \cong I(G)$
Let us compute Ker α. By the definition of the kernel,
we have Ker α = {a$\in$G/α(a) = identity in I(G)}
= {a$\in$G/f_a(x) = x for all x$\in$G}

$= \{a \in G / axa^{-1} = x \text{ for all } x \in G\}$

$= \{a \in G / ax = xa \text{ for all } x \in G\} = \mathbb{Z}(G)$

Thus $G/\mathbb{Z}(G) \cong I(G)$.

3.3.5. Self Assessment Question : For any group G, prove the following.

(i) G is abelian if and only if I(G) is trivial

(ii) I(G) is a normal subgroup of Aut(G).

3.4: AUTOMORPHISMS OF A CYCLIC GROUP:

Let us recall that a group G is said to be cyclic if there exists an element a generating G, that is, $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$. In this case, a is called a generator of G.

There can be more than one generator of a group G. For example 1 and –1 are both generators of the group $\mathbb{Z}$ of integers under addition. In this section we shall determine all the automorphisms of a cyclic group and prove that there is a one-to-one correspondence between the automorphisms of a cyclic group G and the generators of G. Let us begin with the following :

3.4.1. Theorem: Let G be a group, f an automorphism of G and $a \in G$. Then a is a generator of G if and only if f(a) is a generator of G.

Proof : Given that G is a group and f is an automorphism of G and $a \in G$. Suppose a is a generator of G. Then $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$.
Now f is an automorphism and in particular, f is a surjection, so that f(G) = G.
Now we have $G = f(G) = \{f(a)^n / n \in \mathbb{Z}\} = \langle f(a) \rangle$
Therefore f(a) is a generator of G.
Conversely suppose that f(a) is a generator of G. Since f is an automorphism, f^{-1} is also an automorphism of G.
Since f^{-1} is an automorphism and since f(a) is a generator of G, we have $f^{-1}(f(a))$ is a generator of G and so a is a generator of G.

In the following, we shall determine all the automorphisms of a cyclic group. First, let us recall that for any integer n > 1, the set
$U_n = \{r \in \mathbb{Z}^+ / r < n \text{ and } r \text{ and } n \text{ are relatively prime}\}$ is a group under multiplication modulo n.
For example,

$U_2 = \{1\}$
$U_3 = \{1,2\}$
$U_4 = \{1,3\}$
$U_5 = \{1,2,3,4\}$
$U_{12} = \{1,5,7,11\}$
First, let us take up the case of a finite cyclic group.

3.4.2. Self Assessment Question: Determine the sets U_{30} and U_{13}.

3.4.3. Theorem: Let G be a finite cyclic group of order n > 1 and $G = \langle a \rangle$. Then
(1) An element $b \in G$ is a generator of G if and only if $b = a^r$ for some $r \in U_n$ (i.e, 0 < r < n and r is relatively prime to n)

(2) Aut(G) $\cong U_n$

Proof: Let G be a finite cyclic group of order n>1 and G = < a >

Let $b \in G$. Suppose b = a^r for some $r \in U_n$. Since r is relatively prime to n, these exist integers α and β such that $\alpha r + \beta n = 1$ and hence

$a = a^{\alpha r + \beta n} = (a^r)^{\alpha} . (a^n)^{\beta} = b^{\alpha}$ (Since a^n = e and b = a^r)

Since G = < a >, every element of G is of the form a^m, m $\in \mathbb{Z}$ and hence it follows that any element of G is of the form b^k, k $\in \mathbb{Z}$. Thus G = <b> and hence b is a generator of G.

Conversely suppose that b is a generator of G. Since G = < a > and o(G)=n, we have b = a^r for some 0 < r < n. Also a $\in$ G = <b> and hence a = b^s for some integer s. Now $a^{1-rs} = a.(a^r)^{-s} = ab^{-s} = e$ (since a = b^s) and hence o(a) divides 1–rs. Since o(a) = n, it follows that nt =1–rs or 1= nt + rs, which implies that r is relatively prime to n; that is, r $\in U_n$ and b = a^r.

2) Now we show that Aut (G) $\cong U_n$.

For any r$\in U_n$, define $g_r : G \to G$ by $g_r(x) = x^r$ for all x$\in$G

Then clearly g_r is a homomorphism. We shall verify that g_r is a bijection, so that it becomes an automorphism of G. Since r is relatively prime to n, there exist integers s and t such that rs + nt=1.

Now for any x, y$\in$G,

$g_r(x) = g_r(y) \Rightarrow x^r = y^r \Rightarrow (x^r)^s = (y^r)^s$ and

$(x^n)^t = e = (y^n)^t \Rightarrow x^{rs+nt} = y^{rs+nt} \Rightarrow x=y$ (since rs + nt = 1)

Therefore g_r is a injection. Further, by (1) above,

G = < a^r > and we have

y$\in$G $\Rightarrow$ y = $(a^r)^m$ for some integer m.

$\Rightarrow y = (a^m)^r = g_r(a^m)$ and $a^m \in G$.

Therefore g_r is a surjection and hence g_r is an automorphism of G.

Now, define the mapping $\psi : U_n \to$ Aut(G) by

$\psi(r) = g_r$ for any r$\in U_n$. First we show that ψ is a homomorphism

Note that o(a) = n and for any m $\in \mathbb{Z}$, a^m = e if and only if n divides m. For any r, s$\in U_n$, let rs = t, where t is the remainder obtained by dividing the usual product rs with n; i.e, if rs = qn +t, o $\leq$t <n, then rs = t. Also note that x^n = e for all x$\in$G.

Now, $(g_r \circ g_s)(x) = g_r(g_s(x)) = (x^s)^r = x^{rs} = x^{qn+t} = (x^n)^q . x^t = e.x^t = x^t = g_{rs}(x)$ for all x$\in$G.

Therefore $g_r \circ g_s = g_{rs}$ and hence ψ is a homomorphism of U_n into Aut(G).

Now we show that ψ is an injection.

For any r, s $\in U_n$, consider $\psi(r) = \psi(s) \Rightarrow g_r = g_s$

$\Rightarrow g_r(a) = g_s(a) \Rightarrow a^r = a^s \Rightarrow a^{r-s} = e$

$\Rightarrow$ r – s = o (Since r–s < n and o(a) = n)

$\Rightarrow$ r = s

Therefore ψ is an injection.

No we show that ψ is a surjection.

Let f$\in$Aut(G). Then by 2.4.1 Theorem, f(a) is a generator of G. BY (1), f(a) = a^r for some

$r \in U_n$. If $x = a^m \in G$, then $f(x) = f(a^m) = f(a)^m = (a^r)^m = (a^m)^r = x^r = g_r(x)$.

Therefore $f = g_r = \psi(r)$ and hence ψ is a surjection. Thus ψ is an automorphism of G and so $Aut(G) \cong U_n$.

3.4.4. Self Assessment Question: Determine all the automorphisms of the group $\mathbb{Z}_{10}$ of integers modulo 10.

3.4.5. Theorem: Let G be an infinite cyclic group. Then Aut(G) consists only two automorphisms, namely, the identity mapping and the map $x \mapsto x^{-1}$.

Proof : Given that G is an inifinite cyclic group. Then $G = < a >$ for some $a \in G$ and $a^n \neq e$ for all non-zero integers n. Let f be an automorphism of G.
Then $f(a) \in G = < a >$ and hence $f(a) = a^n$ for some $n \in \mathbb{Z}$. By 3.4.1 theorem, f(a) is a generator of G and $G = < f(a) >$.
Therefore $a = f(a)^m = (a^n)^m = a^{nm}$ and hence $nm = 1$ which implies that either $n = 1 = m$ or $n = -1 = m$. Therefore $f(a) = a$ or $f(a) = a^{-1}$.
If $f(a) = a$, then $f(x) = x$ for all $x \in G$ and hence f is an identity mapping. If $f(a) = a^{-1}$, then $f(x) = x^{-1}$ for all $x \in G$. Thus, the identity mapping and the mapping $x \mapsto x^{-1}$ are the only automorphisms of G.

3.4.6. Self Assessment Question: Determine all the automorphisms of the group Z of integers.

3.4.7. Self Assessment Question: If G is an inifinite cyclic group, prove that $Aut(G) \cong \mathbb{Z}_2$.

3.5. MODEL EXAMINATION QUESTIONS:

3.5.1. Prove that the set Aut(G) of all automorphisms of a group G forms a group under composition of mappings.

3.5.2. Define the notion of the centre $\mathbb{Z}(G)$ of a group G and prove that $G/\mathbb{Z}(G)$ is isomorphic to the group I(G) of all inner automorphic of G.

3.5.3. For a cyclic group G of order n, prove that $Aut(G) \cong U_n$.

3.5.4. Determine all the automorphisms of an infinite cyclic group.

3.6 SUMMARY:

In this lesson, we have learnt the concept of an automorphism of a group G and proved that the set Aut(G) of all automorphisms of G is a group under the compositon of mappings. Also, we have defined the notion of an inner automorphism of a group G and proved that these form a group which is isomorphic to the quotient group $G/\mathbb{Z}(G)$, where $\mathbb{Z}(G)$ is the centre of G. Finally, we have completely determined all the automorphisms of a cyclic group. In particular, if G is a cyclic group of order n, we have proved that Aut (G) is isomorphic to the group U_n of positive integers less than n and relatively prime to n.

3.7 TECHINICAL TERMS:

- Automorphism
- Inner Automorphism
- The centre $\mathbb{Z}(G)$
- Cyclic group
- The group U_n
- The group $\mathbb{Z}_n$

3.8 ANSWERS TO SELF ASSESSMENT QUESTIONS:

3.2.3: (1) $\Rightarrow$ (2)
For any a, b $\in$ G, consider $f(ab) = (ab)^{-1} = b^{-1}a^{-1}$
$= a^{-1}b^{-1}$ (since G is abelian)
$= f(a)\, f(b)$
Therefore f is a homomorphism
Let $a \in G$. Then $a^{-1} \in G$. Consider $f(a^{-1}) = (a^{-1})^{-1} = a$.
Therefore f is a surjection (onto)
Further, for any a, $b \in G$, consider $f(a) = f(b)$
$\Rightarrow a^{-1} = b^{-1} \Rightarrow a = b$
Therefore f is an injection. Thus f is an automorphism of G.
(2) $\Rightarrow$ (3).
For any a, $b \in G$, consider $(ab^{-1}) = f(ab) = f(a)\, f(b) = a^{-1}b^{-1}$
There fore $(ab)^{-1} = a^{-1}b^{-1}$
(3)$\Rightarrow$ (4)
For any a, b $\in$ G, consider $(ab) = (a^{-1})^{-1}(b^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}\,(a^{-1})^{-1} = ba$
Consider $a^2b^2 = a(ab)b = a(ba)b = (ab)^2$
so $a^2b^2 = (ab)^2$
(4)$\Rightarrow$ (5)
Let a, b $\in$ G, we have $(ab)^0 = e = e.e = a^0b^0$
$(ab)^1 = a.b = a^1.b^1$ and $(ab)^2 = a^2b^2$
There fore 0, 1 and 2 are three consecutive integers n
such that $(ab)^n = a^nb^n$ for any a, $b \in G$
(5) $\Rightarrow$ (1)
Let n be an integer such that
$(ab)^{n-1} = a^{n-1}\, b^{n-1}$, $(ab)^n = a^nb^n$ and $(ab)^{n+1} = a^{n+1}\, b^{n+1}$ for all a, b $\in$ G.
Now for any a, $b \in G$, consider $a^{n-1}(ab^{n-1})b = a^nb^n$
$= (ab)^n = (ab)^{n-1}(ab) = a^{n-1}(b^{n-1}a)b$
$\Rightarrow ab^{n-1} = b^{n-1}a$ (By cancellation laws)
similarly $ab^n = b^na$
Now, consider $(ab)b^{n-1} = ab^n = b^na = b(b^{n-1}a) = b(ab^{n-1})$
$= (ba)b^{n-1} \Rightarrow ab = ba$ (cancellation laws)
Hence G is abelian.

3.2.5: Suppose $f: G \to G^1$ is an isomorphism of groups and a $\in$ G. Now we show that the order of a and the order of f(a) are the same.
Assume that o(a) = n and o(f(a)) = m. Then $a^n = e$ and $(f(a))^m = e^1$, where e and e^1 are the identities in G and G^1 respectively
Since f is an isomorphism of G onto G^1,
we have $a^t = e \Leftrightarrow f(a^t) = f(e) = e^1 \Leftrightarrow f(a)^t = e^1$ for any positive integer t $\rightarrow$(1)

From (1), we have $a^n = e \Leftrightarrow f(a)^n = e^1$
Therefore m/n (since o(f(a)) = m
Also from (1), we have $(f(a))^m = e^1 \Leftrightarrow a^m = e$
Therefore n/m (since o(a) = n)
Hence m = n, that is, o(a) = o(f(a)).

3.3.3: Consider the centre $\mathbb{Z}(G)$ of the group G. Now we show that $\mathbb{Z}(G)$ is a normal subgroup of G.
$\mathbb{Z}(G) \neq \phi$ since $e \in \mathbb{Z}(G)$
Now for any a, b$\in \mathbb{Z}(G)$ and x∈G, consider (ab)x = a(bx)
= (bx)a = (xb)a = x(ba) = x(ab)
Therefore ab$\in \mathbb{Z}(G)$
Now let a$\in \mathbb{Z}(G) \Rightarrow$ ax = xa
Consider ax = xa $\Rightarrow axa^{-1} = xaa^{-1} = xe = x$
$\Rightarrow axa^{-1} = x \Rightarrow a^{-1}axa^{-1} = a^{-1}x \Rightarrow exa^{-1} = a^{-1}x$
$\Rightarrow xa^{-1} = a^{-1}x$
Therefore $a^{-1} \in \mathbb{Z}(G)$
Thus Z(G) is a subgroup of G.
Now for any a$\in \mathbb{Z}(G)$and g ∈ G,
we have $gag^{-1} = agg^{-1} = a \in \mathbb{Z}(G)$
Hence $\mathbb{Z}(G)$is a normal subgroup of G.

3.3.5. Let G be any group

(i) G is abelian ⇔ ab = ba for any a, b ∈ G
⇔ G = $\mathbb{Z}(G)$ ⇔ G/ $\mathbb{Z}(G)$ is trivial
⇔ I(G) is trivial (by 3.3.4)

(ii) $f_a \in I(G)$ and h∈ Aut(G)
Then for any x∈G, $(ho\ f_a\ oh^{-1})(x) = h(f_a\ (h^{-1}(x))$
$= h(ah^{-1}(x)a^{-1}) = h(a)\ h(h^{-1}(x))h(a^{-1})$
$= h(a)\ xh(a)^{-1} = f_{h(a)}(x)$
Therefore $hof_a\ oh^{-1} = f_{h(a)} \in I(G)$
Thus I(G) is a normal subgroup of Aut (G).

3.4.2: U_{30} = {1,7,11,13,17,19,23,29}
U_{13} = {1,2,3,4,5,6,7,8,9,10,11,12}

3.4.4: Consider U_{10} ={1,3,7,9}
By 3.4.3 theorem (2), Aut ($\mathbb{Z}_{10}$) ≅ U_{10}. Since o(U_{10})=4,
there are four automorphisms of $\mathbb{Z}_{10}$. These are x↦ x, x↦ x^3, x↦ x^7 and x↦ x^9
Note that 9x is the inverse of x for any x∈ $\mathbb{Z}_{10}$.

3.4.6. By 3.4.5 theorem, the only automorphisms of $\mathbb{Z}$ are the mappings x ↦ x and x↦ –x (since $\mathbb{Z}$ is infinite cyclic groups).

3.4.7. Let G be an infinite cyclic group.Then Aut (G) = {id, f} where id is the identity mapping of G and f is defined by $f(x) = x^{-1}$ for all x∈G. Any group of order 2 must be isomorphic to $\mathbb{Z}_2$ and hence Aut(G) = $\mathbb{Z}_2$.

3. 9 SUGGESTED READINGS:

1) I.N. Herstein, ‘Topics in Algebra’, Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, ‘Algebra’, Springer- Verlag, New York, 1974.
4) Serge Lang, ‘Algebra’, Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. V. Samba Siva Rao

LESSON -4

CAYLEY'S THEOREM

OBJECTIVES:

Objectives of this lesson are to

- prove the bisections of any set onto itself from a group.
- state and prove theCayley's theorem.
- quote certain important applications of Cayley's theorem.

STRUCTURE:

4.1: INTRODUCTION:

Most of the groups when they were first identified, were in the form of a set of transformations of a particular mathematical structure. Most finite groups appeared as groups of bijections of an n element set onto itself for some positive integer n. It is known that the S(X) of all bijections of a set X onto itself forms a group under the usual composition of mappings. The English mathematician Cayley's first noted that any abstract group can be viewed as a subgroup of the group S(X) for a suitable set X. In this lesson, we shall prove this theorem of Cayley and derive certain important consequences.

4.2: GROUP OF PERMUTATIONS:

The Cayley's theorem states that any group can be identified with a subgroup of the group of permutations on a suitable set. Before taking up the proof of the Cayley's theorem, we shall first prove that the permutations on any set from a group. Let us begin with the following.

4.2.1. Definition: For any non-empty set X, any bijection of X onto itself is called a permutation or symmetry on X. The set of all permutations on X will denoted by A(X).

4.2.2. Theorem: For any non-empty set X, A(X) is a group under the composition of mappings.

Proof: Let us recall that an injective (one-one) and surjective (onto) function is called a bijection and that the composition of two dijections is again bijection.

Now, let X be a non-empty set. Then the composition 'o' is a binary operation on A(X). Clearly 'o' is an associative operation. Also, the map id: $X \to X$, defined by $id(x) = x$ for all $x \in X$, acts as the identity element in A(X); that is, $f \circ id = f = id \circ f$

For any $f \in A(X)$. Further, for any bijection $f: X \to X$, we can define $f^{-1}: X \to X$ by

$f^{-1}(y) = x$ if and only if $f(x) = y$ (Since f is a bijection, there exists unique x in X such that $f(x) = y$). Then, clearly f^{-1} is a permutation on X and $f \circ f^{-1} = id = f^{-1} \circ f$

Therefore, each element of A(X) has inverse. Thus A(X) is a group under the composition o of mappings.

4.2.3. Self Assessment Question: List all the elements of A(X), where X = {1, 2, 3}.

4.3: CAYLEY'S THEOREM:

In this section, we shall prove that any abstract group can be identified with a group of permutations on a suitable set X (that is a subgroup of A(X)).

4.3.1. Theorem (Cayley's Theorem): Any group is isometric to a group of permutations on a set.

Proof: Let G be a group, that is, G is a non-empty set together with a binary operation satisfying the axioms of group. Take X to be the set G, ignoring the binary operation on it. For each $a \in G$, define $t_a: X \to X$ by $t_a(x) = ax$ for all $x \in X$. Note that X = G and the product ax in G is written as ax. Then t_a is a bijection; for

$t_a(x) = t_a(y)$ for any $x, y \in X$

$\Rightarrow ax = ay$

$\Rightarrow x = y$

(by cancellation laws) and, for any $y \in X$, $a^{-1}y \in X$. And $t_a(a^{-1}y) = a(a^{-1}y) = y$

Therefore $t_a \in A(X)$, the group of permutations on X.
Let $H = \{ t_a / a \in G \}$

we shall prove the following for any $a, b \in G$:

(1) $t_a \circ t_b = t_{ab}$

(2) $t_e = id$, the identify map on X

(3) $t_a^{-1} = t_{a^{-1}}$

For any $x \in G$, consider

$t_a \circ t_b(x) = t_a(t_b(x)) = a(bx) = (ab)x = t_{ab}(x)$
Therefore, $t_a \circ t_b = t_{ab}$.
Also $t_e(x) = ex = x = id(x)$ for any $x \in G$ and hence $t_e = id$
Now, $t_a \circ t_{a^{-1}} = t_{aa^{-1}} = t_e = id = t_{a^{-1}a} = t_{a^{-1}} \circ t_a$ and
hence $t_a^{-1} = t_{a^{-1}}$

These (1), (2) & (3) imply that H is a subgroup of A(X)

We shall prove that $G \cong H$
Define $f: G \to H$ by $f(a) = t_a$ for any $a \in G$

Since every element in H is of the form t_a for some $a \in G$, f is a surjection.

Also, by(1) above, $f(ab) = t_{ab} = t_a \circ t_b = f(a) \circ f(b)$ for any $a, b \in G$ and hence f is a homomorphism. Also, for any $a, b \in G$, $f(a) = f(b)$ that implies $t_a = t_b$

that implies $t_a(e) = t_b(e) \Rightarrow ae = be \Rightarrow a = b$.

Therefore f is an injection, Thus f: G $\rightarrow$ H is an isomorphism and hence G is isomorphic to the subgroup H of A(X).

The above theorem enables us to identify any abstract group as a more concrete object, namely, as a group of permutations. However, there are certain short comings; for if G is a group of order n, then the group A(X), considered in the proof of the above theorem, has n! elements. Our group G of order n is some what lost in the group A(X). Which is huge in comparison to G. Now, one can ask the question: Can we find a more economical X so as to find smaller A(X) in which G can be identified This is accomplished in the following, which is actually a generalization of theorem 4.3.1

4.3.2. Theorem: Let G be a group and H a subgroup of G. Let X be the set of all left cosets of H in G. Then there is a homomorphism f of G into A(X) such that the kernel of f is the largest normal subgroup of G which is contained in H.

Proof: Given that G is a group and H is a subgroup of G. Also given that X = {xH /x $\in$ G} For any a $\in$ G, define g_a : X$\rightarrow$ X by g_a (xH) = (ax)H for any xH $\in$ X. First notice that, g_a is well-defined, in the sense that g_a (xH) does not depend on x, but it depends on the whole coset xH, in which x is a particular element.

For xH = yH

$\Rightarrow x^{-1}y \in H$

$\Rightarrow (ax)^{-1}(ay) = x^{-1}a^{-1}ay = x^{-1}y \in H$

$\Rightarrow (ax)H = (ay)H$

$\Rightarrow g_a(xH) = g_a(yH)$

Therefore g_a is well defined Now we shall verify that g_a is a bijection of X onto itself

For any xH, yH belongs to X, consider

$g_a(xH) = g_a(yH)$

$\Rightarrow (ax)H = (ay)H$

$\Rightarrow (ax)^{-1}(ay) \in H$

$\Rightarrow x^{-1}y = (ax)^{-1}(ay) \in H$

$\Rightarrow xH = yH$

Therefore g_a: X$\rightarrow$X is an injection.

Also, for any yH$\in$X $(a^{-1}y)H \in X$ and

$g_a((a^{-1}y)H) = (a(a^{-1}y))H = yH$

Therefore g_a is a surjection and hence g_a is a permutation on X; that is $g_a \in A(X)$ for each a $\in$ G. Now define f: G $\rightarrow$ A(X) by f(a) = g_a for any a$\in$G For any a, b$\in$G and xH $\in$ X, we have $(g_a \circ g_b)(xH) = g_a(g_b(xH)) = (a(bx))H = (ab)xH = g_{ab}(xH)$ and hence $g_a \circ g_b = g_{ab}$ This says that f(ab) = f(a)f(b). Therefore f is a homomorphism. Now, let us evaluate kernel of f.

$\ker f = \{a \in G / f(a) = id\} = \{a \in G / g_a = id\}$

$= \{a \in G / g_a(xH) = xH \text{ for all } xH \in X\}$

$= \{a \in G / axH = xH \text{ for all } x \in G\}$

$= \{a \in G / x^{-1}ax \in H \text{ for all } x \in G\}$

Being the kernel of a homomorphism, Ker f is a normal subgroup of G (see 2.3.3)and clearly ker f $\subseteq$ H(for, a $\in$ Ker f $\Rightarrow x^{-1}ax \in H$ for all x $\in$ G $\Rightarrow e^{-1}ae \in H \Rightarrow a \in H$)

Also, if N is a normal subgroup of G which is contained in H, then N $\subseteq$ Ker f (for, a $\in$ N $\Rightarrow$ $x^{-1}ax \in N \subseteq H$ for all x $\in$ G $\Rightarrow$ a $\in$ Ker f).

Thus, ker f is the largest normal subgroup of G which is contained in H.

4.3.3.Self Assessment Questions: Deduce Cayley's theorem from the above theorem 4.3.2.

4.4: APPLICATIONS OF CAYLEY'S THEOREM:

We shall apply Cayley's theorem of the previous section in proving certain results on the structure of certain finite groups. Let us begin with the following.

4.4.1. Definition: A group G is called simple if it has no non trivial normal subgroups; that is, if {e} and G are the only normal subgroups of G.

4.4.2. Examples: The trivial group {e} is clearly simple. Also, any group of order a prime is simple, for if G is a group of order p and p is prime and if H is a subgroupof G, then O(H) divides O(G) = p (by Lagrange's theorem) and hence O(H) = 1 or p. So that H = {e} or H = G.

4.4.3. Self Assessment Question: For any positive integer n>1, prove that the group Z_n is simple if and only if n is a prime number.

Let us recall that the order of a subgroup H of a finite group G divides the order of G and O(G)/O(H) is equal to the number of distinct left (right) cosets of H in G. Also, O(G)/O(H) is known as the index of H in G and is denoted by i(H).We shall use theorem 4.3.2 in proving the following.

4.4.4. Theorem: Let H be a proper subgroup of a finite group G such that O(G) does not divide i(H)!. Then H contains a non trivial normal subgroup of G and in particular, G is not simple.

Proof: Given that H is a proper subgroup of a finite group G such that O(G) does not divide i(H)!. Let X be the set of all left cosets of H in G. The $|X|$ = i(H) and O(A(X)) = i(H)!. By theorem 4.3.2, there exits a homomorphism f :G $\rightarrow$ A(X) such that ker f is the largest normal subgroup of G which is contained in H. Since H $\neq$ G and ker f $\subseteq$ H, it follows that Ker f is a proper normal subgroup of G. If kerf = {e}, then f is a monomorphism and hence G $\cong$ f(G) and f(G) is a subgroup of A(X) and therefore O(G) = O(f(G)) divides O(A(X)) = i(H)!, which is a contradiction to the hypothesis. Therefore Ker f $\neq$ {e}. Thus H contains a non trivial normal subgroup of G(namely, Ker f) which implies that G is not simple.

4.4.5. Example: Suppose G is a group of order 36 and G has a subgroup H of order 9. Then i(H) = $\frac{O(G)}{O(H)}$ = 4 and hence O(G) does not divide i(H)!. Therefore there is a nontrivial normal subgroup of G contained in H(by theorem 4.4.4) and G is not simple.

4.4.6. Self Assessment Question: Suppose G is a group of order 175 and G has a subgroup of order 25. Then prove that G is not simple.

4.4.7. Example: Let H be a subgroup of order 11 in a group G of order 99.Then i(H) = $\frac{O(G)}{O(H)}$ = $\frac{99}{11}$ = 9 and O(G) does not divide i(H)!. Then, by theorem 4.4.4, there exists a non trivial normal subgroup N of G which is contained in H. Since O(H) = 11, which is a prime number and since O(N) is a divisor of O(H), it follows that O(N) = O(H) (note that O(N) > 1, since N is non trivial) and hence N = H. Thus H is a normal sub group of G. To summaries, any subgroup of order 11in a group of order 99 is normal.

4.4.8. Self Assessment Question: Prove that any subgroup of order 13 in a group of order 65 is normal.

4.4.9. Theorem: Any non abelian group of order 6 is isomorphic to A(X), where X is a three element set.

Proof: Let G be a non-abelian group of order 6. Then G has an element of order 2(See4.4.10). Let $a \in G$ be an element of order 2. That is, $e \neq a \in G$ and $a^2 = e$.
Put H = {e, a}

Then H is a subgroup of order 2 in G and $i(H) = \frac{O(G)}{O(H)} = 3$. Let X be the set of left cosets of H in G. Then A(X) is a group of order 3!. (since X has 3 elements); that is, o(A(X)) = 3!. By Theorem 4.3.2, there is a homomorphism $f: G \to A(X)$ such that ker f is the largest normal subgroup of G which is contained in H. In particular, Ker $f \subseteq H$ and Ker f is a normal subgroup of G. Since O(H) = 2, it follows that ker f = {e} or Ker f = H. We shall argue that ker $f \neq H$.

Otherwise, suppose that Ker f = H. Then H is a normal subgroup of G and hence $xax^{-1} \in H$ for all $x \in G$. But $xax^{-1} \neq e$ (since $a \neq e$) and therefore $xax^{-1} = a$. This implies that xa = ax for all $x \in G$. Therefore $a \in Z(G)$, the centre of G and $H \subseteq Z(G) \subseteq G$.

Since O(H) = 2, we have that 2 divides O(Z(G)) and O(Z(G)) is a divisor of O(G) = 6. From these, it follows that O(Z(G)) = 2 or 6. But $O(Z(G)) \neq 6$ (for, since G is a non abelian). Z(G) is a proper subset of G. Therefore O(Z(G)) = 2 and H = Z(G). Now, choose $b \in G$ such that $b \notin H$ and consider the normalizer N(b) of b;

i.e, $N(b) = \{x \in G / bx = xb\}$

Then Z(G) is a proper subgroup of N(b)(Since $b \in N(b)$ and $b \notin H = Z(G)$) and hence 2 is a proper divisor of O(N(b)) and O(N(b)) is a divisor of O(G) = 6. Therefore O(N(b)) = 6 = O(G) and hence G = N(b) so that bx = xb for all $x \in G$; that is, $b \in Z(G) = H$, which is a contradiction to the choice of b.Thus Ker $f \neq H$ and hence Ker f = {e}. Therefore, f is a monomorphism of G into A(X) and hence $G \cong f(G) \subseteq A(X)$

But O(f(G)) = O(G) = 6 = O(A(X))

Therefore, f(G) = A(X) and hence $f: G \to A(X)$ is a surjection. Thus f is an isomorphism of G onto A(X) and $G \cong A(X)$.

4.4.10. Self Assessment Question: Prove that any finite group of even order has an element of order 2.

Actually, we prove later a more general result than 4.4.10. If G is a finite group and P is a prime number dividing O(G), then G has an element of order p. This is nothing but the Cauchy's theorem (2.6.1) for a general group which will be proved later. However, we can try to prove 4.4.10 by elementary methods.

4.5. MODEL EXAMINATION QUESTIONS:

4.5.1. Prove that the set A(X) of permutations on a set X is a group under the composition of mappings.

4.5.2. State and prove the Cayley's theorem.

4.5.3. Let H be a subgroup of a group G and X be a set of all left cosets of H in G. Then prove that there is a homomorphism f of G into the permutation group A(X) such that Ker f is the largest normal subgroup of G that contained in H.

4.5.4. Let H be a proper subgroup of a finite group G such that O(G) does not divide i(H)!. Then prove that G is not simple.

4.5.5. Prove that any non abelian group of order 6 is isomorphic to the group ofpermutations on a three element set.

4.6 SUMMARY:

In this lesson, we have learnt that the permutations on any set form a group under the composition of mappings and the Cayley's theorem which states that any group is isomorphic to a group of permutations on a suitable set. We have also proved a generalized version of cayley's theorem and applied this to prove that certain groups are not simple; in particular, we have proved that any non abelian group of order 6 is isomorphic to the group of permutations on a three element set.

4.7 TECHNICAL TERMS:

- Permutations
- Group of permutations A(X)
- Cayley's theorem
- Simple group.

4.8 ANSWERS TO SELF ASSESSMENT QUESTIONS:

4.2.3 Given that X = {1, 2, 3}. Consider the maps id, α, β of X into X as are defined below.

id(1) = 1	$\alpha(1) = 2$	$\beta(1) = 2$
id(2) = 2	$\alpha(2) = 1$	$\beta(2) = 3$
id(3) = 3	$\alpha(3) = 3$	$\beta(3) = 1$

Then id, $\alpha, \beta \in$ A(X) and α o β, β o α and β^2 are all other elements in A(X). Thus A(X) = {id, α, β, α o β, β o α, β^2 }.

4.3.3: Take H = {e} in theorem 4.3.2. Then Ker f $\subseteq$ {e} and hence Ker f = {e}, so that f is an injective homomorphism of G into A(X), where X is the set of all left cosets of H in G. Thus G is isomorphic to a group of permutations on a set X. Note that, in this case X is bijective with G.

4.4.3: Suppose n is a prime number. For any subgroup H of Z_n, O(H) is a divisor of $O(Z_n)$ = n and hence O(H) = 1 or n so that H = {0} or H = Z_n. Therefore Z_n has no nontrivial (normal) subgroups and hence Z_n is simple. Conversely, suppose that n is not a prime number. Then n = mk for m, k > 1.
Consider H = {m, 2m,……, (k-1)m}. Then H is a non trivial normal subgroup of Z_n and therefore Z_n is not a simple group.

4.4.6: Given that G is a group of order 175 and G has a subgroup H of order 25. Then i(H) = $\frac{O(G)}{O(H)}$ = 7 and O(G) does not divide i(H)! By theorem 4.4.4, there exists a non trivial normal subgroup N of G such that $N \subseteq H$. Since $H \neq G$, it follows that $N \neq G$. Thus G is not simple.

4.4.8. Imitate the argument given in 4.4.7.

4.4.10: Let G be a finite group and O(G) be even. If G is an abelian group, then we can use the Cauchy's theorem (2.6.1). If the Cauchy's theorem (2.6.1) is proved for a arbitrary group, then we are through (Infact we prove 2.6.1 for a general group later). But here is an elementary proof.

For each $a \in G$, let $A_a = \{a, a^{-1}\}$. Then the A_a's form a partition of G, that is, for any a, $b \in G$, either $A_a = A_b$ or $A_a \cap A_b = \phi$ and $\bigcup_{a \in G} A_a$, A_a may consists of only one element(This happens when $a = a^{-1}$). For example $A_e = \{e\}$. If, for each $a \neq e$, A_a is a two element set, then O(G) = 2m+1 for some positive integer m, which is a contradiction to the hypothesis that O(G) is even. Therefore there exists $a \neq e$ such that A_a is a singleton set; that is, $a = a^{-1}$.

Thus $a \neq e$ and $a^2 = e$ and hence a is of order 2.

4.9 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.V.Samba Siva Rao

LESSON -5

PERMUTATION GROUPS

OBJECTIVES:

Objectives of this lesson are to

- define the concept of the symmetric group S_n of degree n.
- prove that any permutation on a finite set is a product of disjoint cycles.
- define the notion of the alternating group A_n.
- prove that A_n is a normal subgroup of index 2 in S_n.

STRUCTURE:

5.1: INTRODUCTION:

In the previous lesson, we have proved that the set A(X) of permutations on any set X is a group under the composition of mappings and also proved the Cayley's theorem which state that any abstract group is isomorphic to a subgroup of the permutation group A(X) for a suitable set X, infact we have taken X to be the underlying set of the group itself. In particular, any finite group is isomorphic to a group of permutations on a finite set. For this reason, the groups of permutations on finite sets become prominent in the theory of structure of finite groups. In this lesson, we discuss these groups and prove certain important properties.

5.2: THE SYMMETRY GROUP S_n:

If X and Y are sets and if there is a bijection $\alpha : X \to Y$, then the groups A(X) and A(Y) of permutations on X and Y respectively are isomorphic under the isomorphism $f \longmapsto \alpha \circ f \circ \alpha^{-1}$. Therefore, if X is a finite set with n elements, then the permutation groups A(X) and $A(I_n)$ are isomorphic, where $I_n = \{1, 2, 3, \ldots, n\}$.

5.2.1. Definition: Let n be any positive integer and $I_n = \{1, 2, 3, \ldots, n\}$. Then the permutation group $A(I_n)$ is called the symmetric group of degree n and is denoted by S_n.

The elements of the symmetric group S_n are permutations on $I_n = \{1, 2, 3, ..., n\}$. If $f \in S_n$, then f(1), f(2), ..., f(n) are n distinct elements of I_n and hence $I_n = \{f(1), f(2),....., f(n)\}$. For convenience, we describe $f \in S_n$ by

$$f = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{bmatrix}$$

For example $f \in S_9$ defined by f(1) = 4, f(2) = 6, f(3) = 9, f(4) = 5, f(5) =7, f(6) = 1, f(7) = 3, f(8) = 2 and f(9) = 8 is denoted by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 5 & 7 & 1 & 3 & 2 & 8 \end{pmatrix}$$

5.2.2. Self Assessment Question: Let $f \in S_7$ be given by

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 6 & 2 & 3 & 4 \end{pmatrix}$, then what are f(3) and f(6).

If f and g are permutations in S_n, then recall that $f \circ g$ is defined by $(f \circ g)(i) = f(g(i))$ and that S_n is a group under this composition of mappings.

5.2.3. Self Assessment Question: Let f and $g \in S_8$ be given by

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 3 & 4 & 6 & 8 & 2 \end{pmatrix}$ and

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 8 & 3 & 2 & 5 & 6 \end{pmatrix}$ then complete $f \circ g$ and f^{-1}

5.2.4. Self Assessment Question: Compute $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 1 & 3 & 2 \end{pmatrix}$ in S_6

5.2.5. Note: Let n and m be positive integers and n < m. Define $\theta : S_n \to S_m$ by

$$\theta(f)(i) = \begin{cases} f(i) \text{ if } 1 \le i \le n \\ i \text{ if } n < i \le m \end{cases}$$

for any $f \in S_n$. Then as you can easily check, θ is a monomorphism. In other words, S_n is isomorphic to a subgroup of S_m and hence, we can identify permutations in S_n with those in S_m.

5.2.6. Example:

The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$ in S_5 can be identified with $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 3 & 2 & 6 & 7 & 8 \end{pmatrix}$ in S_8.

5.3: CYCLES AND TRANSPOSITIONS:

In this section, we shall discuss a special type of permutations, namely cycles. These cycles play a very important role in the study of permutations. Infact, we shall prove that any permutation can be expressed as a product of disjoint cycles in a unique way, in some sense. Let us begin with the following.

5.3.1. Definition: Let n be any positive integer and $a_1, a_2, \ldots\ldots\ldots, a_r$ be distinct elements in $I_n = \{1, 2, \ldots, n\}$ and r > 1. Let f: $I_n \to I_n$ be defined by

$$f(a) = \begin{cases} a_{i+1} & \text{if } a = a_i \ 1 \le i < r \\ a_1 & \text{if } a = a_r \\ a & \text{if } a \ne a_i \ 1 \le i \le r \end{cases}$$

Then f is a permutation on I_n and is denoted by $(a_1 a_2 \ldots\ldots\ldots a_r)$. This is called an r-cycle or a cycle of length r.

For example, the cycle f = (3 4 2 6 8) is a permutation in S_8 (or in S_n for $n \ge 8$) defined by

f(3) = 4, f(4) = 2, f(2) = 6, f(6) = 8, f(8) = 3 and f(a) = a for all $a \notin \{3,4,2,6,8\}$.

Note that the cycles (3 4 2 6 8) and (2 6 8 3 4) are same.

5.3.2. Self Assessment Question:
Let f = (5 2 7 3 6 8) a cycle in S_{10}. Then what is f(i) for any $1 \le i \le 10$?

5.3.3. Self assessment question: is the permutation
f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 3 & 7 & 4 & 6 & 9 & 2 & 8 \end{pmatrix}$ a cycle in S_9? If so, write f in the cycle notation.

5.3.4. Definition: Two cycles f = (a_1, a_2, ..., a_r) and g = (b_1, b_2, ..., b_s) are said to be disjoint if $a_i \neq b_j$ for any $1 \le i \le r$ and $1 \le j \le s$; that is, f and g are called disjoint if the sets {a_1, a_2, ..., a_r} and {b_1, b_2, ..., b_s} have no common elements.

5.3.5. Examples: The cycles (4 6 3 5 2) and (7 1 8 9) are disjoint while the cycles (5 3 4 2 8) and (4 1 6 7) are not disjoint.

5.3.6. Note: If f and g are disjoint cycles in S_n, then f o g = g o f for, if f = (a_1a_2.....a_r) and g = (b_1b_2.....b_s) with $a_i \neq b_j$, then (f o g)(a) = f(a) = a = g(a) = (g o f)(a), if $a \neq a_i$ and $a \neq b_j$
and f o g(a_i) = f(a_i) = a_{i+1} = g(a_{i+1}) = g o f(a_i) and similarly

(f o g) (b_j) = (g o f) (b_j) Thus f o g = g o f. This is to say that any two disjoint cycles commute.

Now we shall prove the following theorem which express any permutation as a product of disjoint cycles. Remember that an r-cycle is defined only where r > 1.

5.3.7.Theorem: Let f be any non-identity permutation in S_n. Then f can be expressed as a product of disjoint cycles each of length >1. Also, this expression is unique in the sense that, if

$f = \alpha_1 \text{ o } \alpha_2 \text{ o } \ldots\ldots\text{o } \alpha_k$ and

$f = \beta_1 \text{ o } \beta_2 \text{ o } \ldots\ldots\text{o } \beta_m$

where α_i 's and β_j 's are disjoint cycles, then k = m and there is a permutation σ in S_m such that $\beta_j = \alpha_{\sigma(j)}$ for each $1 \le j \le m$.

Proof: Given that f is a non-identity permutation in S_n. Write T = {$a \in I_n$ / $f(a) \neq a$}. Since f is not the identity map, it follows that $\phi \neq T \subseteq I_n$. Choose $a_1 \in T$ and consider a_1, $f(a_1)$, $f^2(a_1)$,.....

These are all elements of I_n and hence these can not all be distinct (Since I_n is finite). Therefore, there exists m < k such that $f^m(a_1) = f^k(a_1)$ and hence $f^{k-m}(a_1) = a_1$ and k – m > 0. Therefore there is a positive integer r such that $f^r(a_1) = a_1$. Now, let r_1, be the least positive integer such that $f^{r_1}(a_1) = a_1$. Then $r_1 > 1$, since $f(a_1) \neq a_1$. Consider the r_1- cycle

$\alpha_1 = (a_1\ f(a_1)\ f^2(a_1) \ldots\ldots f^{r_1-1}(a_1))$

If $T_1 = \{a_1, f(a_1), f^2(a_1), \ldots\ldots, f^{r_1-1}(a_1)\}$, then f and α_1 are equal on T_1. If $T_1 = T$, then $f = \alpha_1$. Otherwise, we can choose $\alpha_2 \in T - T_1$ and repeat the above procedure to construct an r_2-cycle.

$\alpha = (a_2\ f(a_2)\ f^2(a_2).....f^{r_2-1}(a_2))$, where $f^{r_2}(a_2) = a_2$. Again f and α_2 are equal on the set $T_2 = \{a_2, f(a_2), f^2(a_2)....., f^{r_2-1}(a_2)\}$. Also T_1 and T_2 are disjoint and hence α_1 and α_2 are disjoint cycles. If $T_1 \cup T_2 \neq T$, we continue the procedure to construct cycle α_3 and so on. Since T is finite, this process should terminate at a finite stage; that is, we get that the disjoint sets $T_1, T_2,....., T_k$ and cycles $\alpha_1, \alpha_2, ..., \alpha_k$ such that $T_1 \cup T_2 \cup ..... \cup T_k = T$.

$\alpha = (a_i\ f(a_i) f^2(a_i).....f^{r_i-1}(a_i))$, $f^{r_i}(a_i) = a_i$

$T_i = \{a_i, f(a_i), f^2(a_i),....., f^{r_i-1}(a_i))\}$ and f and α_i are same on T_i. All this data gives us that $f = \alpha_1 o \alpha_2 o \alpha_3 o..... o \alpha_k$ and $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k$ are pairwise disjoint cycles (note that each α_i is identity on T_j for $i \neq j$)

To prove the uniqueness, suppose $f = \beta_1 o \beta_2 o \beta_3 o..... o \beta_m$ be another expression of f as a product of disjoint cycles β_i's Suppose $m \leq k$. Suppose $a \in I_n$ such that $\beta_1(a) \neq a$ (that is, a is involved in the cycle β_1). Then $\beta_j(a) = a$ for all $j \neq 1$ and $f(a) = (\beta_1 o \beta_2 o \beta_3 o..... o \beta_m)(a) = \beta_1(a) \neq a$ and hence there exists j_1 such that $(\alpha_{j_1})(a) \neq a$ and $\alpha_j(a) = a$ for all $j \neq j_1$. Then it follows that $\beta_1 = \alpha_{j_1}$ and by the cancellation law, $\beta_2 o \beta_3 o..... \beta_m = \prod_{j \neq j_1} \alpha_j$.

Now, let us continue the above procedure to get $j_2, j_3,....., j_m$ such that $\beta_i = \alpha_{j_i}$ for $2 \leq i \leq m$. If $m < k$, we get that the product of certain α_j's is identity, which is a contradiction. Therefore $m = k$ and $i \mapsto j_i$ is a permutation of {1, 2, ..., m} such that $\beta_i = \alpha_{j_i}$. Hence the theorem is proved.

5.3.8. Self Assessment Question: Imitate the procedure given in the above proof to express the following permutations in S_{12} as a product of disjoint cycles.

(1) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 2 & 7 & 6 & 10 & 4 & 1 & 12 & 5 & 9 & 11 & 8 \end{pmatrix}$

(2) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 5 & 3 & 7 & 2 & 6 & 9 & 10 & 4 & 12 & 11 & 1 \end{pmatrix}$

(3) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 2 & 1 & 11 & 7 & 4 & 10 & 8 & 9 & 6 & 3 & 12 \end{pmatrix}$

5.3.9. Definition: A 2-cycle is called a transposition. That is, for any $a \neq b \in I_n$ the permutation which maps a to b and b to a and keeping all the other elements of I_n fixed is called a transposition.

For example the 2- cycles (4 5), (3 4) (5 9) are all transpositions. We can easily check that any r-cycle $\alpha = (a_1 a_2 .....a_r)$ can be expressed as $\alpha = (a_1 a_r)\ o\ (a_1 a_{r-1})\ o\ ..... o(a_1 a_2)$ which is a product of r-1 number of transpositions.

5.3.10. Self Assessment Question: Express the cycle (6 9 4 2 7 5) as a product of transpositions.

5.3.11. Theorem: Any permutation in S_n ($n > 1$) can be expressed as a product of transpositions.

Proof: Let $n > 1$ and f be a permutation in S_n. If f is identity, then

$f = (a\ b) \circ (a\ b)$ for any $a \neq b \in I_n$.
Suppose f is not the identity. By theorem 5.3.7.
we can write $f = \alpha_1 \circ \alpha_2 \circ \alpha_3 \ldots \circ \alpha_s$ where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are cycles and each cycle α_i is a product of transpositions. Therefore f is a product of transpositions.

5.3.12. Self Assessment Questions: If α is an r-cycle, then prove that $O(\alpha) = r$ and that the order of any transposition is two.

5.4: THE ALTERNATING GROUP A_n:

In the previous section, we have proved that any permutation can be expressed as a product of transpositions. But this expression may not be unique as in theorem 5.3.7. However, we have the following.

5.4.1. Theorem: Let f be permutation in S_n and $f = \alpha_1 \circ \alpha_2 \circ \alpha_3 \circ \ldots\ldots \circ \alpha_k$ and $f = \beta_1 \circ \beta_2 \circ \beta_3 \circ \ldots\ldots \circ \beta_m$ be two representations of f as products of transpositions α_i' s and β_j' s. Then K is even if and only if m is even.

proof: Since the theorem is trivial for n = 1 or 2, we can suppose that n > 2. Consider the polynomial in n-variables given by

$$p = p(x_1, x_2, \ldots\ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

For any permutation f in S_n, let $f(p) = \prod_{i<j} (x_{f(i)} - x_{f(j)})$.
Clearly $(f \circ g)(p) = f(g(p))$ for any $f, g \in S_n$. We can easily verify that $\alpha(p) = -p$ for any transposition α in S_n .
Now if $f = \alpha_1 \circ \alpha_2 \circ \alpha_3 \circ \ldots\ldots \circ \alpha_k = \beta_1 \circ \beta_2 \circ \beta_3 \circ \ldots\ldots \circ \beta_m$, then $(-1)^k p = f(p) = (-1)^m p$ and hence $(-1)^k = (-1)^m$ which implies that k is even if and only if m is even.

5.4.2. Self Assessment Question: Let n = 5. In this case, what is the polynomial p given in the above proof. What is f(p) if

(1) $f = (3\ 5\ 2\ 1) \circ (2\ 4)$

(2) $f = (2\ 5)$

5.4.3. Definition: A permutation f is called an even permutation if f can be expressed as a product of even number of transpositions. f is called odd if it is not even.

In theorem 5.4.1, we have proved that, if f is a product of even number of transpositions, then it cannot be a product of odd number of transpositions. Therefore, the concept of even permutation (5.4.3) is well defined. Also, in view of theorem 5.3.11, any permutation is either even or odd.

5.4.4. Self Assessment Question: Determine which of the following permutations are even?

(1) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$

(2) $g = (3\ 5\ 1\ 4) \circ (7\ 6) \circ (2\ 8)$

(3) $h = (3\ 2) \circ (7\ 4) \circ (1\ 8) \circ (2\ 3\ 8) \circ (4\ 6)$

(4) $\alpha = (5\ 8\ 2\ 6\ 4\ 7)$

5.4.5. Self Assessment Question: Prove that an r - cycle is even if and only if r is odd.

5.4.6. Theorem: For any n > 1, the set of all even permutations is a normal subgroup of index 2 in S_n.

Proof: Consider the group G = {1, -1} under the usual multiplication of real numbers. Let A_n be the set of all even permutations in S_n, n > 1. Then A_n is a subgroup of S_n.

Define $\theta: S_n \to G$ by

$$\theta(f) = \begin{cases} 1 \text{ if } f \text{ is even} \\ -1 \text{ if } f \text{ is odd} \end{cases}$$

Since f o g is even if and only if either both f and g are even or both of them are odd, it follows that θ is a homomorphism. Since 1 is the identity element in the group G, we have ker $\theta = \{f \in S_n / \theta(f) = 1\} = A_n$. Therefore A_n is a normal subgroup of S_n (by theorem 2.3.3). Also, by the fundamental theorem of homomorphisms (2.5.1), we have

$$S_n / A_n = S_n / Ker\,\theta \cong G.$$

Since G is a two element group, so is the quotient group S_n / A_n.

Since $|S_n| = |A_n| \; |S_n / A_n| = |A_n| . 2$, it follows that A_n is of index 2.

5.4.7. Definition: The group even permutations in S_n is called the alternating group of degree n and is denoted by A_n.

5.4.8. Self Assessment Question: For any n > 1, prove that $O(A_n) = \frac{n!}{2}$.

5.4.9. Self Assessment Question: List all the elements of A_2, A_3 and A_4.

5.5. MODEL EXAMINATION QUESTION:

5.5.1. Prove that any permutation in S_n can be uniquely expressed as a product of disjoint cycles.

5.5.2. Define the notion of the alternating group A_n and prove that it is a normal subgroup of index 2 in S_n.

5.6 SUMMARY:

In this lesson, we have introduced the notion of the symmetric group S_n and proved that any permutation in S_n can be expressed as a product of disjoint cycles. Further, we have introduced the notion of an even permutation and provedthat the set of all even permutations is a normal subgroup of index 2 in S_n.

5.7 TECHNICAL TERMS:

- Permutation
- Symmetric group S_n
- Cycle
- Transposition
- Even permutation
- Odd permutation
- Alternating group A_n
- Disjoint cycles.

5.8 ANSWERS TO SELF ASSESSMENT QUESTIONS:

5.2.2 f(3) = 1 and f(6) = 3

5.2.3 $f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 5 & 2 & 1 & 7 & 4 & 6 \end{pmatrix}$

$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 5 & 1 & 6 & 2 & 7 \end{pmatrix}$

5.2.4

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 4 & 1 & 3 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 5 & 2 & 4 & 1 & 3 \end{array}$$

$$\therefore \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

5.3.2 $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 7 & 6 & 4 & 2 & 8 & 3 & 5 & 9 & 10 \end{pmatrix}$

5.3.3 f = (1 5 4 7 9 8 2)

5.3.8 (1) Choose a such that f(a) ≠ a. For example f(4) ≠ 4 and consider 4, f(4), $f^2(4)$, …. so on until we get set 4 again. In this example, we have 4, f(4) = 6, $f^2(4) = f(6) = 4$

Now we have the cycle (4 6). Take some other than 4 or 6, such that f(a) ≠ a. For example, we can take 5, since f(5) ≠ 5. Then 5, f(5) =10, $f^2(5) = 9$, $f^3(5) = 5$

Then we have the cycle (5 10 9). Next pic 3 to set 3, f(3) = 7 $f^2(3) = 1$, $f^3(3) = 3$.

and we have the cycle (3 7 1). Again pic 8 to set 8, f(8) = 12, $f^2(8) = 8$.

and consider the cycle (8 12). The other elements, namely 2 and 11 are fixed by f. Thus we have

(1) f = (4 6) o (5 10 9) o (3 7 1) o (8 12)

(2) g = (1 8 10 12) o (2 5) o (4 7 9)

(3) h = (1 5 7 10 6 4 11 3)

5.3.10 (6 9 4 2 7 5)

= (6 5) o (6 7) o (6 2) o (6 4) o (6 9)

5.3.12: Let $\alpha = (a_1 a_2 \ldots\ldots a_r)$ be an r-cycle.

Then $\alpha^r(a_1) = \alpha^{r-1}(\alpha(a_1)) = \alpha^{r-1}(a_2) = \alpha^{r-2}(a_3) = \ldots\ldots\ldots = \alpha(a^r) = a_1$. For any $1 \leq i \leq r$, $\alpha = (a_i.a_{i+1}\ldots\ldots\ldots\ldots, a_r . a_1. a_2\ldots\ldots a_i)$ and hence $\alpha^r(a_i) = a_i$ for every $1 \leq i \leq r$. Thus $\alpha^r = id$. Also $\alpha^i \neq id$ for any $i < r$ and hence $O(\alpha) = r$. If α is a transposition, then it is a 2- cycle and hence $O(\alpha) = 2$.

5.4.2: Consider the polynomial x_1

$p = p(x_1, x_2, x_3, \ldots\ldots\ldots, x_5) = \prod_{i<j}(x_i - x_j)$

i.e, $p = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$

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

$f(p) = (x_3 - x_4)(x_3 - x_5)(x_3 - x_1)(x_3 - x_2)(x_4 - x_5)(x_4 - x_1)(x_4 - x_2)(x_5 - x_1)(x_5 - x_2)(x_1 - x_2)$

(2) f = (2 5) and hence

$f(p) = (x_1 - x_5)(x_1 - x_3)(x_1 - x_4)(x_1 - x_2)(x_5 - x_3)(x_5 - x_4)(x_5 - x_2)(x_3 - x_4)(x_3 - x_2)(x_4 - x_2)$

5.4.4 (1) f = (1 3 8 2 7) o (4 6)

= (1 7) o (1 2) o (1 8) o (1 3) o (4 6)

Therefore f is odd since f is a product of odd number of transpositions.

(2) g = (3 5 1 4) o (7 6) o (2 8)
= (3 4) o (3 1) o (3 5) o (7 6) o (2 8)

Therefore g is odd since g is a product of odd number of transpositions.

(3) h = (3 2) o (7 4) o (1 8) o (2 3 8) o (4 6)
= (3 2) o (7 4) o (1 8) o (2 8) o (2 3) o (4 6)

Therefore h is even since h is a product of even number of transpositions

(4) α = (5 8 2 6 4 7)
= (5 7) o (5 4) o (5 6) o (5 2) o (5 8), which is a product of odd number of transpositions and hence α is odd.

5.4.5. Any r - cycle $\alpha = (a_1a_2\ldots\ldots\ldots a_r)$ can be expressed as $\alpha = (a_1\ a_r) o (a_1\ a_{r-1}) o \ldots\ldots o (a_1\ a_2)$ which is a product of r–1 number of transpositions. Thus α is even if and only if r – 1 is even if and only if r is odd.

5.4.8: A_n is a normal subgroup of index 2 in S_n (by 5.4.6) and hence

$2 = O(S_n / A_n) = \frac{O(S_n)}{O(A_n)} = \frac{n!}{O(A_n)}$ therefore $O(A_n) = \frac{n!}{2}$

5.4.9: $A_2 = \{id\}$

$A_3 = \{(1\ 2\ 3), (2\ 1\ 3), id\}$

$A_4 = \{id, (1\ 2\ 3), (2\ 1\ 3), (2\ 3\ 4), (3\ 2\ 4), (3\ 4\ 1), (4\ 3\ 1), (1\ 2) o (3\ 4), (1\ 3) o (2\ 4), (1\ 4) o (2\ 3), (1\ 2\ 4), (2\ 1\ 4)\}$

$O(A_4) = 12 = \frac{4!}{2} = \frac{O(S_4)}{2}$

5. 9 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.V.Samba Siva Rao

.

LESSON - 6

ANOTHER COUNTING PRINCIPLE

OBJECTIVES:

The objectives of this lesson are to

- define the concepts of conjugate class and normalizer of an element of a group.
- obtain the class equation of a finite group.
- prove that any group of order p^n (p is prime, n>0) has a nontrivial centre and that any group of order p^2 is abelian.
- state and prove the Cauchy's theorem for general finite groups.
- determine the conjugate classes in S_n.

STRUCTURE:

6.1: INTRODUCTION:

We introduce an equivalence relation on a given finite group G and find a neat algebraic description for the size of each equivalence class. Using these we deserve an equation known as "the class equation" of any finite group and deduce several beautiful and powerful results on the structure of finite groups. In particular, we extend the Cauchy's theorem for finite abelian groups to general finite groups.

6.2: THE CONJUGACY RELATIONS:

6.2.1.Definition: Let G be a group and a, $b \in G$. we say that b is a conjugate of a if $b = c^{-1}ac$ for some $c \in G$. If b is a conjugate of a, we write it as $a \sim b$ .This relation '~' is called the conjugacy relation on G**.**

6.2.2. Theorem: Let G be a group. The relation conjugacy is an equivalence relation on G.

Proof Let $a, b, c \in G$

(i) $a \sim a$ as $a = e^{-1} a e$ where e is the identity element of G.

Therefore, '~' is reflexive

(ii) Suppose that $a \sim b$

Then $b = x^{-1} a x$ for some $x \in G$

Now $xb = a x$ and $xbx^{-1} = a$

So, $x^{-1} \in G$ and $a = (x^{-1})^{-1} bx^{-1}$.

$\Rightarrow b \sim a$

Therefore, '~' is symmetric.

(iii) Suppose that $a \sim b$ and $b \sim c$.

Then $b = x^{-1}ax$ and $c = y^{-1}$ by for some $x, y \in G$.

Now $c = y^{-1}$ by $= y^{-1}(x^{-1}ax)y = (y^{-1}x^{-1})\,a(xy) = (xy)^{-1}a(xy)$ and $x, y \in G$.

Therefore, '~' is transitive.

Hence the conjugacy relation '~' is an equivalence relation on G.

6.2.3. Self Assessment Question: If G is an abelian group and $a, b \in G$, prove that $a \sim b \Leftrightarrow a = b$.

6.2.4. Definition: Let G be a group and $a \in G$.Then the equivalence class of 'a' w.r.t '~' is called the conjugate class of a in G, and is denoted by C(a).

Thus $C(a) = \{b \in G / a \sim b\} = \{x^{-1}ax / x \in G\}$.

6.2.5. Notation: For any element a in a group G, the number of elements of the conjugate class C(a) is denoted by C_a.

6.2.6. Note that for any elements a and b in a group G, the conjugate classes C(a) and C(b) are either disjoint or identical and therefore the distinct conjugate classes in G form a partition of G, and hence $O(G) = \sum C_a$ where the sum runs over a set consisting of one element from each conjugate class.

6.2.7. Definition: Let G be a group and $a \in$ G. Then the set $\{x \in G / xa = ax\}$ is called the normalizer of a, and is denoted by N(a);

That is, $N(a) = \{x \in G / xa = ax\}$.

6.2.8. Lemma: Let G be a group and $a \in G$. Then N(a) is a subgroup of G.

Proof : Since ea = a = ae, we have $e \in N(a)$ and hence N(a) is a non-empty subset of G.

Let $x, y \in N(a)$.

Then ax = xa and ay = ya.

$\Rightarrow$ ax = xa and $y^{-1}a = ay^{-1}$.

Now $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$.

So $xy^{-1} \in N(a)$.

Therefore, N(a) is a subgroup of G.

6.2.9. Note: For any subgroup H of a subgroup G, the set of right cosets of H may not form a group (unless H is normal in G) under the usual operation.

6.2.10. Lemma: Let a be an element of a group G, C(a) the conjugate class and N(a) the normalizer of a in G. Then the set C(a) is bijective with the set of all right cosets of N(a) in G.

Proof: Let $a \in$ G.

Consider $C(a) = \{x^{-1}ax / x \in G\}$ and $N(a) = \{x \in G / xa = ax\}$.

Let X be the set of all right cosets of N(a) in G;

That is, X = $\{N(a)\,x / x \in G\}$

Define f: C(a) $\rightarrow$ X by $f(x^{-1}ax) = N(a)x$ for any $x^{-1}ax \in C(a), x \in G$.

First observe that, for any $x, y \in G$,

$x^{-1}ax = y^{-1}ay \Rightarrow axy^{-1} = xy^{-1}a$
$\Rightarrow xy^{-1} \in N(a)$
$\Rightarrow N(a)x = N(a)y$

So, f is well defined.
Also, for any $x, y \in G$, $f(x^{-1}ax) = f(y^{-1}ay) \Rightarrow N(a)x = N(a)y$
$\Rightarrow xy^{-1} \in N(a)$
$\Rightarrow a(xy^{-1}) = (xy^{-1})a$
$\Rightarrow x^{-1}ax = y^{-1}ay$

So, f is one - to - one.

Let $N(a)x \in X$ where $x \in G$.

Now $x^{-1}ax \in C(a)$ and $f(x^{-1}ax) = N(a)x$
Therefore f is onto X.
Hence, $f : C(a) \to X$ is a bijection.

6.2.11. Self Assessment Question : For any group G, prove that the center $Z(G) = \bigcap_{a \in G} N(a)$

6.3: THE CLASS EQUATION OF A FINITE GROUP :

In this section the class equation of a finite group is derived. This equation is useful in proving several important results in the structure theory of finite groups.

6.3.1. Theorem: Let G be a group and $a \in$G. Then $C_a = \frac{o(G)}{o(N(a))}$.

Proof : Consider $C(a) = \{x^{-1}ax / x \in G\}$ and $N(a) = \{x \in G / xa = ax\}$.
Let X denote the set of all right cosets of N(a) in G. Since G is finite, we have that C(a), N(a), X are all finite sets. We know that the number of right cosets of N(a) in G is $\frac{o(G)}{o(N(a))}$.

So the number of elements in X is $\frac{o(G)}{o(N(a))}$.

By lemma 6.2.10, X is bijective with C(a). That is, the sets X and C(a) have the same number of elements.

Therefore, $C_a = \frac{o(G)}{o(N(a))}$ where C_a is the number of elements of C(a).

6.3.2. Theorem(The Class Equation):

Let G be a finite group. Then $O(G) = \sum \frac{o(G)}{o(N(a))}$ where the sum runs over one element a in each conjugate class.

Proof: Let G be a finite group. For $a \in G$, let C_a denote the number of elements of conjugate class C(a). Since the distinct conjugate classes in G form a partition of G, it follows that $O(G) = \sum C_a$ where the sum runs over one element a in each conjugate class.

By theorem 6.3.1, for any $a \in$G, we have $C_a = \frac{o(G)}{o(N(a))}$

Therefore $O(G) = \sum \frac{o(G)}{o(N(a))}$ where the sum runs over one element a in each conjugate class.

6.3.3. Note :

i) Let G be an abelian group. Then Z(G) = G and every conjugate class is a set consisting of exactly one element. So the class equation does not give any new information.

ii) The class equation is useful in the case of non-abelian groups.

6.3.4. Example : Consider the symmetric group of degree 3, S_3 which is the non-abelian group with least number of elements. We have $O(S_3) = 6$.
Let e denote the identity transposition. Put f = (1 2), g = (2 3) and h = (3 1)
Then fg = (1 3 2) and gf = (1 2 3). Cleary $f^{-1} = f$, $g^{-1} = g$, $h^{-1} = h$ and $(fg)^{-1} = gf$.
So, $S_3 = \{e, f, g, h, fg, gh\}$
Also, fh = (1 2 3) = gf and gh = (1 3 2) = fg. Now C(e) = {e},
$C(f) = \{x^{-1}fx / x \in S_3\}$
$= \{ e^{-1}fe, f^{-1}ff, g^{-1}fg, h^{-1}fh, (fg)^{-1}f(fg), (gf)^{-1}f(gf)\}$.
$= \{f, h, g\} = C(g) = C(h)$, and $C(fg) = \{fg, gf\}$.
Therefore C(e), C(f) and C(fg) are three distinct conjugate classes in S_3.

6.3.5. Lemma : Let G be a group and $a \in G$.Then $a \in Z(G)$ if and only if N(a) = G. If G is finite, $a \in Z(G)$ if and only if $O(N(a)) = O(G)$.

Proof : $a \in Z(G) \Leftrightarrow ag = ga$ for all $g \in G$

$\Leftrightarrow g \in N(a)$ for all $g \in G$.
$\Leftrightarrow N(a) = G$

Therefore, $a \in Z(G) \Leftrightarrow N(a) = G \rightarrow (I)$
Suppose that G is finite.
Then N(a) = G if and only if $O(N(a)) = O(G) \rightarrow (II)$
From (I) and (II), we have that
$a \in Z(G) \Leftrightarrow O(N(a)) = O(G)$.

6.4: GROUPS OF ORDER P^n :

Groups of order p^n, where p is a prime number and n is a positive integer, play an important role in the structure theory of finite groups.

6.4.1. Theorem : Let G be a finite group of order p^n, where p is a prime number and n is a positive integer. Then $Z(G) \neq \{e\}$.
Proof : Given that G is a finite group of order p^n, where p is a prime number and n is a positive integer. Take the class equation of G;

$$O(G) = \sum \frac{O(G)}{O(N(a))}$$

where the sum runs over one element 'a' from each conjugate class.
This can be written as $O(G) = \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} \rightarrow (I)$
By lemma 6.3.5, we have $a \in Z(G) \Leftrightarrow o(N(a)) = o(G)$
That is, $a \in Z(G) \Leftrightarrow \frac{O(G)}{O(N(a))} = 1$
So, (I) becomes $O(G) = O(Z(G)) + \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} \rightarrow (II)$
Also, by lemma 6.3.5, we have
$a \notin Z(G) \Leftrightarrow O(N(a)) < O(G) \rightarrow (III)$
Since N(a) is a subgroup of G, by the Lagrange's Theorem, $O(N(a))$ is a divisor of $O(G) = p^n \rightarrow (IV)$
From (III) & (IV), $p \mid \frac{O(G)}{O(N(a))}$ for all $a \notin Z(G)$

and that $p \mid \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))}$

Since $p \mid p^n = O(G)$ and $p \mid \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))}$, we have that $p \mid (O(G) - \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))})$

So from (II), we have that $p \mid O(Z(G))$

Therefore, $O(Z(G)) \geq p > 1$ and hence $Z(G) \neq \{e\}$.

The above theorem can be rephrased as follows:

" Any group of prime power order has nontrivial centre".

6.4.2. Self Assessment Questions : Prove that any group of order 625 has nontrivial center.

6.4.3. Corollary : If G is a finite group of order p^2 where p is a prime number, then G is abelian

Proof : Given that $O(G) = p^2$, where p is a prime number.

Then, by theorem 6.4.1, $Z(G) \neq \{e\}$ and hence $O(Z(G)) > 1$.

Since Z(G) is a subgroup of G, by the Lagrange's Theorem, $O(Z(G))$ is a a divisor of $O(G) = p^2$

So, $O(Z(G)) = p$ or p^2.

If $O(Z(G)) = p^2$, then $O(Z(G)) = O(G)$ and that Z(G) = G and hence G is abelian.

Suppose that $O(Z(G)) = p$.

Choose $a \in G$ such that $a \notin Z(G)$.

We have $Z(G) \subseteq N(a)$ and $a \in N(a)$.

Since $O(Z(G)) = p$ and $a \notin Z(G)$, we have $o(N(a)) \geq p+1$.

Since N(a) is a subgroup of G, $O(N(a)) \mid O(G) = p^2$ e

As $O(N(a)) \geq p+1$ and $O(N(a)) \mid p^2$, we have $O(N(a)) = p^2 = O(G)$.

So, $a \in Z(G)$, a contradiction to $a \notin Z(G)$.

Therefore $O(Z(G)) = p^2 = O(G)$ and hence $Z(G) = G$.

Thus G is abelian.

6.4.4. Self Assessment Question: Prove that any group of order 169 is abelian.

6.5: CAUCHY'S THEOREM

1. Cauchy's theorem was already proved for finite abelian groups in lesson 2(2.6.1).

2. We shall extend this theorem to general finite groups in the following.

6.5.1. Theorem (Cauchy's Theorem):

Let G be a finite group and p be a prime number. If $p \mid O(G)$, then G has an element of order p.

Proof : Suppose that $p \mid O(G)$. Then $O(G) \geq P$.

We shall use induction on $O(G)$ to prove the theorem. Since $O(G) \geq P$, we can start induction at p. If $O(G) = p$, then G is a cyclic group of order p and hence every nonidentity element of G is of order p. Now suppose that $O(G) > p$ and assume that the theorem is true for all groups of order less than that of G.

Case (i) : Suppose G has a subgroup H and $O(H) < O(G)$ and $p \mid O(H)$. Then by our induction hypothesis, H has an element b(say) of order p. Now $b \in G$ and $O(b) = p$.

Case (ii) : Suppose G has no subgroup H such that $O(H) < O(G)$ and $p \mid O(H)$ Take the class equation of G; $O(G) = \sum \frac{O(G)}{O(N(a))}$ where the sum runs over one element 'a' from each

conjugate class. This can be written as

$O(G) = O(Z(G)) + \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))} \rightarrow (1)$

By our supposition, $p \mid O(N(a))$ for $N(a) \neq G$. So, $N(a) \neq G$, $p \mid \frac{o(G)}{o(N(a))}$ and that P| $\sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$ Since $p \mid O(G)$ and $p \mid \sum_{N(a) \neq G} \frac{O(G)}{O(N(a))}$, by (1), we have that $p \mid O(Z(G))$

So, by our supposition, $O(Z(G)) \not< O(G)$ and that O(Z(G)) = O(G) and hence Z(G) = G. This shows that G is abelian. Therefore by Cauchy's theorem for abelian groups, G has an element of order p. This completes the induction and hence the theorem.

6.5.2. Self Assessment Question : Prove that there exists an element $a \neq e$ in a group of order 793 such that $a^{61} = e$.

6.5.3. Self Assessment Question : Prove that any group of even order has an element $a \neq e$ such that $a^2 = e$.

6.6: CONJUGATE CLASSES IN S_n:

In this section, we use several results on the conjugate classes to determine all the conjugate classes in the symmetric group S_n. Let us recall that the elements of S_n are the permutations on the set $I_n = \{1,2,..n\}$ and that any nonidentity permutation is a product of disjoint cycles, each of length > 1 (See theorem 4.3.7). In fact, we have defined an r-cycle only when r > 1 (see definition 4.3.1). Now, let us agree, for convenience, that 1-cycle is defined to be the identity map (identity element in S_n). With this convention, we can rephrase theorem 4.3.7 as given in the following.

6.6.1. Theorem : Any permutation f in S_n can be written as $f = \alpha_1.\alpha_2.\alpha_3 \ldots\ldots \alpha_k$ where α_i is a cycle of length r_i, $1 \leq i \leq k$ with $r_1 \leq r_2 \leq \ldots \leq r_k$ and $r_1 + r_2 + \ldots + r_k = n$. (In other words, any permutation in S_n is a product of disjoint cycles)

Proof : Let $f \in S_n$

Suppose f is the identity permutation in S_n. Then f can be written as product of n number of 1-cycles, (i.e., f = (1) (2) (3) ----- (n)) each of which is a cycle of length 1, and hence we are through.

Suppose f is not the identity permutation in S_n. Then by Theorem 4.3.7, f can be written as $f = \alpha_1.\alpha_2 \ldots\ldots\ldots\alpha_k$, where each α_i is a cycle of length $s_i > 1$, $1 \leq i \leq k$. Observe that, for any $a \in I_n$, $(a)f \neq a \Leftrightarrow (a)\alpha_i \neq a$ for some i with $1 \leq i \leq k$ and $(a)\alpha_j = a$ for $j \neq i$.
Write $T = \{a \in I_n / (a) f = a\}$. Since T is finite, we can write T as $T = \{a_1, a_2, \ldots\ldots, a_t\}$

Now $f = (a_1).(a_2) \ldots\ldots (a_k).\alpha_1.\alpha_2.\ldots\ldots\ldots.\alpha_k$. Since α_i's are disjoint, they commute with each other and hence we can rearrange $\alpha_1.\alpha_2 \ldots\ldots\ldots\alpha_k$, such that their lengths are in increasing order.

Also, for any $a \in I_n$, $(a)f \neq a \Leftrightarrow a$ is involved in some α_i , $1 \leq i \leq k$. Therefore $f = \beta_1 . \beta_2 \ldots\ldots\ldots \beta_k.. \alpha_1.\alpha_2 \ldots\ldots\ldots\alpha_k$ where each β_i is a cycle of length 1, and α_i is a cycle of length s_i , $1 \leq i \leq k$ with $1 \leq 1 \leq \ldots\ldots\ldots \leq 1 \leq s_1 \leq s_2 \leq \ldots\ldots\ldots \leq s_k$ and $1 + 1 + \ldots\ldots\ldots + 1 + s_1 + s_2 + \ldots\ldots\ldots + s_k = t + (n - t) = n$.

6.6.2. Definition: Let n be a positive integer. A finite increasing sequence of positive integers whose sum is n, is called a partition of n; that is, a finite sequence $\{ r_1, r_2, \ldots\ldots, r_k \}$ of positive integers is called a partition of n if $(i)\ r_1 \le r_2 \le \ldots\ldots \le r_k$, and $(ii)\ r_1 + r_2 + \ldots\ldots + r_k = n$

The number of partitions of n is denoted by p(n).

6.6.3. Examples :

p(1) = 1, since {1} is the only partition of 1.
p(2) = 2, since {1, 1} and {2} are the only partitions of 2.
p(3) = 3, since {1, 1, 1},{1, 2} and {3} are the only partitions of 3.
p(4) = 5, since {1, 1, 1, 1}, {1, 1, 2}, {1, 3}, {2, 2} and {4} are the only partitions of 4.

6.6.4 Theorem : The number of conjugate classes in S_n is p(n), the number of partitions of n.

Proof : We shall exhibit a one-to-one correspondence between the conjugate classes in S_n and partitions of n. Any $f \in S_n$ can be expressed as $f = \alpha_1 . \alpha_2 \ldots\ldots\ldots \alpha_k$, where each α_i is a cycle of length r_i with $r_1 \le r_2 \le \ldots\ldots\ldots \le r_k$ and $r_1 + r_2 + \ldots\ldots\ldots + r_k = n$ (see theorem 6.6.1) ; that is, $\{r_1, r_2, \ldots\ldots, r_k\}$ is a partition of n. Further , by the uniqueness proved in Theorem 5.3.7, any representation of f as product of cycles yields the same partition of n. We call this unique partition as 'the partition induced by f'. Now we prove the following :

(i) For any $f , g \in S_n$ f is a conjugate of g if and only if both f and g induce the same partition of n.

(ii) Any partition of n is induced by some $f \in S_n$. These two give us a bijection $C(f) \to$ the partition induced by f of the set of conjugate classes in S_n onto the set of partitions of n.

i) L et $f , g \in S_n$ such that f ~ g. Then $f = h^{-1}.g.h$ for $h \in S_n$. Suppose $g = \alpha_1 . \alpha_2 \ldots\ldots\ldots \alpha_k$ ------ (I) where α_i 's are cycles of length r_i with $r_1 \le r_2 \le \ldots\ldots\ldots \le r_k$ and $r_1 + r_2 + - - - + r_k = n$.Then $\{ r_1, r_2, \ldots\ldots, r_k\}$ is the partition of n induced by g. We shall prove that the same partition is induced by f also ; that is, f has a similar representation as in (1) for g, which yields the same partition $\{ r_1, r_2, \ldots\ldots, r_k\}$.

Now $f = h^{-1} \circ g \circ h = (h^{-1} \circ \alpha_1 \circ h) \circ (h^{-1} \circ \alpha_2 \circ h) \circ - - - - \circ (h^{-1} \circ \alpha_k \circ h)$.

Therefore, $f = \beta_1 \circ \beta_2 \circ \ldots\ldots\ldots \beta_k$ where $\beta_i = h^{-1} \circ \alpha_i \circ h \ \forall\ 1 \le i \le k$.

If the cycle $\alpha_i = (a_1, a_2, \ldots\ldots, a_{r_i})$ then, clearly, $h^{-1} \circ \alpha_i \circ h = ((a_1)h, (a_2)h, \ldots\ldots, (a_{r_i})h)$ which is again a cycle of length $r_i \ \forall\ 1 \le i \le k$.

Thus $\{r_1, r_2, \ldots\ldots, r_k\}$ is the partition induced by f also.

Conversely, suppose that both f and g induce the same partition $\{r_1, r_2, \ldots\ldots, r_k\}$.

Then f and g have representations of the form $f = \alpha_1 \circ \alpha_2 \circ \ldots\ldots\ldots \circ \alpha_k$ and $g = \beta_1 \circ \beta_2 \circ \ldots\ldots\ldots \circ \beta_k$ where α_i and β_i are cycles, each of length , $r_i , 1 \le i \le k$ with $r_1 \le r_2 \le \ldots\ldots\ldots \le r_k$ and $r_1 + r_2 + \ldots\ldots\ldots + r_k = n$. For $1 \le i \le k$, write $\alpha_i = (a_{i_1}, a_{i_2}, \ldots\ldots, a_{i_{ri}})$ and $\beta_i = (\beta_{i_1}, \beta_{i_2}, \ldots\ldots, \beta_{i_{ri}})$. Then $\{a_{i_j}\} = \{1,2, \ldots\ldots\ldots, n\} = \{b_{i_j}\}$, and for any $i \ne j$, the set $\{a_{i_1}, a_{i_2}, \ldots\ldots, a_{i_{ri}}\}$ and $\{a_{j_1}, a_{j_2}, \ldots\ldots, a_{j_{rj}}\}$ are disjoint ($\because \alpha_i$ and α_j are disjoint cycles). Similarly $\{b_{i_1}, b_{i_2}, \ldots\ldots, b_{i_{ri}}\}$ and $\{b_{j_1}, b_{j_2}, \ldots\ldots, b_{j_{rj}}\}$ are disjoint cycles.

Now, define $h : \{1, \ldots\ldots, n\} \to \{1, \ldots\ldots, n\}$ by $(a_{i_j})h = b_{i_j}\}$. Then $h \in S_n$ and $h^{-1} \circ f \circ h = g$, so that f ~ g.

ii) Let $\{r_1, r_2, \ldots\ldots, r_k\}$ be a partition of n. Then $0 < r_1 \le r_2 \ldots\ldots \le r_k$ and $r_1 + r_2 + \ldots\ldots + r_k = n$. For $1 \le i \le k$, write $\alpha_i = (r_{i-1} + 1, r_{i-1} + 2, \ldots\ldots, r_{i-1} + r_i)$, where $r_o = 0$. Then each α_i is a cycle of length r_i. Put $f = \alpha_1 \alpha_2 \ldots\ldots \alpha_k$. Then f is a permutation in S_n which induces the partition $\{r_1, r_2, \ldots\ldots, r_k\}$.

This completes the proof.

6.6.5. Self Assessment Question : If $\alpha = (a_1, a_2, \ldots\ldots, a_r)$ is a cycle in S_n and $h \in S_n$, Prove that $h^{-1} \alpha h$ is the cycle $((a_1)h, (a_2)h, \ldots\ldots, (a_r)h)$.

6.6.6. Self Assessment Question : How many conjugate classes are there in each of S_1, S_2, S_3, S_4, and S_5.

6.7. MODEL EXAMINATION QUESTIONS :

6.7.1. State and derive the class equation of a finite group.
6.7.2. State and prove Cauchy's theorem for finite groups.
6.7.3. Prove that any group of order p^2 is abelian, where p is a prime.
6.7.4. For any positive integer n, prove that the number of conjugate classes in S_n is equal to the number of partitions of n.

6.8. EXERCISES :

6.8.1. If N is a normal subgroup of a group G and $a \in N$, Prove that $C(a) \subseteq N$.
6.8.2. If N is a normal subgroup of a finite group G, Prove that O(N) = $\sum C_a$ for some choices of a in N.
6.8.3. If in a finite group G, an element a has exactly two conjugates, prove that G has a normal subgroup $N \ne \{e\}, G$.
6.8.4. Find all the conjugate classes in S_3 and verify the class equation for S_3.
6.8.5. List all the conjugate classes in S_4, find the C_a's and verify the class equation
6.8.6. Find all the conjugate classes in A_5 and the number of elements in each conjugate class, where A_5 is the alternating group of degree 5.
6.8.7. Exhibit two elements in A_5 which are conjugate in S_5, but not in A_5.
6.8.8. Prove that A_5 is simple.
6.8.9. If o(G) = p^2 where p is a prime, prove that G has a subgroup of order p^n for all $0 \le n \le r$ (use theorem 5.4.1).
6.8.10. For any group G, prove that G is abelian if and only if $G/Z(G)$ is cyclic.
6.8.11. Prove that any group of order 15 is cyclic.
6.8.12. Prove that any subgroup of order p^{n-1} in a group G of order p^n is normal in G, where p is a prime number.
6.8.13. Prove that any group of order 28 is not simple.
6.8.14. Find the number of conjugates of (1 2) (3 4) is S_n, $n \ge 4$.
6.8.15. If O(G) = 28 and G has a normal subgroup of order 4, prove that G is abelian.
6.8.16. If H is a proper subgroup of a group G of order p^n, where p is a prime number, prove that there exists $x \in G$ such that $x \notin H$ and $x^{-1}Hx = H$

6.9 SUMMARY

In this lesson, you have learnt the concept of conjugacy relation on a group G and, for any $a \in G$, the conjugate class C(a) and the normalizer N(a) and proved that C(a) is bijective with the set of right cosets of N(a) in G. Using this, we have derived the class equation of a finite group which is a crucial tool in proving the Cauchy's Theorem for a general finite group. Also, we have proved that the centre of a group of prime power order is nontrivial and deduced that any group of order p^2 is abelian if p is a prime number. Further we have determined the conjugate classes of the symmetric group S_n by proving that the number of conjugate classes in S_n is equal to the number of partitions of n.

6.10 TECHNICAL TERMS

- Conjugacy relation, conjugate class, normalizer of a class equation, Cauchy's theorem for finite groups, partitions of n.

6.11 ANSWER TO SELF ASSESSMENT QUESTIONS:

6.2.3. $a \sim b \Rightarrow a = c^{-1}bc$ for some $c \in G$

$\Rightarrow a = c^{-1}cb = b$ (since G is abelian)

$a = b \Rightarrow a = e^{-1}be \Rightarrow a \sim b$

6.2.10. $x \in Z(G) \Leftrightarrow xa = ax$ for all $a \in G \Leftrightarrow x \in N(a)$ for all $a \in G$

$\Leftrightarrow x \in \bigcap_{a \in G} N(a)$

6.4.2. Let G be a group of order 625. Then $O(G) = 625 = 5^4 = p^n$ where p = 5 is a prime number and n = 4. So, by theorem 6.4.1, the centre Z(G) is nontrivial.

6.4.4. 169 is of the form p^2 where p = 13 is a prime number Now use Theorem 6.4.3.

6.5.2. Let G be a group of order 793. Then O(G) = 793 = 61x13. Now 61 divides O(G) and 61 is a prime number. So, by Cauchy's Theorem (6.5.1), G has an element of order 61. Therefore there exists $a \neq e$ in G such that $a^{61} = e$.

6.5.3. Similar to 6.5.2; for, if G is a group of even order, then 2 divides O(G) and 2 is a prime number.

6.6.5. Let $\alpha = (a_1, a_2, \ldots\ldots, a_r)\ h \in S_n$ and $\beta = ((a_1)h,\ (a_2)h, \ldots\ldots,\ (a_r)h)$.

Now we prove that $\alpha \circ h = h \circ \beta$.

For any $a \in I_n$,

$$(a)(h\circ\beta) = ((a)h)\beta = \begin{cases} (a_{i+1}) & if\ a = a_i, i < r \\ (a_1)h & if\ a = a_r \\ (a)h & if\ a = a_i,\ 1 \le i \le n \end{cases} = (a)(\alpha \circ h)$$

This shows that $h \circ \beta = \alpha \circ h$ and hence $h^{-1} \circ \alpha \circ h = \beta$.

6.6.6. Follows from 6.6.4 and from the facts that p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5 and p(5) = 7. The number of conjugate classes in S_1, S_2, S_3, S_4 and S_5 is 1, 2, 3, 5 and 7, respectively.

6.12 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. K. SIVA PRASAD

LESSON -7

SYLOW'S THEOREM

OBJECTIVES:

The objectives of this lesson are to

- prove that the Sylow's theorem in three different methods.
- define the notion of a p-Sylow subgroup and prove that any two p- Sylow subgroups of a group are conjugate to each other.
- prove that the number of p-Sylow subgroups of a group G is a divisor of O(G) and is of the form 1+kp, $k \geq 0$.

STRUCTURE:

7.1. INTRODUCTION:

Lagrange's theorem tells us that the order of a subgroup of a finite group is a divisor of the order of that group. The converse of this theorem is not true; thatis, for any divisor m of O(G), there may not exist any subgroup of order m in G. For example, there are no subgroups of order 6 in A_4, even if 6 is a divisor of $O(A_4)$.There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. In this direction, a classic theorem due tothe Norwegian mathematician Sylow is the basic and widely used one. We present three proofs which are of completely diverse nature.

7.2: THE FIRST PROOF OF SYLOW'S THEOREM:

In this section, we present an elegant and simple elementary proof of Sylow's theorem which uses certain basic ideas from number theory and combinotories. For any positive integers n and k with $k \leq n$, the number of ways of picking a subset of k elements from a set of n elements is equal to $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

7.2.1: Lemma: If $n = p^{\alpha}m$, where p is a prime number, $p^r | m$ and $p^{r+1} \nmid m$ *then* $p^r \mid \binom{p^{\alpha}m}{p^{\alpha}}$ and $p^{r+1} \nmid \binom{p^{\alpha}m}{p^{\alpha}}$

Proof : Now $\binom{p^{\alpha}m}{p^{\alpha}} = \frac{(p^{\alpha}m)!}{(p^{\alpha})!(p^{\alpha}m-p^{\alpha})!}$

$$= \frac{p^{\alpha}m(p^{\alpha}m-1)---(p^{\alpha}m-i)---(p^{\alpha}m-p^{\alpha}+1)}{p^{\alpha}(p^{\alpha}-1)---(p^{\alpha}-i)---(p^{\alpha}-p^{\alpha}+1)}$$

On the right side of the above equation, it can be easily seen that except for the term m in the numerator, any power of p dividing $(p^{\alpha}m - i)$ is the same as that dividing $p^{\alpha} - i$.

So, on the right side of the above equation, all powers of p are cancelled out except the power which divides *m*.
Therefore, $p^{r} \mid \binom{p^{\alpha}m}{p^{\alpha}}$ and $p^{r+1} \nmid \binom{p^{\alpha}m}{p^{\alpha}}$

7.2.2: Self Assessment Question: In the above, verify that for any $\beta \leq \alpha$, $p^{\beta} \mid p^{\alpha}$m –i $\Leftrightarrow$ $p^{\beta} \mid p^{\alpha}$ –i

7.2.3: Theorem (Sylow's Theorem - I):

Statement: Let G be a finite group, p be a prime number and α be a nonnegative integer. If $p^{\alpha} \mid O(G)$, then G has a subgroup of order p^{α}.

Proof: Since $p^{\alpha} \mid O(G)$, we have that O(G) = $p^{\alpha}m$, where m is a positive integer.
Hence the prime p may or may not divide m.
Let p^{r} be the largest power of p that divides m.
Then we have $r \geq 0$, $p^{r} \mid m$ and $p^{r+1} \nmid m$.

Let *M* be the set of all subsets of G each with p^{α} elements.
The number of elements in M is $\binom{p^{\alpha}m}{p^{\alpha}}$, which is divisible by p^{r} and not divisible by p^{r+1} (by lemma 7.2.1).
Define a relation '$\sim$' on M as follows:
For any A, B $\in$ M, A$\sim$ B $\Leftrightarrow$ A = Bx for some x $\in$G.
It can be easily verified that '$\sim$' is an equivalence relation on M as follows:
For A$\in$ M, let $\bar{A}$ denote the equivalence class containing A in M and $|\bar{A}|$ denote the number of elements in $\bar{A}$. Since the equivalence classes form a partition of M,
we get that $\binom{p^{\alpha}m}{p^{\alpha}} = |M| = \sum|\bar{A}| \rightarrow (1)$
Since p^{r+1} does not divide $\binom{p^{\alpha}m}{p^{\alpha}}$, by (1), it follows that p^{r+1} does not divide $|\bar{A}|$ for some equivalence class $\bar{A}$.
Let $\bar{A}$ = {A_1, A_2,…,A_n}.
Now A ~A_i for all i and $p^{r+1} \nmid$ n.
Put H = $\{g \in G \mid Ag = A\}$
Then H is a subgroup of G.

We prove that O(H) = p^{α}
Since A ~ A_i, we have that $A_i = Ag_i$ for some $g_i \in G$ and $\bar{A}$ = {Ag_1, Ag_2,…, Ag_n}
Let us consider the right cosets Hg_i, for i = 1,…,n.
For i, j with $1 \leq i, j \leq n$,
$Hg_i = Hg_j \Leftrightarrow g_i g_j^{-1} \in H$
$\Leftrightarrow Ag_i g_j^{-1} = A$
$\Leftrightarrow A g_i = Ag_j$
$\Leftrightarrow i = j$
This shows that Hg_1, Hg_2,....., Hg_n are all the distinct right cosets of H in G

Suppose Hg is a right coset in G where $g \in G$. We have $Ag \sim A$
$\Rightarrow Ag = Ag_i$ for some i with $1 \leq i \leq n$

$\Rightarrow g_i g^{-1} \in H$ for some i

$\Rightarrow Hg = Hg_i$ for some i.

So, Hg is one of Hg_i, $1 \leq i \leq n$. Therefore Hg_1, Hg_2 ,....., Hg_n are only distinct right cosets of H in G.

Since Hg_i, $1 \leq i \leq n$ form a partition of G, it follows that $p^\alpha m = O(G) = n.O(H)$

As $p^r | m$, $p^{\alpha+r} | p^\alpha m = n.O(H)$

Since $p^{r+1} \nmid n$ and $p^{\alpha+r} | n.O(H)$, it follows that $p^\alpha | o(H)$ $\rightarrow$ (2)

If $a \in A$, then for all $h \in H$, $ah \in Ah = A$

This implies that A has atleast O(H) number of elements.

Since $A \in M$, $p^\alpha = |A| \geq O(H)$ $\rightarrow$ (3)

From (2) and (3), $(OH) = p^\alpha$

Thus there exists a subgroup H of G of order p^α

7.2.4. Self Assessment Question: In any group of order 2500, prove that there is a subgroup of order 125.

7.2.5. Corollary: Let G be a finite group and p be a prime number. If $p^m | O(G)$ and $p^{m+1} \nmid O(G)$, then G has a subgroup of order p^m.

Proof: This is an immediate consequence of theorem 7.2.3. The above corollary has an importance, even though it is a direct consequence of theorem 7.2.3. The reason is that 7.2.5 implies 7.2.3 (see 7.2.6 and 7.2.7, given below). Therefore, in order to prove the main theorem, the Sylow's theorem-I, it is enough if we prove 7.2.5. This is what we are going to do in the second proof and third proof given in the next two sections.

7.2.6: Self Assessment Question: Let G be a group of order p^n where p is a prime number. Then for each $0 \leq r \leq n$, prove that G has a subgroup of order p^r.

7.2.7: Self Assessment Question: In any group of order 405, prove that there is a subgroup of order 81.

7.2.8: Definition: Let G be a finite group and let p be a prime number such that $p^m | O(G)$ and $p^{m+1} \nmid O(G)$. Then any subgroup of G of order p^m is called a p-Sylow subgroup of G.

7.3: THE SECOND PROOF:

As it is mentioned in the introduction to this lesson, we present another proof of the Sylow's Theorem-1 which is completely different from the first proof given in the previous section and is based on induction on the order of the given group.

7.3.1: Theorem: Let G be a finite group and p be a prime number. If $p^m | O(G)$ and $p^{m+1} \nmid O(G)$, then G has a subgroup of order p^m

Proof: If m = 0, then G has the subgroup {e}, which is of order p^m. Suppose m is a positive integer.

We prove the theorem by using induction on O(G). As $p^m | O(G)$ and m > 0, $O(G) \geq p$. So, we start induction at p.

If O(G) = p, then G itself is a subgroup of order p^n, where m = 1. Suppose o(G) > p and assume

that the theorem is valid for all groups of order less than o(G). Consider the center Z(G) ={a ∈G | ax = xa for all x ∈ G} which is a normal subgroup of G.

Case (i) Suppose p | O(z(G))
Now Z(G) is a finite group whose order is divided by p.
So, by the Cauchy's theorem (2.11.3), Z(G) has an element of order p. Let a∈Z(G) such that $a \neq e$ ad $a^p = e$.
Put N = (a), the subgroup generated by a.
Then N is a normal subgroup of G ($\because xa^ix^{-1} = a^i$ *for all* $x \in G$ *and* $a^i \in N$)
and O(N) = p ($\because O(a) = p$)
So, we can form the quotient group G/N.
As p> 0, $O(G/N) = \frac{O(G)}{O(N)} = \frac{O(G)}{p} < O(G)$
Also, since $P^m \mid O(G)$ and $p^{m+1} \nmid O(G)$, it follows that $p^{m-1} \mid O(G/N)$ and $p^m \nmid O(G/N)$.
$\therefore$ by the induction hypothesis, G/N has a subgroup, say $\bar{H}$ of order p^{m-1}
Let H = $\{x \in G / Nx \in \bar{H}\}$
Then H is a subgroup of G containing N as a normal subgroup and H/N = $\bar{H}$
Now $O(H) = \frac{O(H)}{O(N)} O(N) = O\left(\frac{H}{N}\right). O(N) = O(\bar{H}).O(N) = p^{m-1}.p = p^m$
Thus ∃ a subgroup H of order p^m in G.

Case (ii) Suppose p ∤ O(Z(G))
Take the class equation $O(G) = \sum \frac{O(G)}{O(N(a))}$ where this sum runs over one element a in each conjugate class.
The above class equation can be written as
$O(G) = O(Z(G)) + \sum_{i=1}^{n} \frac{O(G)}{O(N(a_i))}$ where $a_1, a_2, \ldots\ldots\ldots\ldots, a_n$ are elements such that $C(a_1), \ldots, C(a_n)$ are all the distinct conjugate classes each with more than one element.
We have $|\bar{C}(a)| = \frac{O(G)}{O(N(a))}$ for $a \in G$
Since each $|C(a_i)| > 1$, it follows that each $N(a_i) \neq G$, $1 \leq i \leq n$.
As $p^m \nmid O(G)$ where m > 0, P | O(G).
Since p | O(Z(G)), we get that $P \nmid \frac{O(G)}{O(N(a_i))}$ for some i

$\Rightarrow p^m \nmid \frac{O(G)}{O(N(a_i))}$ for some i

Since $p^m \mid O(G) = \frac{O(G)}{O(N(a_i))} . O(N(a_i))$ and $p^m \nmid \frac{O(G)}{O(N(a_i))}$, we have $p^m \mid O(N(a_i))$
Also, $O(N(a_i)) < O(G)$. As $p^{m+1} \nmid O(G)$, $p^{m+1} \nmid O(N(a_i))$.
So, by the induction hypothesis, $N(a_i)$ has a subgroup of order p^m. But anysubgroup of $N(a_i)$ is a subgroup of G also. Thus G has a subgroup of order p^m.

7.3.2: Theorem (Sylow's Theorem –I):

Let G be a finite group and p be a prime number. If $p^\alpha \mid O(G)$, then G has a subgroup of order p^α.

Proof: Let m be a non-negative integer such that $p^m \mid O(G)$ and $p^{m+1} \nmid O(G)$.Then by theorem 7.3.1, there exists a subgroup K of order p^m in G
But, given $p^\alpha \mid O(G)$

So, $\alpha \leq m$ and $p^{\alpha} \mid O(K)$

Therefore, by 7.2.6, K has a subgroup H of order p^{α}.
This implies that H is also a subgroup of G of order p^{α}.

7.4: THE THIRD PROOF:

In this section we present another proof of the Sylow's theorem which is completely different from either of the two earlier proofs. Here we shall first prove that the symmetric group S_{p^k} or degree p^k has a p-Sylow subgroup and later prove that, if G and M are finite groups such that $G \subseteq M$ and M has a p-Sylow subgroup, then G has a p-Sylow subgroup. Finally we shall use the Cayley's theorem to get a sufficiently large K such that G is embedded in S_{p^k}. Recall the order of S_{p^k} is $(p^k)!$

7.4.1: Definition: Let p be a fixed prime number. For any positive integer k, n(k) is defined to the the positive integer such that $p^{n(k)} \mid (p^k)$! and $p^{n(k)+1} \nmid (p^k)!$. In other words, $p^{n(k)}$ is the largest power of p that divides $(p^k)!$

7.4.2: Lemma: For any positive integer k, $n(k) = \sum_{i=1}^{k} p^{i-1} = 1 + p+p^2+\ldots..+ p^{k-1}$.

Proof: We shall use induction on k
If k =1, then $(p^k)! = p! = 1.2\ldots(1–p).p$.
Since $p \mid p!$ and $p^2 \nmid p$!, n(1) =1
Now, let k >1 and assume that the lemma is true for k–1.
Then we have $n(k–1) = 1 + p + p^2 + \ldots + p^{k–2}$.
It is clear that only the multiples of p, that is, p, 2p,..., p^{k-1}.p are divisors of $(p^k)!$
So, n(k) must be a power of p which divides
$p(2p)(3p)\ldots(p^{k–1}\ p).p^{p^{k-1}}.(p^{k-1})!$
Therefore, $n(k) = p^{k–1} + n(k–1) = p^{k–1} + p^{k–2} + \ldots + p+1$.

7.4.3: Lemma: For any prime p and positive integer k, the symmetric group S_{p^k} has a p-Sylow subgroup.

Proof: Let p be a prime number and k be a positive integer. We have to prove that S_{p^k} has a subgroup of order $p^{n(k)}$ where $n(k) = 1 + p + p^2 +\ldots+ p^{k–1}$.

We shall prove this by using induction on k.
If k = 1, then the cycle (1 2 ..... p) is an element of order p in S_p and so it generates a subgroup of order $p = p^{n(1)}$ (since n(1) =1) in S_p. Therefore, the lemma holds good for k = 1.
Now, let k >1 and assume that the lemma is true for k = 1. Then $S_{p^{k-1}}$ has a subgroup of order $p^{n(k–1).}$
Let us divide the integers 1,2,3,…, p^k into p clumps, each with $p^{k–1}$ elements as follows:

$\{1,2,3,.....,p^{k-1}\}, \{ p^{k–1} + 1,\ p^{k–1} + 2,.....,2p^{k–1}\}, ..., \{(p–1)\ p^{k–1} + 1, (p–1)\ p^{k–1} + 2,\ldots, p^k\}$.

Consider the cycles $\alpha_1, \alpha_2, \ldots\ldots\ldots\ldots, \alpha_{p^{k-1}}$ defined by

$\alpha_1 = (1, p^{k-1} + 1,\ 2p^{k-1} + 1, \ldots\ldots\ldots\ldots\ldots, (p-1).\ p^{k-1} + 1)$

$\alpha_2 = (2, p_2^{k-1} + 2, 2p^{k-1} + 2, \ldots\ldots\ldots\ldots\ldots, (p-1).\ p^{k-1} + 2)$

. . .

. . .

. . .

$\alpha_{p^{k-1}} = (p^{k-1}, 2p^{k-1}, 3p^{k-1}\ldots\ldots\ldots\ldots, p^k)$

Clearly $\alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_{p^{k-1}}$ are disjoint cycles, each of length p and hence $\alpha_i^p = e$, identity and $\alpha_i \alpha_j = \alpha_j \alpha_i$ for all $1 \leq i, j \leq p^{k-1}$.

Put $\sigma = \alpha_1 \alpha_2 \ldots\ldots\ldots \alpha_{p^{k-1}}$. Then $\sigma^p = e$ and σ satisfies the following property:

If $g \in S_{p^k}$ such that g(i) = i for all $i > p^{k-1}$, then $\sigma^{-j} g \sigma^j(i) = i$ for all $i \notin \{ jp^{k-1} + 1, jp^{k-1} + 2, \ldots, (j+1)p^{k-1}\}$.

Let $A = \{ g \in S_{p^k} \mid g(i) = i \text{ for all } i > p^{k-1}\}$

Then A is a subgroup of S_{p^k}.

Also, the mapping $g \mapsto g / I_{p^{k-1}}$ gives us an isomorphism of A onto $S_{p^{k-1}}$ and hence $A \cong S_{p^{k-1}}$.

By the induction hypothesis, A has a subgroup B_1 of order $p^{n(k-1)}$,

For $2 \leq j \leq p$, write $B_i = \sigma^{-(i-1)} B_1 \sigma^{i-1}$ and $B = B_1 B_2 \ldots\ldots\ldots B_p$

Each B_i is isomorphic to B_1 and hence $o(B_i) = o(B_1) = p^{n(k-1)}$ $\forall$ i

Also, for any $i \neq j$, $B_i B_j = B_j B_i$ (since $B_i(s) \neq s \Rightarrow B_j(s) = s$)

Therefore, B is a subgroup of S_{p^k}.

Also, since $B_i \cap B_j = \{e\}$ for $i \neq j$, it follows that

$O(B) = O(B_1)O(B_2) \ldots\ldots\ldots O(B_p)$

$= p^{n(k-1)} . p^{n(k-1)} \ldots\ldots\ldots p^{n(k-1)} = p^{n(k-1)p}$

Further, since $\sigma^p = e$ and $B_i = \sigma^{-(i-1)} B_1 \sigma^{i-1}$, it follows that $\sigma^{-1} B \sigma = B$.

Let $H = \{\sigma^j b \mid b \in B \text{ and } 0 \leq j \leq p-1\}$.

Since $\sigma \notin B$ and $\sigma^{-1} B \sigma = B$, we get that H is a subgroup of S_{p^k} and $O(H) = p.O(B) = p.p^{n(k-1)p} = p^{n(k-1)p+1} = p^{n(k)}$

Thus there exists a subgroup H of order $p^{n(k)}$ in S_{p^k}.

7.4.4: Self Assessment question: Prove that H, defined in the above proof is a subgroup of S_{p^k}.

7.4.5: Self Assessment question: Prove that $n(k-1).p+1 = n(k)$.

Before we reach the third proof of the Sylow's theorem, we need the following terminology.

7.4.6: Definition: Let G be a group and let A and B be subgroups of G. For any $x \in G$, let $AxB = \{axb \mid a \in A \text{ and } b \in B\}$. Then AxB is called a double coset of A, B in G.

7.4.7:Lemma: Let G be a group and let A and B be subgroups of G. Define a binary relation ~ on G as follows:

For any $x,y \in G$, $x \sim y \Leftrightarrow y = a x b$ for some $a \in A$ and $b \in B$.

Then ~ is an equivalence relation on G and the equivalence class of $x \in G$ is the set $AxB = \{ axb \mid a \in A, b \in B\}$

Proof: Let x, y,z $\in$G
(i) x ~ x as x = e x e, e$\in$ A $\cap$ B

(ii) Suppose that x ~ y

Then y = a x b for some a$\in$A and b$\in$B
Now a^{-1}y = xb and x = $a^{-1}yb^{-1}$, where $a^{-1}\in$A and $b^{-1}\in$B. So, y~x.
(iii) Suppose that x ~y and y~z

Then y = a_1 x b_1 and z = a_2yb_2 for some a_1, $a_2\in$A and b_1, $b_2\in$B

Now z = a_2 yb_2 = a_2 (a_1xb_1) b_2 = (a_2 a_1)x(b_1 b_2) where a_2, a_1 $\in$A and b_1, b_2 $\in$B. So, x~z
Therefore, '~'is an equivalence relation on G.

If [x] is the equivalence class containing x, then

[x] = { y$\in$G |x~y}

= {y$\in$G |y = a x b, a$\in$A,b$\in$B}

= {a x b/a$\in$A, b$\in$B}

= A x B

7.4.8 Lemma : If A, B are finite subgroups of a group G and x$\in$G, then the number of elementsin the double coset A x B is given by

$$|A \times B| = \frac{O(A).O(B)}{O(A \cap (xBx^{-1}))}$$

Proof: Let x$\in$G

Now we show that the sets AxB and $AxBx^{-1}$ have the same number of elements.

Define f : A x B $\rightarrow$A x Bx^{-1} by f(a x b) = $axbx^{-1}$for all axb$\in$AxB where a$\in$A and b$\in$B.
Suppose that f(a_1xb_1) = f(a_2 x b_2) where a_1,$a_2\in$A and b_1,$b_2\in$B.
Then we have a_1 x b_1x^{-1} = a_2x b_2x^{-1}
This implies that a_1 x b_1 = a_2x b_2 (by right cancellation law) So, f is one - one.

Let y$\in$A x Bx^{-1}

Then y = $axbx^{-1}$ for some a$\in$A, b$\in$B

Now axb$\in$AxB and f (a x b) = a x b x^{-1} = y. So, f is onto Ax Bx^{-1}.
Therefore f is a bijection of A x b onto A x Bx^{-1}

Hence, A x B and Ax Bx^{-1} have the same number of elements.

That is, |A x B| = |Ax Bx^{-1}|
Note that xBx^{-1} is a subgroup of G as B is a subgroup of G and O(B) = O(xBx^{-1}). Therefore,
|A x B| = | A x Bx^{-1}|

= | A . (xBx^{-1})|

$$= \frac{o(A).o(xBx^{-1})}{o(A \cap (xBx^{-1}))}$$

$$= \frac{o(A).o(B)}{o(A \cap (xBx^{-1}))}.$$

7.4.9. Self Assessment Question: For any subgroups A and B of a group G, prove that any two distinct double cosets are disjoint and that, if G is finite,

$O(G)=\sum_{i=1}^{n}|Ax_iB| = \sum_{i=1}^{n}\frac{O(A).O(B)}{O(A\cap(xBx^{-1})}$

7.4.10. Lemma: Let G be a subgroup of a finite group M and p be a prime number.Suppose that M has a p-Syllow subgroup Q. Then G has a p- Sylow subgroup P. In fact, P = G $\cap$ xQx^{-1} for some x$\in$M.

Proof: Suppose that M has a p-Sylow subgroup Q. Then O(Q) = p^m where p^m | O(M) and p^{m+1} $\nmid$ O(M) $\rightarrow$ 1. We shall prove that $G \cap xQx^{-1}$ is a p – Sylow subgroup of G for some x$\in$M.

Suppose p^n | o(G) and p^{n+1} $\nmid$ O(G).

Then o(G) = p^n.k for some integer k with p $\nmid$ k

Now we have to prove that O($G \cap xQx^{-1}$) = p^n for some x $\in$M

Consider the double cosets G xQ of G, Q in M. Since the double cosets from a partition of M, we have o(M) = $\sum |GxQ|$ where the sum runs over one element x form each double coset of G, Q in M.

By Lemma 7.4.8, we have | GxQ | = $\frac{o(G).o(Q)}{o(G\cap(xQx^{-1})} = \frac{(kp^n).p^m)}{o(G\cap(xQx^{-1}))}$

Observe that $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, and is a subgroup of G, and O(xQx^{-1}) = O(Q) = p^{m_x} and that o(G $\cap$ xQx^1) = p^{m_x} for some integer $0 \le m_x \le m$ and $0 \le m_x \le n$.

So, |GxQ| = $\frac{k.p^n.p^m}{p^{m_x}}$

If m_x < n for all x, then $p^{m+1} \mid \frac{k.p^n.p^m}{p^{mx}} = |GxQ|$ and that $p^{m+1} \mid \sum GxQ = O(M)$, which is a contradiction since p^{m+1} $\nmid$ O(M) .

So for some x$\in$M, m_x= n and that for this x, O($G \cap xQx^{-1}$) = p^n

Therefore, P := $G \cap xQx^{-1}$ is a p - Sylow subgroup of G.

In the following we present a third proof of the Sylow's theorem.

7.4.11: Theorem: (Sylow's theorem I):

Let G be a finite group, p be a prime number and α be any positive integer. If $p^\alpha \mid O(G)$, then G has a subgroup of order p^α.

Proof: Let o(G) = n. Consider the symmetric group of degree n, S_n. By Cayley's theorem (4.3.1), G can be regarded as a subgroup of S_n. Choose k such that $n \le p^k$. Now $I_n \subseteq I_{p^k}$ and hence any permutation on I_n can be regarded as a permutation on I_{pk} (see 4.2.5). Therefore, S_n can be regarded as a subgroup of S_{p^k} and hence G is a subgroup of S_{p^k}. By lemma 7.4.3. S_{p^k} has a p-Sylow subgroup. So, by lemma 7.4.10, G has a p-Sylow subgroup. Let P be a a p-Sylow subgroup of G. Now O(p) = p^m, where $p^m \mid$ O(G) and p^{m+1} $\nmid$ o(G). Since $p^\alpha \mid o(G)$, $\alpha \le m$. So, by 7.2.6. P has a subgroup of order p^α which will be a subgroup of G also.

7.5: SYLOW'S THEOREM:

Let G be a finite group. If P is a p-Sylow subgroup of G, then for any x$\in$G, xPx^{-1} is also

a p-Sylow subgroup of G, since O (xpx^{-1}) = O(p). In the following,we shall prove that any other p – Sylow subgroup of G must be of the form xpx^{-1} for some $x \in G$. Let us recall that two subgroups H and K of G are said to be conjugate if $H = xkx^{-1}$ for some $x \in G$

7.5.1: Theorem (Sylow's Theorem II):

If G is a finite group, p a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid O(G)$, then any two subgroups of G of order p^n are conjugate.

Proof: Let P and Q be subgroups of G, each of order p^n; that is, P and Q are p–Sylow subgroups of G. We have to prove that $P = xQx^{-1}$ for some $x \in G$. Double coset decomposition of G with subgroups P and Q is given by $G = \cup PxQ$ where the union runs over one element x from each double coset.

Now, $O(G) = \sum |PxQ|$ where the sum runs over one element x from each double coset.

For any $x \in G$, we have (by 7.4.8)

$$|PxQ| = \frac{O(P).O(Q)}{O\left(p \cap \left(xQx^{-1}\right)\right)} = \frac{p^n p^n}{O\left(p \cap \left(xQx^{-1}\right)\right)}$$

Observe that $p \cap (xQx^{-1})$ is a subgroup of P and is a subgroup of xQx^{-1} and that $O(p \cap (xQx^{-1}))$ $= p^{n_x}$ for some $0 \leq n_x \leq n$.

So, for any $x \in G$, $|PxQ| = \frac{p^n p^n}{p^{n_x}}$

If $n_x < n$ for all x, then $p^{n+1} \mid \frac{p^n p^n}{p^{n_x}} = |pxQ|$ for all x and that $p^{n+1} \mid \sum |PxQ| = O(G)$

which is a contradiction to the fact that $p^{n+1} \nmid O(G)$; So, $n_x = n$ for some $x \in G$.
Therefore, $O(p \cap (xQx^{-1})) = p^n = O(p)$ and
Hence $p \cap (xQx^{-1}) = p$ and that $p \subseteq (xQx^{-1})$
But $O(P) = O(xQx^{-1}) = p^n$. So, $P = xQx^{-1}$
Thus there exists $x \in G$ such that $p = xQx^{-1}$
Hence P and Q are conjugate.

7.5.2. Self Assessment Question:

Determine all 2-Sylow subgroups of S_3 and A_4.

7.5.3. Self Assessment Question:

Prove that a p-Sylow subgroup is normal if and only if it is the unique p-Sylow subgroup.

7.5.4. Definition: Let G be a group and H be a subgroup of G. Then the normalizer of H in G, denoted by N(H), is defined as $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

Note that if H is a subgroup of G, then N(H) is a subgroup of G, and H is a normal subgroup of N(H).

7.5.5. Lemma: Let G be a finite group and p be a prime number. Then the number of p-Sylow subgroups of G is equal to O(G) / O(N (P)) where P is a p-Sylow subgroup of G. In particular, this number is a divisor of O(G).

Proof: Let P be any p-Sylow subgroup of G and let X be the set of all p-Sylow subgroups of G. Then, by Sylow's theorem II (7.5.1) we have

$X = \{xpx^{-1} \mid x \in G\}$

It is easy to see that the mapping $xpx^{-1} \longmapsto N(P)x$ is a bijection of X onto the set of right cosets of N(P) in G.

So, the number of p-Sylow subgroups is equal to the index of N(P) in G which is same as O(G) / O(N (P)) and this divides O(G).

7.5.6 Self Assessment Question:

Prove that the number of p-Sylow subgroups of a group G is a divisor of the index of a p-Sylow subgroup in G.

7.6. SYLOW'S THEOREM - III:

In the previous section, we have proved that the number of p-Sylow subgroups of a group G is a divisor of O(G). The following gives us more information about this number.

7.6.1 Theorem (Sylow's Theorem-III) : Let G be a finite group and p be a prime number. Then the number of p-Sylow subgroups of G is of the form 1+pk for some integer $k \geq 0$.

Proof: Let P be any p-Sylow subgroup of G. Then $O(P) = p^n$ where $p^n \mid O(G)$ and $p^{n+1} \nmid o(G)$. Consider the normalizer of P in G, N(P). By lemma 7.5.5, the number of p-Sylow subgroups of G is equal to $\frac{O(G)}{O(N(P))}$.

Now we show that the number of p-Sylow subgroups of G is of the form 1+pk forsome integer $k \geq 0$. Consider the double cosets pxp, $x \in G$.

Suppose px_1p, px_2p, ..., px_rp are all the distinct double cosets in G where $x_i \in G$. For i = 1,2, ...,r.

Since these form a partition of G, we have $o(G) = \sum_{i=1}^{r} |Pxi\ P|$

We can assume that $x_1, x_2, \ldots\ldots, x_l \in N(P)$ and $x_{l+1}, \ldots\ldots, x_r \notin N(P)$.

Observe that $x \in N(P) \Leftrightarrow xPx^{-1} = P \Leftrightarrow xP = Px$.

So, for $x \in N(p)$, $PxP = Px$ a right coset of p in N(P), and $o(PxP) = o(Px) = o(P) = p^n$

Also, $x \notin N(P) \Leftrightarrow xPx^{-1} \neq P \Leftrightarrow P \cap (xPx^{-1}) \neq P$

So, for $x \notin N(P)$, $O(P \cap (xPx^{-1})) = p^n x$ for some $0 \leq n_x < n$ therefore for $x \notin N(P)$,

$|PxP| = \frac{O(P).O(P)}{O(P \cap (xpx^{-1}))} = \frac{p^n p^n}{p^n x} = p^{2n-n_x}$ and $2n - n_x \geq n+1$

This implies that $p^{n+1} \mid |pxp|$ for every $x \notin N(P)$

Now $o(G) = \sum_{i=1}^{r} |Px_i\ P| = \sum_{i=1}^{r} |Px_i\ P| + \sum_{i=1+1}^{r} |Px_i\ P|$

$= lp^n + p^{n+1}.k$ for some integer $k \geq 0$.

Let $x \in N(p)$. Then $Px = PxP = Px_i\ P$ for some $1 \leq i \leq r$.

This shows that every right coset of P in N(P) must be of the form Px_i for some $1 \leq i \leq l$. So, there are exactly l number of distinct right cosets of P in N(P),

As $x_i \in Px_i\ P$, $x_i \in Px$. So, $x^{-1} x_i \in P \subseteq N(P)$

which implies that $x_i \in N(P)$ and hence $1 \leq i \leq l$.

l = the index of P in N(P) $= \frac{o(N(P))}{O(P)} = \frac{O(N(P))}{p^n}$.

Therefore, $O(G) = O(N(P)) + p^{n+1}.k$

(Or)

$$\frac{O(G)}{O(N(P))} = 1 + pk.$$

Hence, the number of p-Sylow subgroups of G is of the form 1+pk for some $k \geq 0$.

In the following examples, we shall demonstrate how these three Sylow theorems can be used to know about the structure of finite groups.

7.6.2: Example : Let G be a group of order $11^2.13^2$. We shall show that G is abelian.

By 7.5.6 and 7.6.1, the number of 11- Sylow subgroups of G is of the form 1+11k for some integer $k \geq 0$ and $(1+11k) \mid O(G)$. It is clear that $(11^2, 1+11k) = 1$. So, $(1+11k) \mid O(G) = 11^2.13^2$ implies $(1+11k) \mid 13^2$ only for k = 0, 1+11k divides 13^2. So, the number of 11-Sylow subgroups is 1+11(0) =1.

Also, the number of 13-Sylow subgroups of G is 1+13k for some integer $k \geq 0$ and $(1+13k) \mid O(G)$. As $(13^2, 1+13k)=1$, $(1+13k) \mid O(G) = 11^2.13^2$ implies $(1+13k) \mid 11^2$. Only for k = 0, 1+13k divides 11^2. So, the number of 13-Sylow subgroups is1+13(0) =1.

Let H be the 11- Sylow subgroup of G of order 11^2 and K be the 13-Sylow subgroup of G of order 13^2. Since each conjugate of H is a 11-Sylow subgroup of G, H is a normal subgroup of G. Similarly, K is a normal subgroup of G.

Since $O(H \cap K)$ is a common divisor of 11^2 and 13^2, $O(H \cap K)=1$; that is, $H \cap K = \{e\}$.

So, $|HK| = \frac{O(H).O(K)}{O(H \cap K)} = \frac{11^2.13^2}{1} = O(G)$

Therefore, G = HK

Further, for any $x \in H, y \in K$, we have

$xyx^{-1}y^{-1} = (xyx^{-1})\, y^{-1} \in K$ ($\because$ K is normal)

$= x(yx^{-1}y^{-1}) \in H$ ($\because$ H is normal)

and hence $xyx^{-1}y^{-1} \in H \cap K = \{e\}$. This implies that

$xyx^{-1}y^{-1} = \{e\}$ and that xy = yx

Thus xy = yx for all $x \in H$ and $y \in K$

Let $g_1, g_2 \in G$. Now $g_1 = x_1y_1$ and $g_2 = x_2y_2$ for some $x_1, x_2 \in H$ and $y_1, y_2 \in K$. Observe that H and K are abelian groups as their orders are of the prime squares

Now $g_1g_2 = (x_1\ y_1)\ (x_2\ y_2)$

$= (x_1y_1x_2)\ y_2$

$= (x_2\ x_1)\ (y_2y_1)$

$= (x_2y_2)\ (x_1y_1)$

Therefore, $g_1g_2 = g_2g_1$

Hence, G is an abelian group.

7.6.3: Self Assessment Question: Prove that any group of order 1225 is abelian.

7.6.4: Example: We shall prove that any group of order 72 is not simple. Let G be a group of order 72. Then, $O(G) = 72 = 2^3.3^2$. The number of 3-Sylow subgroups of G is 1+3K for some integer $k \geq 0$ and $(1+3k) \mid o(G) = 72$. Since $(3^2, 1+3k) = 1$, we have $1+3k \mid 2^3$.

The only factors of 8 of the form 1+3k are 1 and 4. So, the number of 3-Sylow subgroups is 1 or 4. If the number of 3 –Sylow subgroups is 1, then there is a unique 3-Sylow subgroup which must be normal and is of order 3^2, so that it is a nontrivial proper normal subgroup of G.

Suppose the number of 3-Sylow subgroups is 4. Let P be a 3-Sylow subgroup of G. By lemma 7.5.5, $\frac{O(G)}{O(N(P))} = 4$: that is , i(N(P)) = 4.

Since $O(G) \nmid i(N(P))!$, it follows , by theorem (4.4.4) that N(P) contains a nontrivial normal

subgroup H of G.
As $H \subseteq N(P) \neq G$, H is a normal subgroup of G.
Therefore G is not simple.

7.6.5: Problem: Show that a group of order 108 has a normal subgroup of order 3^k,where k = 2 or 3.

Solution: Let G be a group of order 108 = $2^3.3^3$. By 7.5.6 and 7.6.1, the numberof 3-Sylow subgroups of G is of the form 1+3k for some integer $k \geq 0$, and (1+3k) | O(G) = 108. Since (3^3, 1+3k) =1, (1+3k)\$2^3$. Now k = 0 or 1.

Case (i): Suppose k = 0
Then 1 + 3k= 1+3(0) =1
So, G has only one 3-Sylow subgroup which must be normal and is of order 3^3.

Case (ii) : Suppose k =1.
Then 1 +3k = 1+ 3(1) = 4.
So, G has four 3–Sylow subgroups. Let A and B be any two 3 - Sylow subgroups of G. Now O(A)= O(B) = 3^3.
Since $A \cap B$ is a subgroup of A and B, O(A∩B)| O(A) = 3^3. So, O(A∩B)=1 or 3 or 3^2
If O(A∩B) = 1 or 3, then
$|AB| = \frac{O(A).O(B)}{O(A \cap B)} = \frac{3^3 \times 3^3}{O(A \cap B)} > O(G) = 2^2 \times 3^3$, which is a contradiction
Therefore, O(A∩B) = 3^2
We know that for a group of order p^n, any subgroup of it of order p^{n-1} is a normal subgroup of it, where p is a prime and n is a positive integer. So, $A \cap B$ is a normal subgroup of A and B.
Therefore, $A \subseteq N(A \cap B)$ and $B \subseteq N(A \cap B)$, where $N(A \cap B)$ is the normalizer of $A \cap B$ in G and is a subgroup of G.
So, $AB \subseteq N(A \cap B)$. But $|AB| = \frac{O(A).O(B)}{O(A \cap B)} = \frac{3^3 \times 3^3}{3^2} = 81.$
We have $O(N(A \cap B)) \geq 81$ and $O(N(A \cap B)) | O(G) = 2^2 \times 3^3$.
Therefore, $O(N(A \cap B))$= O(G) and that $N(A \cap B)$ = G.
Hence, $A \cap B$ is a normal subgroup of G of order 3^2.

7.6.6: Problem: Let G be a finite group of order pq where p,q are prime numbers and p > q.

If $q \nmid (p-1)$, then show that G is cyclic.

Solution: Suppose $q \nmid (p-1)$. We shall prove that G is cyclic. The number of p- Sylow subgroups of G is of the form 1+pk for some integer $k \geq 0$ and 1+pk | O(G) = pq. Since (p, 1+pk) =1, 1+pk | q.
It is possible only when k =0 as p > q.
So, there is only one (1+p(0)=1) p-Sylow subgroup A of G of order p, which must be normal in G. The number of q-Sylow subgroups of G is of the form 1+qk for some integer $k \geq 0$, and 1+qk | O(G) = pq.
Since (q,1+qk) =1, 1+qk | p
Since p is prime and p > q , 1+qk = 1 or p
If 1+qk = p, then qk = p –1 and that q | (p–1), a contradiction to $q \nmid (p-1)$. So 1+qk =1; that is the number of q -Sylow subgroups of G is 1. Thus there exists a unique q-Sylow subgroup B of G of order q which must be normal in G. Since each of A and B has order a prime number, both A and B are cyclic and that A = (a) for some $e \neq a \in A$, B = (b) for some $e \neq b \in B$. Observe that $A \cap B = \{e\}$ as O(A) = p and O(B) = q are prime numbers with p > q.

Now AB is a normal subgroup of G and O(AB) = $\frac{O(A).O(B)}{O(A\cap B)}$ = O(A) . O(B) = pq = O(G) and that G = AB. We show now that O(ab) = pq.

Since A and B are normal subgroups of G and a∈A, b∈B and $A \cap B$ ={e}, we have ab = ba.

Consider $(ab)^{pq}$ = (ab) (ab)……..(ab) (pq times)

$= a^{pq}\, b^{pq}$

$= (a^p)^q\, (b^q)^p$

$= e^q.e^p$ ($\therefore$ O(a) = p & O(b) = q)

= e.e = e

Suppose n is a positive integer and $(ab)^n$ = e. Then $a^n b^n$ = e and that $a^{-n} = b^n \in A \cap B = \{e\}$ implies a^n = e and b^n = e. Since O(a) = p amd O(b) = q, p|n andq|n, so that pq |n as (p,q)=1. Thus n $\geq$ pq. Therefore, pq is the least positive integer such that $(ab)^{pq}$ = e. This is to say that O(ab) = pq. Hence G = (ab) is a cyclic group.

7.7. MODEL EXAMINATION QUESTIONS:

7.7.1. State and prove Sylow's theorem–I

7.7.2. Define the concept of a p-Sylow subgroup and prove that any two p-Sylow subgroups of a finite group are conjugate.

7.7.3: State and prove Sylow's theorem - III

7.7.4: Prove that the number of p-Sylow subgroups of a finite goup G is a divisor of O(G) and is of the form 1+ pk, k$\geq$0.

7.8. EXERCISE:

7.8.1: Prove that any group of order 1986 is not simple.

7.8.2: If G is a group of order 385, show that its 11-Sylow subgroup is normal and its7-Sylow subgroup is in the center of G.

7.9 SUMMARY:

In this lesson we have learnt the three Sylow's theorems on the existence of p-Sylow subgroups of a finite group. Using these Sylow's theorems,we have determined the structure of certain group of given orders.

7.10 TECHNICAL TERMS:

- P-Sylow subgroup
- Conjugate subgroups
- Sylow's theorems
- Normalizer N(P)
- Double coset A x B
- Simple group
- Cyclic group

7.11 ANSWERS TO SELF ASSESSMENT QUESTIONS:

7.2.2: Since $\beta \leq \alpha$, we have $p^\beta \mid p^\alpha$ and $p^\beta \mid p^\alpha$ m. Therefore, $p^\beta \mid p^\alpha$ m – i $\Leftrightarrow$ $p^\beta \mid p^\alpha$ – i .

7.2.4: Let G be a group of order 2500 = $5^4.2^2$. We have 5^3 | O(G) and 5 is prime. By theorem 7.2.3, G has a subgroup of order 5^3=125.

7.2.6: We may assume that O(G) = p^n where n $\in \mathbb{Z}^+$.We shall use induction on n. If n =1,

then {e} and G are subgroups of orders p^o and p^1 respectively. Now suppose that n > 1 and assume that the result is true for all groups of order p^m, m <n. Then by theorem 6.4.1, $Z(G) \neq \{e\}$. Since Z(G) is a subgroup of G, $O(Z(G)) \mid O(G) = p^n$ and hence $O(Z(G)) = p^\alpha$, $\alpha > o$. Since $p \mid O(Z(G))$, by Cauchy's theorem, Z(G) has an element of order p. Let $e \neq a \in Z(G)$ and $a^p = e$. Now (a) is a normal subgroup of G (since ax =xa for all $x \in G$) and G/(a) is of order p^{n-1}. Since $p^r \mid O(G)$, $0 < r \leq n$, We have $p^r \mid O(G/(a))$ and hence G/(a) has a subgroup of order p^{r-1}. If K is a subgroup of G/(a), then the subgroup H defined by $H = \{x \in G \mid (a)\ x \in K\}$ has order p^r in G , (since H/(a) = k and (a) =p).

7.2.7: This follows from the facts that $81 = 3^4$, $3^4 \mid 405$ and 3 is prime and by theorem7.2.3, G has a subgroup of order $3^4 = 81$, if o(G) = 405.

7.4.4: Since $\sigma^{-1}B\sigma = B$, we have $\sigma^{-j} B \sigma^j = B$ and hence $B\sigma^j = \sigma^j B$.

Now for any $0 \leq i, j \leq p-1$ and $b_1, b_2 \in B$,

$$(\sigma^i b_1)(\sigma^j b_2)^{-1} = \sigma^i b_1 b_2 \sigma^{-j} \epsilon \sigma^j B \sigma^{-j}$$

$$= B\sigma^i\sigma$$

$$= B\sigma^k$$

$$= \sigma^k B \text{ for some } 0 \leq k \leq p-1 \text{ (since } \sigma^p = e)$$

Thus H is a subgroup of S_{p^k}.

7.4.5: By lemma 7.4.2, $n(k) = 1+p+p^2+ \ldots\ldots\ldots\ldots +p^{k-1}$

$$= 1+p(1+p+p^2+\ldots\ldots\ldots+p^{k-2})$$

$$= 1+ p.n(k-1).$$

7.4.10: This follows from the fact that the double cosets A x B, $x \in G$, form a partition of G and by lemma 7.4.8.

7.5.2: (i) $O(S_3) = 3! = 6$ and the order of any 2-Sylow subgroup of S_3 must be 2. Let f = (1 2) , g = (2 3) and h = (3 1). Then (f), (g) and (h) are all the 2-Sylow subgroups of S_3 (Note that the number of 2-Sylow subgroups of S_3 is a divisor of 6 and is of the form 1+2k and hence it is 1 or 3 ; In this case, it is 3).

(ii) $O(A_4) = 12$ and hence the order of any 2-Sylow subgroups is $2^2 = 4$ and there arethree 2-Sylow subgroups in A_4.

7.5.3: Let P be a p-Sylow subgroup of G. Then any p-Sylow subgroup is of the form xpx^{-1} for some $x \in G$. Therefore

P is unique $\Leftrightarrow$ $xPx^{-1} = P$ for all $x \in G$

$\Leftrightarrow$ P is normal.

7.5.6: Let P be a p-Sylow subgroup of G and let N(P) be the normalizer of p. We know that the number of p-Sylow subgroups is equal to $\frac{O(G)}{O(N(P))}$.

Since $P \subseteq N(p)$, we have $i(p) = \frac{O(G)}{O(P)} = \frac{O(G)}{O(N(P))} \cdot \frac{O(N(P))}{O(P)}$ (since O(p) | O(N(p))) and hence $\frac{O(G)}{O(N(P))}$ is a divisor of i(P).

7.6.3: $1225 = 5^2 \times 7^2$ and now imitate the argument given in 7.6.2.

7.12 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. K. SIVA PRASAD

LESSON -8

DIRECT PRODUCTS

OBJECTIVES:

The objectives of this lesson are to

- ❖ define the concept of an external direct product of groups and quote certain examples
- ❖ define the notion of an internal direct product and prove that any internal direct product is isomorphic to an external direct product and vice- versa.

STRUCTURE:

8.1. INTRODUCTION:

If (A, •) and (B, $*$) are any two groups, we can define a binary operation on the Cartesian product A x B in a natural way as $(a_1, b_1) . (a_2, b_2) = (a_1.a_2, b_1 * b_2)$, and with respect to this binary operation, A x B becomes a group whose properties largely depend on those of A and B. In this lesson we discuss certain necessary and sufficient conditions for a group G to be represented as A x B where A and B are groups again.

8.2. EXTERNAL DIRECT PRODUCTS:

We are already in the habit of using the same symbol '+' to denote the addition of real numbers, addition of complex numbers, addition of matrices, addition of functions and on several other occasions. There is no ambiguity if we are aware of what elements are to be added. Therefore, we have agreed to denote the binary operation on an abstract group by the symbol, and even this is not mentioned explicitly, with this understanding, we are simply saying that "G is a group" instead of " (G, •) is a group".

8.2.1: Definition: Let A and B be two groups. Define a binary operation '•'on the Cartesian product A x B as follows:
For any $(a_1, b_1) , (a_2, b_2) \in$ A x B, define
$(a_1, b_1) . (a_2, b_2) = (a_1. a_2, b_1. b_2)$ where $a_1. a_2$ is the product of a_1 and a_2 in A and $b_1. b_2$ is the product of b_1 and b_2 in B. A x B is called the external direct product of A and B and the binary operation defined on A x B is called as component wise operation.

8.2.2. Theorem: Let A and B be two groups. Then A x B is a group under the binary operation defined as above.

Proof: Let (a, b), (a^1, b^1), $(a^{11}, b^{11}) \in$A x B

Now $((a, b).(a^1, b^1)).(a^{11}, b^{11})$

$= (aa^1, bb^1).(a^{11}, b^{11})$

$= ((aa^1)a^{11}, (bb^1)b^{11})$

$= (a(a^1a^{11}), b(b^1b^{11}))$ (by the associatively in A and B)

$= (a, b).(a^1a^{11}, b^1b^{11})$

$= (a, b)((a^1,b^1).(a^{11}, b^{11}))$

Therefore'$\bullet$'is associative in A x B

Let e and e^1 denote the identity elements in A and B, respectively.

Then $(e, e^1) \in$ A x B,

and $(a, b)(e, e^1) = (ae, be^1)$

$= (a, b)$

$= (ea, e^1b)$

$= (e, e^1)(a, b)$

Therefore, (e, e^1) is the identity element in A x B.

We have $a^{-1} \in$ A and $b^{-1} \in$ B. So, $(a^{-1}, b^{-1}) \in$ Ax B and

$(a, b). (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1})$

$= (e, e)$

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

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

Therefore, (a^{-1}, b^{-1}) is the inverse of (a, b) in A x B; That is, $(a, b)^{-1} = (a^{-1}, b^{-1})$
Hence, A x B is a group.

The above idea can be extended to the product of any finite number of groups. Explicitly we have the following theorem.

8.2.3: Theorem: Let G_1, G_2, ..., G_n be groups and $G = G_1 x\ G_2 x$ .....x G_n, the cartesian product of G_1, G_2, ..., G_n. Then G is a group under component wise product [G is called the (external) direct product of G_1, G_2, ……, G_n].

Proof: Let $(g_1, g_2, ..., g_n), (g_1^1, g_2^1, ..., g_n^1), (g_1^{11}, g_2^{11}, ..., g_n^{11}) \in G$

(i) $(g_1, g_2, ..., g_n)(g_1^1, g_2^1, ..., g_n^1) = (g_1g_1^1, g_2 g_2^1, ..., g_ng_n^1) \in G.$

(ii) $(g_1, g_2, …., g_n)((g_1^1, g_2^1, …., g_n^1)(g_1^{11}, g_2^{11}, ..., g_n^{11}))$

$= (g_1, g_2, …., g_n) (g_1^1g_1^{11}, g_2^1g_2^{11}, ..., g_n^1g_n^{11})$

$= (g_1(g_1^1g_1^{11}), g_2(g_2^1g_2^{11}), ……, g_n(g_n^1g_n^{11}))$

$= ((g_1g_1^1)g_1^{11}, (g_2g_2^1)g_2^{11}, ……, (g_ng_n^1)g_n^{11})$

$= (g_1 g_1^1, g_2 g_2^1, \ldots, g_n g_n^1)\ (g_1^{11}, g_2^{11}, \ldots, g_n^{11})$

$= ((g_1, g_2, \ldots, g_n)(g_1^1, g_2^1, \ldots, g_n^1))\ (g_1^{11}, g_2^{11}, \ldots, g_n^{11})$

Therefore, '•'is associative in G.

(iii) Let e_i denote the identity element of G_i, $1 \le i \le n$

Then $(e_1, e_2, \ldots, e_n) \in G$ and

$(e_1, e_2, \ldots, e_n)(g_1, g_2, \ldots\ldots, g_n) = (e_1 g_1, e_2 g_2, \ldots\ldots, e_n g_n)$

$= (g_1, g_2, \ldots\ldots, g_n)$

$= (g_1 e_1, g_2 e_2, \ldots, g_n e_n)$

$= (g_1, g_2, \ldots\ldots, g_n)(e_1, e_2, \ldots, e_n)$

Therefore, $(e_1, e_2, \ldots, e_n)$ is the identity element of G.

(iv) We have $g_i^{-1} \in G_i$, $1 \le i \le n$.
So, $(g_1^{-1}, g_2^{-1}, \ldots\ldots, g_n^{-1}) \in G$ and
$(g_1, g_2, \ldots\ldots, g_n)(g_1^{-1}, g_2^{-1}, \ldots\ldots, g_n^{-1}) = (e_1, e_2, \ldots, e_n)$

$= (g_1^{-1}, g_2^{-1}, \ldots\ldots, g_n^{-1})\ (g_1, g_2, \ldots\ldots, g_n)$

Therefore $(g_1^{-1}, g_2^{-1}, \ldots\ldots, g_n^{-1})$ is the inverse of $(g_1, g_2, \ldots\ldots, g_n)$ in G or equivalently

$(g_1, g_2, \ldots\ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots\ldots, g_n^{-1})$

Thus, G is a group.

8.2.4. Self Assessment Question: Let A and B be groups, a ∈ A and b ∈ B. Suppose O(a) = n in A and O(b) = m in B. Then prove that O(a,b) = l.c.m of{n,m}in A x B.

8.3. INTERNAL DIRECT PRODUCTS:

Take the additive group Z_6 of integers modulo 6. Then $Z_6 = \{0, 1, 2, 3, 4, 5\}$.
Let A = {0, 3} and B = {0, 2, 4}. Now A and B are subgroups of Z_6.

So, we can treat A and B as groups on their own. It can be easily verified that every element x in Z_6 has a unique representation of the form x = a + b with a ∈ A and b ∈ B.

Also, the map (a, b) ↦ a + b: A x B → Z_6 is an isomorphism of A x B onto Z_6. Hence Z_6 is isomorphic to the external direct product of the groups A and B. This motivates the following.

8.3.1. Definition: Let G be a group and $N_1, N_2, \ldots\ldots, N_k$ be normal subgroups of G. Then G is called internal direct product of $N_1, N_2, \ldots\ldots, N_k$ if
(i) $G = N_1 N_2 \ldots\ldots N_k$, and

(ii) every element $g \in G$ can be uniquely expressed as $g = a_1 a_2 \ldots a_n$ with $a_i \in N_i$, $1 \le i \le k$.

8.3.2. Lemma: Let $N_1, N_2, \ldots, N_k$ be normal subgroups of a group G such that G is the internal direct product of $N_1, N_2, \ldots, N_k$. Then the following hold for any $i \neq j$.

(i) $N_i \cap N_j = \{e\}$.

(ii) $ab = ba$ for any $a \in N_i$ and $b \in N_j$.

Proof: Let $1 \le i \ne j \le k$

(i) Let $x \in N_i \cap N_j$. Then $x \in G = N_1 N_2 \ldots\ldots\ldots N_k$.

This implies that x = e..... e xe.....e and

x = e.....e.....e xe.....e

(i^{th} position)

Since G is the internal direct product of $N_1, N_2, \ldots, N_k$, the element $x \in G$ has a unique representation as a product of elements of N_i, I = 1, 2, ..., k. So, x = e. Therefore, $N_i \cap N_j = \{e\}$.

(ii) Let $a \in N_i$ and $b \in N_j$

Consider $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in N_i$ (since $a \in N_i$ and N_i is normal)

$= (aba^{-1})\, b^{-1} \in N_j$ (since $b \in N_j$ and N_j is normal)

Therefore, $aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$ and
hence $aba^{-1}b^{-1} = e$;
That is, $ab = ba$

8.3.3. Theorem: Let G be a group and suppose that G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_k$. Let $T = N_1 \times N_2 \times \ldots \times N_k$, the external direct product of $N_1, N_2, \ldots, N_k$. Then T is isomorphic to G.

Proof: Define $f: T \to G$ by $f(x_1, x_2, \ldots, x_k) = x_1 x_2 \ldots x_k$ for all $(x_1, x_2, \ldots, x_k) \in T$.
By lemma 8.3.2 (ii), we have $ab = ba$ for all $a \in N_i$ and $b \in N_j$ and $i \neq j$……..(1)
We show that f is an isomorphism. Let $(x_1, x_2, \ldots, x_k), (y_1, y_2, \ldots, y_k) \in T$.

(i) Now $h((x_1, x_2, \ldots, x_k)(y_1, y_2, \ldots, y_k))$

$= h(x_1y_1, x_2y_2, \ldots, x_ky_k)$

$= (x_1y_1)(x_2y_2) \ldots (x_ky_k)$

$= x_1(y_1x_2)y_2x_3y_3 \ldots x_ky_k$ (by(1))

$= x_1 (x_2y_1)y_2x_3y_3 \ldots x_ky_k$

$= x_1x_2x_3y_1y_2y_3x_4y_4 \ldots x_ky_k$

$= (x_1, x_2, ..., x_k)(y_1, y_2, \ldots, y_k)$

$= h(x_1, x_2, ..., x_k)h(y_1, y_2, \ldots, y_k)$

Therefore, h is a homomorphism.

(ii) Suppose that $h(x_1, x_2, ..., x_k) = h(y_1, y_2, \ldots, y_k)$

Then $x_1x_2.....x_k = y_1y_2.....y_k$

Since G is the internal direct product of $N_1, N_2, ..., N_k$ and $x_i, y_i \in N_i$, $1 \le i \le k$,

we have $x_1 = y_1, x_2 = y_2, ..., x_k = y_k$

So, $(x_1, x_2, ..., x_k) = (y_1, y_2, \ldots, y_k)$

Therefore, h is one-one.

(iii) Let $g \in G$. Now $g = n_1n_2.....n_k$ for some $n_i \in N_i, 1 \le i \le k$. So$(n_1, n_2, \ldots, n_k) \in T$ and

$T(n_1, n_2, ..., n_k) = n_1n_2.....n_k = g$

Therefore, T is onto G. Hence, T is isomorphic to G.

8.3.5. Theorem: Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 x G_2 x.....x G_n$, the external direct product of $G_1, G_2, \ldots, G_n$. For any $1 \le i \le n$, let $\overline{G}_i = \{(e_1,...e_{i-1}, g_i, e_{i+1}....., e_n) \ / \ g_i \in G_i\}$. Then each $\overline{G}_i$ is a normal subgroup of G, G is the internal direct product of $\overline{G}_1, \overline{G}_2,\ldots, \overline{G}_n$ and G_i is isomorphic to $\overline{G}_i$, $1 \le i \le n$.

Proof: Fix $1 \le i \le n$.
Clearly $\overline{G}_i \subseteq G$ and $\overline{G}_i \neq \phi$ as $(e_1, e_2, \ldots, e_n) \in \overline{G}_i$ We shall prove that $\overline{G}_i$ is a normal subgroup of G.
Let $(e_1, \ldots e_{i-1}, g_i, e_{i+1}\ldots, e_n), (e_1, e_2, \ldots e_{i-1}, g_i^1, e_{i+1}\ldots, e_n) \in \overline{G}_i$ and $(x_1, x_2,....., x_n) \in G$
(i) $(e_1, \ldots e_{i-1}, g_i, e_{i+1}\ldots, e_n)(e_1, e_2, \ldots, e_{i-1}, g_i^1, e_{i+1}\ldots, e_n)=(e_1, e_2, ..e_{i-1}, g_ig_i^1, e_{i+1}.., e_n) \in \overline{G}_i$
(ii) $(e_1, \ldots e_{i-1}, g_i, e_{i+1}\ldots, e_n)^{-1}=(e_1, e_2, \ldots e_{i-1}, g_i^{-1}, e_{i+1}\ldots, e_n) \in \overline{G}_i$
So, $\overline{G}_i$ is a subgroup of G.
(iii) Now $(x_1, .., x_{i-1}, x_i, x_{i+1} ,.., x_n) (e_1, \ldots e_{i-1}, g_i, e_{i+1}\ldots, e_n) (x_1, .., x_{i-1}, x_i, x_{i+1}, .., x_n)^{-1}$
$= (e_1, \ldots e_{i-1}, x_ig_ix_i^{-1}, e_{i+1}\ldots, e_n) \in \overline{G}_i$.
Therefore, $\overline{G}_i$ is a normal subgroup of G, $1 \le i \le n$.

Also, for any $g = (g_1, g_2, ..., g_n) \in G$, we can write
$g = (g_1, e_2, \ldots, e_n).(e_1, g_2, e_3, \ldots, e_n).....(e_1, e_2, \ldots, e_{n-1}, g_n) \in \overline{G}_1\overline{G}_2..... \overline{G}_n$

Therefore any element of G can be expressed as an element in the product $\overline{G}_1\overline{G}_2..... \overline{G}_n$. It can be easily verified that this representation is unique also.
Hence, G is the internal direct product of $\overline{G}_1, \overline{G}_2,\ldots, \overline{G}_n$. Now for any $1 \le i \le n$, define f_i: $G_i \to \overline{G}_i$ by $f_i(g_i) = (e_1, ..., e_{i-1}, g_i, e_{i+1},....., e_n)$for all $g_i \in G_i$. It is easy to see that f_i is an isomorphism. Hence, $G_i \cong \overline{G}_i$. $1 \le i \le n$.

8.3.6: Problem: Let G be a group and N_1, N_2, ..., N_k be normal subgroups of G. Then prove that G is the internal direct product of N_1, N_2, ..., N_k, if and only if, the following are satisfied.

(i) ..... $G = N_1N_2.....N_k$

(ii) For each $1 \le i \le n$, $N_i \cap (N_1N_2.....N_{i-1}N_{i+1}.....N_k) = \{e\}$

Solution: First assume that G is the internal direct product of N_1, N_2, ..., N_k.

Then any element g of G can be uniquely expressed as $g = a_1a_2\ldots a_k$ where $a_i \in N_i$, $1 \le i \le k$.

This implies that $G = N_1N_2.....N_k$. Fix $1 \le i \le k$.

Let $a \in N_i \cap (N_1N_2,...N_{i-1}N_{i+1}.....N_k)$. Then $a \in N_i$ and $a=a_1a_2.....a_{i-1}a_{i+1}.....a_n$ for some $a_j \in N_j$ all $j \ne i$.

So, ee...e.a.e.....e = $a = a_1a_2.....a_{i-1}ea_{i+1}.....a_k \in N_1N_2.....N_k = G$.

By the uniqueness, it follows that $a_j = e$ for all $j \ne i$ and $a = e$.

Therefore $N_i \cap (N_1N_2,...N_{i-1},N_{i+1}.....N_k) = \{e\}$ for i = 1,2,…,k

Conversely, assume the conditions (i) and (ii).

We shall show that G is the internal direct product of N_1,N_2, ...,N_k

Let $g \in G$ and $g = a_1a_2.....a_k = b_1b_2.....b_k$ where a_i, $b_i \in N_i$ for i=1, 2, ..., k. Fix $1 \le i \le k$.

Then we have $a_1a_2.....a_i = b_1b_2.....b_k\, a_k^{-1}a_{k-1}^{-1}\ldots\ldots\, a_{i+1}^{-1}$

$\Rightarrow a_i = a_{i-1}^{-1}a_{i-2}^{-1}.....a_2^{-1}a_1^{-1}b_1b_2\ \ldots\ldots b_ka_k^{-1}a_{k-1}^{-1}\ldots.a_{i+1}^{-1} \rightarrow (\alpha)$

Let $1 \le j \le n$ with $j \ne i$ be fixed.

Clearly, $N_j \subseteq N_1N_2\ldots.N_{i-1}N_{i+1}.....N_k$

So, $N_i \cap N_j \subseteq N_i \cap (N_1N_2.....N_{i-1}N_{i+1}\ldots N_k) = \{e\}$

and that $N_i \cap N_j = \{e\}$. Since N_i and N_j are normal subgroups of G, by 8.3.2, we

have ab = ba for all $a \in N_i$ and $b \in N_j$. So, (α) becomes

$a_i = (a_1^{-1}b_1^{-1}).....(a_{i-1}^{-1}b_{i-1}^{-1})(a_{i+1}^{-1}b_{i+1}^{-1}).....(a_k^{-1}b^k)b_i$

$\Rightarrow a_ib_i^{-1} = (a_1^{-1}b_1)\ \ldots\ldots(a_{i-1}^{-1}b_{i-1})(a_{i+1}^{-1}b_{i+1})\ldots\ldots(a_k^{-1}b_k)$

Now $a_ib_i^{-1} \in N_i \cap (N_1N_2.....N_{i-1}N_{i+1}\ldots. N_k) = \{e\}$

$\Rightarrow a_i = b_i$, $1 \le i \le k$.

Therefore every element g in G has a unique representation of the form $g = a_1.a_2\ldots a_k$ with $a_i \in N_i$, $1 \le i \le k$.

Hence G is the internal direct product of N_1,N_2, ……, N_k.

8.3.7. Problem: Any finite abelian group is the (internal) direct product of its p-Sylow subgroups.

Solution: Let G be a finite abelian group and o(G) = n > 1.

Now n = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots\ldots, \alpha_k$ are positive integers. By Sylow's theorem-I, G has a p_i-Sylow subgroup N_i of order $p_i^{\alpha_i}$,$1 \le i \le k$.

Since G is abelian, each N_j, $1 \le j \le k$ is a normal subgroup of G. We show now that G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_k$.

Let $x \in N_1 \cap N_2$. Then $o(x) \mid o(N_1) = p_1^{\alpha_1}$ and $o(x) \mid o(N_2) = p_2^{\alpha_2}$.

So, $O(x) \mid (p_1^{\alpha_1}, p_2^{\alpha_2}) = 1$ and that $o(x) = 1$ and that $x = e$. Therefore, $N_1 \cap N_2 = \{e\}$ and $O(N_1N_2) = \frac{O(N_1)O(N_2)}{O(N_1 \cap N_2)} = \frac{p_1^{\alpha_1} p_2^{\alpha_2}}{1} = p_1^{\alpha_1} p_2^{\alpha_2} = O((N_1)O(N_2)$

Let $y \in N_3 \cap N_1N_2$.

Now $O(y) \mid O(N_3)$ and $O(y) \mid O(N_1N_2) = p_1^{\alpha_1} p_2^{\alpha_2}$

So, $O(y) \mid (p_3^{\alpha_3}, p_1^{\alpha_1} p_2^{\alpha_2}) = 1$ and that $o(y) = 1$ and that $y = e$.

Therefore $N_3 \cap N_1N_2 = \{e\}$ and

$$O(N_1N_2\,N_3) = \frac{O(N_1\,N_2)O(N_3)}{O(N_1\,N_2 \cap N_3)} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}}{1}$$

$$= O(N_1N_2).O(N_3)$$

Continuing this we get that $N_i \cap N_1N_2 \ldots\ldots N_{i-1} = \{e\}$ for $i = 2,3,\ldots,k$ and

$O(N_1, N_2, \ldots, N_k) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k} = n$.

Since $N_1N_2\ldots\ldots N_k$ is a normal subgroup of G and $O(G) = n$, we have that $G = N_1N_2\ldots N_k$.

Hence, G is an internal direct product of its p-Sylow subgroups $N_1, N_2, \ldots\ldots, N_k$.

8.4. MODEL EXAMINATION QUESTIONS:

8.4.1. If $G_1, G_2, \ldots\ldots, G_n$ are groups, Prove that the product $G = G_1 \times G_2 \times \ldots \times G_n$ is also a group under coordinate wise operation.

8.4.2. Define the notion of an internal direct product and prove that it is isomorphic to an external direct product.

8.4.3. Let $G = G_1 \times G_2 \times \ldots\ldots \times G_n$, where each G_i is a group. Then prove that there exist normal subgroups $N_1, N_2, \ldots\ldots, N_n$ of G such that G is the internal direct product of $N_1, N_2, \ldots\ldots, N_n$ and $G_i \cong N_i$ for all $1 \le i \le n$.

8.5. EXERCISES:

8.5.1. Let $G_1, G_2, \ldots\ldots, G_n$ be groups and $G = G_1 \times G_2 \times \ldots\ldots \times G_n$. Then prove that there are normal subgroups $N_1, N_2, \ldots\ldots, N_n$ of G such that $G/N_i \cong G_i$ for all $1 \le i \le n$.

8.5.2. For any groups G_1, G_2, G_3,

Prove that $G_1 \times G_2 \cong G_2 \times G_1$ and $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

8.5.3. Let G be a group and let T = G x G. Let D = {(g, g) $\in$ G x G | g $\in$ G}. Then prove that D is a subgroup of T and D $\cong$ G. Also, prove that D is normal in G if and only if G is abelian.

8.6 SUMMARY:

In this lesson, we have learnt the concepts of an external direct product and an internal direct product and proved that these two are same, upto isomorphism.

8.7 TECHNICAL TERMS:

- External direct product
- Normal subgroup
- Internal direct product
- Isomorphism

8.8 ANSWERS TO SELF ASSESSMENT QUESTIONS:

8.2.4. n is the smallest positive integer such that $a^n = e$ and similarly m for b.

Let k = l.c.m of {n,m}. We prove that k is the smallest positive integer such that $(a, b)^k = (e, e)$, the identity element in A x B. Since n $\mid$ k and m $\mid$ k, we have that k = ns and k = mt for some positive integer s and t.

Now $(a, b)^k = (a^k, b^k) = (a^{ns}, b^{mt})$

$= ((a^n)^s, (b^m)^t)$

$= (e^s, e^t)$

$= (e, e)$

Also, for any positive integer u,

$(a,b)^u = (e,e) \Rightarrow (a^u, b^u) = (e, e)$

$\Rightarrow a^u = e$ and $b^u = e$

$\Rightarrow o(a) \mid u$ and $o(b) \mid u$

$\Rightarrow n \mid u$ and $m \mid u$

$\Rightarrow k \mid u$

$\Rightarrow k \leq u$

Therefore, k is the smallest positive integer such that $(a,b)^k = (e,e)$ and hence O(a, b) = l.c.m {O(a), O(b)}

8.9 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. K. SIVA PRASAD

LESSON -9

FINITE ABELIAN GROUPS

OBJECTIVES:

The objectives of this lesson are to

- prove that any finite abelian group is a direct product of cyclic groups.
- define the notion of invariants of a finite abelian group and prove that any two abelian groups of order p^n are isomorphic if and only if they have the same invariants.
- derive a formula for the number of non-isomorphic abelian groups of given order.

STRUCTURE:

9.1. INTRODUCTION:

In this lesson, we pay special attention to finite abelian groups. The reason is that no other general class of groups has the structure as completely known as easily described. When one is setting up a structure theory, the overall strategy is to express the complicated algebraic systems in terms of those better behaved we accomplish this in the present lesson by proving that any finite abelian group is a direct product of cyclic groups. We also derive at a formula to know the number of (non-isomorphic) abelian groups of a given order.

9.2: FUNDAMENTAL THEOREM ON FINITE ABELIAN GROUPS:

It is well known that any cyclic group is abelian and that any finite cyclic group must be isomorphic to the additive group Z_n of integers modulo n, where n is the order of the group. In this section we prove that any finite abelian group must be a direct product of finite cyclic groups. That is, in a sense, the finite cyclic groups(or Z_n's) are like building blocks in the theory of finite abelian groups.

9.2.1: THEOREM (FUNDAMENTAL THEOREM ON FINITE ABELIAN GROUPS):

Every finite abelian group is the direct product of cyclic groups.

Proof: Since any finite abelian group is the direct product of its p-Sylow subgroups (by 8.3.7), it is enough to prove that any abelian group of order p^n, where p is a prime number and n is a positive integer, is a direct product of cyclic groups. Let G be a finite abelian group of order p^n, where p is a prime and n is a positive integer. Since $o(G) = p^n$, we know that the order of every element of G must be a power of p. We get an element $a_1 \epsilon G$ of largest order among the elements of G and $O(a_1) = p^k$ $(k \leq n)$. Consider the cyclic subgroup

$A_1 = (a_1) = \{e, a_1, a_1^2 \ldots\ldots, a_1^{p^{k-1}}\}$ of G.

If k = n, then A_1 = G, so that G itself is cyclic in which case the theorem is trivial. Suppose that k < n. Then A_1 is a proper nontrivial subgroup of G. Now, consider the quotient group G/ A_1. As G is abelian, G/A_1 is an abelian group and $O(G/A_1) = \frac{O(G)}{O(A_1)} = \frac{p^n}{p^k} = p^{n-k}$.

We get an element $A_1b_2 \in G/A_1$ of largest order among the elements of G/A_1 and $O(A_1b_2) = p^{n_2}$.

We have that p^{n_2} is the least positive integer such that $(A_1b_2)^{p^{n_2}} = A_1$.

That is, $A_1 b_2^{p^{n_2}} = A_1$, This implies that $b_2^{p^{n_2}} \in A_1$.

Suppose that $(b_2) \cap A_1 \neq \{e\}$.

Now $b_2^{p^{n_2}} = a_1^i$ for some positive integer $1 \leq i \leq p^{n_1}$ ($\because b_2^{p^{n_2}} \in A_1 = (a_1)$)

Since $O(a_1)$ is largest, $O(b_2) = p^{n_1}$, $O(a_1) = p^{n_1}$. Also $O(b_2) \mid O(G) = p^n$ implies $O(a_2)$ is a power of p.

So, $b_2^{p^{n_1}} = e \in A_1$. Therefore, $(A_1b_2)^{p^{n_1}} = A_1 b_2^{p^{n_1}} = A_1 e = A_1$, so that $p^{n_2} \mid p^{n_1}$ and that $n_1 \geq n_2$.

Now $(a_1^i)^{p^{n_1-n_2}} = (b_2^{p^{n_2}})^{p^{n_1-n_2}} = b_2^{p^{n_1}} = e$ and hence $p^{n_1} \mid ip^{n_1-n_2}$ and that i = j p^{n_2} for some integer j.

Put $a_2 = a_1^{-j} b_2$. Then $a_2 \in A_1b_2$ and hence $A_1a_2 = A_1b_2$

Also, $a_2^{p^{n_2}} = (a_1^{-j}b_2)^{p^{n_2}} = a_1^{-jp^{n_2}} . b_2^{p^{n_2}}$

$= a_1^{-i} b_2^{p^{n_2}}$

$= a_1^{-i} a_1^i = e$.

Therefore, $a_2^{p^{n_2}} = e$ and hence $o(a_2) \mid p^{n_2}$.

Let t be a positive integer and $a_2^t = e$.

Now $e = a_2^t = (a_1^{-j}b_2)^t = a_1^{-jt} b_2^t$.

So, $b_2^t = a_1^{jt} \in A_1$. Since p^{n_2} is the least positive integer with $b_2^{p^{n_2}} \in A_1$, we have that $p^{n_2} \leq t$, so that $O(a_2) = p^{n_2}$.

Put $A_2 = (a_2)$. Let $x \in A_1 \cap A_2$.

Then $x \in A_1 = (a_1)$ and $x \in A_2 = (a_2)$.

Now $x = a_2^l$ for some integer l and that

$X = a_2^l = (a_1^{-j}b_2)^l = a_1^{-jl} b_2^l \in A_1 \cap A_2$, and hence $b_2^l = x a_1^{jl} \in A_1$;that is $A_1 b_2^l = A_1$;

that is, $(A_1b_2)^l = A_1$. Therefore, $p^{n_2} \mid l$, and so $x = a_2^l = e$.

Hence, $A_1 \cap A_2 = \{e\}$.

If G = A_1 A_2, then G is the internal direct product of A_1 and A_2.

Suppose that G ≠ A_1A_2. Now, consider the quotient group G/A_1A_2. Let A_1 A_2b_3 be an element of largest order in G/A_1A_2 and O($A_1A_2b_3$) = p^{n_3}.

Now $b_3^{p^{n_2}}$ = e ∈ A_1A_2; that is $(A_1A_2b_3)^{p^{n_2}} = A_1A_2b_3^{p^{n_2}}$ = A_1A_2.

Therefore $p^{n_3} | p^{n_2}$ and so $n_3 \leq n_2$.

If $A_1A_2 \cap (b_3)$ ={e}, we get the result .

Suppose that $A_1A_2 \cap (b_3) \neq$ {e}.

We have $b_3^{p^{n_3}} \in A_1A_2$ (since O($A_1A_2b_3$) = p^{n_3})

So, $b_3^{p^{n_3}} = a_1^{i_1}a_2^{i_2}$, for some integer i_1 & i_2.

Consider $(a_1^{i_1}a_2^{i_2})^{p^{n_2-n_3}} = (b_3^{p^{n_3}})^{p^{n_2-n_3}} = b_3^{p^{n_2}} \in A_1$.

$\Longrightarrow a_1^{i_1 p^{n_2-n_3}} . a_2^{i_2 p^{n_2-n_3}} = b_3^{p^{n_2}} \in A_1$.

$\Longrightarrow a_2^{i_2 p^{n_2-n_3}} \in A_1$.

Since O(A_1A_2) = p^{n_2}, we have $p^{n_2} | i_2 . p^{n_2-n_3}$, and so $i_2 = j_2 p^{n_3}$, for some integer j_2.

Also, $(a_1^{i_1}a_2^{i_2})^{p^{n_1-n_3}} = (b_3^{p^{n_3}})^{p^{n_1-n_3}}$

$= b_3^{p^{n_1}} = e.$

This is to say that $a_1^{i_1 p^{n_1-n_3}} = a_2^{-i_2 p^{n_1-n_3}} \in A_1 \cap A_2$ ={e}

That is, $a_1^{i_1 p^{n_1-n_3}} = e$. As O($A_1$)= p^{n_1}, $p^{n_1} | i_1 p^{n_1-n_3}$

This yields that $p^{n_3} | i_1$. This implies that, $i_1 = j_1 p^{n_3}$ for some integer j_1. Let $a_3 = a_1^{-j_1} . a_2^{-j_2} . b_3$.

Then $a_3^{p^{n_3}} = (a_1^{-j_1} . a_2^{-j_2} . b_3)^{p^{n_3}}$

$= a_1^{-j_1 p^{n_3}} . a_2^{-j_2 p^{n_3}} . b_3^{p^{n_3}}$

$= a_1^{-i_1} a_2^{-i_2} b_3^{p^{n_3}}$

$= e$ (since $b_3^{p^{n_3}} = a_1^{i_1}a_2^{i_2}$)

Let 's' be a positive integer such that a_3^s=e.

Now e = $a_3^s = (a_1^{-j_1} . a_2^{-j_2} . b_3)^s = a_1^{-j_1 s} . a_2^{-j_2 s} . b_3^s$.

So, $b_3^s = a_1^{j_1 s} . a_2^{j_2 s} \in A_1A_2$ and that

$A_1A_2 . b_3^s = A_1A_2$ and that $(A_1A_2 . b_3)^s = A_1A_2$

Since O($A_1A_2b_3$) = p^{n_3}, $p^{n_3} | t$ so that $t \geq p^{n_3}$

Therefore, O(a_3) = p^{n_3}. Put $A_3 = (a_3)$

Let y ∈ $A_3 \cap A_1A_2$. Then $y = a_3^{l_3} = a_1^{l_1}a_2^{l_2}$ for some integers l_1, l_2 and l_3

Since $a_3 = a_1^{-j_1}, a_2^{-j_2}.b_3$, we have that $(a_1^{-j_1}.a_2^{-j_2}.b_3)^{l_3} = a_3^{l_3} = a_1^{l_1}a_2^{l_2}$

This is to say that $b_3^{l_3} \in A_1A_2$ and that

$A_1A_2b_3^{l_3} = A_1A_2$ and that $(A_1A_2b_3)^{l_3} = A_1A_2$

So, $p^{n_3} | l_3$ (since $O(A_1A_2b_3 = p^{n_3})$; that is, $l_3 = kp^{n_3}$ for some integer k.

Therefore, $y = a_3^{l_3} = a_3^{kp^{n_3}}$

$= (a_3^{p^{n_3}})^k$

$= e^k$

$= e.$

Hence, $A_3 \cap A_1A_2 = \{e\}$.

If $G = A_1A_2A_3$, we get the result. Otherwise, we continue the process and we get that $G = A_1A_2A_3.....A_k$, where $A_i = (a_i)$, $1 \leq i \leq k$, and $A_i \cap A_1A_2.....A_{i-1} = \{e\}$ for i = 2,3……,k.

Thus, G is the internal direct product of cyclic groups $A_1, A_2, \ldots, A_k$.

9.2.2. Self Assessment Question: Give an example of a non-cyclic abelian group of order p^n, where p is a given prime and n > 1.

9.3. INVARIANTS:

With any abelian group of order p^n, we shall associate a finite sequence of positive integers whose sum is n and these integers are called the invariants of the group .This help us in getting a formula for the number of distinct (non-isomorphic) abelian groups of order p^n, where p is a given prime and n is a positive integer.

9.3.1. Definition: Let G be an abelian group of order p^n, where p is a prime and n is a positive integer. Suppose that $G = A_1A_2\ldots\ldots A_K$, the internal direct product of cyclic subgroups A_i, $1 \leq i \leq k$, and $O(A_i) = p^{n_i}$, $1 \leq i \leq k$ with $n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$. Then the integers $n_1, n_2, \ldots, n_k$ are called the invariants of G.

Note that the subgroups $A_1, A_2, \ldots, A_k$ and their generators in the definition (9.3.1) of invariants are not unique. For, consider the following.

9.3.2. Example: Let G= {e,a,b,ab} with $a^2 = e = b^2$ and ab = ba. Then G is an abelian group of order 2^2. Let A={e, a}, B= {e, b} and c={e, ab}. Then A, B and C are three distinct cyclic subgroups of G, and G = AB, G = AC and G = BC are three different decompositions of G into products of cyclic subgroups though the invariants obtained are same.

9.3.3. Self Assessment Questions: What are the invariants of the group G given in 9.32.

9.3.4. Definition: Let G be an abelian group and s be an integer.
Then $G(s) = \{g \in G / g^s = e\}$
Note that G(s) is a subgroup of G.

9.3.5. Lemma: Let G, G^1 be isomorphic abelian groups and s be an integer. Then G(s) and $G^1(s)$ are also isomorphic.

Proof: Let ϕ be an isomorphism of G onto G^1.

We shall prove that ϕ maps G(s) isomorphically onto $G^1(s)$.

First we prove that $\phi(G(s)) = G^1(s)$

Let $x \in G(s)$.Then we have $x^s = e$, and hence $(\phi(x))^s = \phi(x^s) = \phi(e) = e^1$, the identity in G^1.

So, $\phi(x) \in G^1(s)$. Therefore, $\phi(G(s)) \subseteq G^1(s)$.

Let $u \in G^1(s)$. Then $u^s = e^1$. But, since ϕ is onto, $u = \phi(y)$ for some $y \in G$.

Therefore, $e^1 = u^s = (\phi(y))^s = \phi(y^s)$. Because ϕ is one-to-one, we have $y^s = e$ and so $y \in G(s)$ and hence $u = \phi(y) \in \phi(G(s))$. Therefore, $G^1(s) \subseteq \phi(G(s))$ and hence $\phi(G(s)) = G^1(s)$. Thus ϕ maps G(s) onto $G^1(s)$. Therefore since ϕ is one to one, onto and a homomorphism from G(s) to $G^1(s)$, we have that G(s) and $G^1(s)$ are isomorphic.

9.3.6. Lemma: Let G be an abelian group of order p^n, where p is a prime and n is a positive integer. Suppose that $G = A_1A_2.....A_K$, an internal direct product, where each $A_i = (a_i)$ is cyclic of order p^{n_i}, $1 \le i \le k$ and $n_1 \ge n_2 \ge \ldots \ge n_k > 0$. If m is an integer such that $n_t > m \ge n_{t+1}$, then $G(p^m) = B_1B_2\ldots B_tA_{t+1}.A_{t+2}\ldots\ldots A_k$, where $B_i = (a_i^{p^{n_i - m}})$ and $O(B_i) = p^m$, for $i \le t$. The order of G (p^m) is p^u, where $u = mt + \sum_{i=l+1}^{*} n_i$.

Proof: We have that $G = A_1A_2\ldots\ldots A_k$, an internal direct product, where each $A_i = (a_i)$ is a cyclic subgroup of order p^{n_i}, $1 \le i \le k$ and $n_1 \ge n_2 \ge \ldots \ge n_k > 0$.

Consider $G(p^m) = \{ x \in G / x^{p^m} = e \}$ where $n_i > m \ge n_{t+1}$. It is clear that $x^{p^m} = e$ for all $x \in A_j$, $t+1 \le j \le k$ as $m \ge n_{t+1}$ (since $x \in (a_j)$ implies $x = a_j^l$ for some $0 \le l \le p^{n_j}$ and $a_j^{p^{n_i}} = e$).

So, $A_j \subseteq G(p^m)$ for all $t+1 \le j \le k$.

For $1 \le j \le t$, $(a_j^{p^{n_i - m}})^{p^m} = a_i^{p^{n_i}} = e$ and

$$(a_j^{p^{n_i - m}}) = p^m$$

So, $B_i = (a_j^{p^{n_i - m}}) \subseteq G(p^m)$ and $o(B_i) = p^m$ for all $1 \le i \le t$.

Since $B_1, B_2, \ldots\ldots, B_t, A_{t+1}, A_{t+2}, \ldots\ldots, A_k$ are all contained in $G(p^m)$, their product is also contained in $G(p^m)$…….(i)

Let $x \in G(p^m)$. Then $x^{p^m} = e$ and $x = a_1^{l_1} a_2^{l_2} \ldots\ldots a_k^{l_k}$ for some integers $0 < l_i < p^{n_i}$, $i = 1,2,\ldots..,k$.

So, $e = x^{p^m} = (a_1^{l_1})^{p^m}(a_2^{l_2})^{p^m}\ldots\ldots.(a_k^{l_k})^{p^m}$ and $(a_i^{l_i})^{p^m} \in A_i$, $1 \le i \le k$.

Since the product G = $A_1 A_2 \ldots A_k$ is direct, $(a_i^{l_i})^{p^m} = e$ for all $1 \le i \le k$ and so $p^{n_i} \mid l_i p^m$ for all $1 \le i \le k$. For $1 \le i \le k$, $l_i = p^{n_i - m}. s_i$ for some integer s_i. So, $a_i^{l_i} = (a_i^{p^{n_i-m}})^{s_i} \in B_i$ for all $1 \le i \le t$.

As $x = a_1^{l_1} a_2^{l_2} \ldots a_t^{l_t} a_{t+1}^{l_{t+1}} \ldots a_k^{l_k}$, we see that $x = a_1^{s_1 p^{n_i - m}} \ldots a_t^{l_{t+1}} \ldots a_{t+1}^{l_{t+1}} \ldots a_k^{l_k}$

This is to say that $x \in B_1 B_2 \ldots B_t A_{t+1} . A_{t+2} \ldots \ldots A_k$

Therefore, $G(p^m) \subseteq B_1 B_2 \ldots B_t A_{t+1} . A_{t+2} \ldots \ldots A_k \ldots \ldots$ (ii)

From (i) and (ii), we get $G(p^m) = B_1 B_2 \ldots B_t A_{t+1} . A_{t+2} \ldots \ldots A_k$.

Now $O(G(p^m)) = O(B_1) . O(B_2) \ldots O(B_t) O(A_{t+1}) O(A_{t+2}) \ldots \ldots O(A_k)$

$= p^m . p^m \ldots . p^m . p^{n_{t+1}} p^{n_{t+2}} \ldots p^{n_k}$

$(t - \text{times})$

$= p^{mt} . p^{\sum_{i=t+1}^{k} n_i}$

Thus $O(G(p^m)) = p^u$, where $u = mt + \sum_{i=t+1}^{k} n_i$

9.3.7. Corollary: Let G be an abelian group of order p^n, where p is a prime and n is a positive integer. Suppose that $G = A_1 A_2 \ldots \ldots \ldots A_k$, an internal direct product, where each $A_i = (a_i)$ is cyclic of order p^{n_i}, $1 \le i \le k$ and $n_1 \ge n_2 \ge \ldots \ldots \ge n_k > 0$. Then $O(G(p)) = p^k$.

Proof: By applying the lemma 9.3.6 to the case m =1,

we have t = k and o (G(p)) = p^k (since u = 1k=k).

9.3.8. Theorem: Let p be a prime and n be a positive integer. Then any two abelian groups of order p^n are isomorphic if and only if they have the same invariants.

Proof: Let G and G^1 be two abelian groups and $O(G) = O(G^1) = p^n$.

Suppose that G and G^1 are isomorphic. Let $n_1, n_2, \ldots \ldots, n_k$ be the invariants of G and let $m_1, m_2, \ldots \ldots, m_l$ be the invariants of G^1. Then $G = A_1 A_2 \ldots \ldots A_k$, an internal direct product, where $A_i = (a_i)$ is a cyclic subgroup of order p^{n_i} in G, $1 \le i \le k$ and $n_1 \ge n_2 \ge \ldots \ldots \ge n_k > 0$ and $G^1 = B_1 B_2 \ldots \ldots B_l$, an internal direct product, where $B_j = (b_j)$ is a cyclic subgroup of order p^{m_j} in G^1, $1 \le j \le l$, $m_1 \ge m_2 \ge \ldots \ge m_l > 0$.

Since G and G^1 are isomorphic, by lemma 9.3.5, G(p) and $G^1(p)$ are also isomorphic.

So, $O(G(p)) = O(G^1(p))$. According to the corollary 9.3.7, $O(G(p)) = p^l$ and $O(G^1(P)) = p^l$.

Hence $p^k = p^l$ and so $k = l$. Thus the number of invariants for G and G^1 is the same.

We shall show that $n_j=m_j$ for all $1\leq j \leq k$. Suppose $n_i\neq m_i$ for some $1\leq i\leq k$.

Let 't' be the smallest integer such that $1\leq t \leq k$ and $n_t > m_t$. Then $n_1 = m_1$, $n_2 = m_2$,…, $n_{t-1} = m_{t-1}$,$n_t > m_t$.

Let $m = m_t$. Put $H = \{g^{p^m} / g \in G\}$ and $H^1 = \{y^{p^m} / y \in G^1\}$. Clearly, H and H^1 are subgroups of G and G^1, respectively.

Let $T: G\rightarrow G^1$ be an isomorphism of G onto G^1.

Now $T(H) = H^1$. So, H is isomorphic to H^1

Because $G = (a_1)(a_2)\ldots..(a_k)$, we get that

$H = (a_1^{p^m})(a_2^{p^m})\ldots..(a_t^{p^m})\ldots..(a_s^{p^m})$ where $n_s > m \geq n_{s-1}$.

Because $G = (b_1)(b_2)\ldots.(b_l)$,we get that

$$H^1 = (b_1^{p^m})(b_2^{p^m})\ldots..(b_{t-1}^{p^m})$$

So, the number of invariants of H is $s\geq t$ and the number of invariants of H^1 is $t-1$

As H and H^1 are isomorphic, we have that $s = t-1$ and that $t-1\geq t$, which is a contradiction.

Therefore, $n_i = m_i$ for all $1\leq i\leq k$.

Hence, G and G^1 have the same invariants. Conversely, suppose that G and G^1 have the same invariants $n_1, n_2, \ldots\ldots\ldots, n_k$. Then $G = A_1A_2\ldots..A_k$, an internal direct product and $G^1=B_1 B_2\ldots..B_k$, an internal direct product where $A_i = (a_i)$ and $B_i = (b_i)$ are cyclic subgroups of order p^{ni} in G and G^1, respectively and $n_1 \geq n_2 \geq\ldots\ldots\ldots\geq n_k > 0$. We shall prove that G and G^1 are isomorphic.

Define $T: G\rightarrow G^1$ by $T(a_1^{s_1}a_2^{s_2} \ldots\ldots a_k^{s_k})$

$= b_1^{s_1}b_2^{s_2} \ldots\ldots b_k^{s_k}$ for all $a_1^{s_1}a_2^{s_2} \ldots\ldots a_k^{s_k} \in G$

Since each element $g\in G$ can be expressed uniquely as $g= a_1^{l_1}a_2^{l_2} \ldots\ldots a_k^{l_k}$ with $a_i^{l_i} \in A_i$, $1\leq i\leq k$, it follows that T is well defined.

Let $a_i^{s_i}, a_i^{l_i} \in A_i$, $1\leq i\leq k$.

Now $T((a_1^{s_1}a_2^{s_2} \ldots\ldots a_k^{s_k})(a_1^{l_1}a_2^{l_2} \ldots\ldots a_k^{l_k}))$

$= T(a_1^{s_1+l_1}.a_2^{s_2+l_2} \ldots\ldots a_k^{s_k+l_k})$

$= b_1^{s_1+l_1}.b_2^{s_2+l_2} \ldots\ldots b_k^{s_k+l_k}$

$= (b_1^{s_1}b_2^{s_2} \ldots\ldots b_k^{s_k})(b_1^{l_1}b_2^{l_2} \ldots\ldots b_k^{l_k})$

= T($a_1^{s_1}a_2^{s_2}$ ... ... $a_k^{s_k}$) . T($a_1^{l_1}a_2^{l_2}$ ... ... $a_k^{l_k}$)

Therefore, T is homomorphism.

Suppose that T($a_1^{s_1}a_2^{s_2}$ ... ... $a_k^{s_k}$) = T($a_1^{l_1}a_2^{l_2}$ ... ... $a_k^{l_k}$).

Then $b_1^{s_1}b_2^{s_2}$ ... ... $b_k^{s_k}$ = $b_1^{l_1}b_2^{l_2}$ ... ... $b_k^{l_k}$

Since G^1 is the internal direct product of B_1 B_2 .....B_k, we have $b_i^{l_i} = b_i^{s_i}$, for all 1≤i≤*k*. Now $b_i^{s_i-l_i}$ = e for all 1≤i≤*k*. So, $p^{n_i}|s_i - l_i$ for all 1≤i≤*k*.

As O(a_i) = p^{n_i}, $a_i^{s_i-l_i}$ = e ; That is, $a_i^{s_i} = a_i^{l_i}$ for all 1≤i≤*k*.

So, $a_1^{s_1}a_2^{s_2}$ ... ... $a_k^{s_k}$ = $a_1^{l_1}a_2^{l_2}$ ... ... $a_k^{l_k}$

Therefore, T is one -one

Since T is one-one and O(G) = O(G^1) = p^n, T is onto. Hence, G and G^1 are isomorphic.

9.3.9. Self Assessment Question: For any positive integer m, prove that any two cyclic groups of order m are isomorphic.

9.4. ABELIAN GROUPS OF A GIVEN ORDER:

In this section, we derive a formula for the number of non-isomorphic finite abelian groups of a given order.

Let us recall the following: For any positive integer n, by a partition of n we mean a sequence of positive integers n_1, n_2, ..., n_k such that $n_1 \geq n_2 \geq \ldots \geq n_k$ and $n_1+n_2+\ldots+n_k = n$. The set of all partitions of n is denoted by p(n).

9.4.1. Theorem: For any positive integer n, the number of non-isomorphic abelian groups of order p^n is equal to the number of partitions of n, where p is a given prime.

Proof. Let n be a positive integer and p be a prime number. Let $\{n_1,n_2,.....,n_k\}$ be a partition of n. Then $n = n_1+n_2+\ldots+n_k$ and $n_1 \geq n_2 \geq .....\geq n_k > 0$.

Now $Z_{p^{n_1}} \times Z_{p^{n_2}} \times \ldots\ldots \times Z_{p^{n_k}}$ is an abelain group of order

$p^{n_1}.\, p^{n_2}.....p^{n_k} = p^{n_1+n_2+\ldots\ldots+n_k} = p^n$.

In this way we get p(n) number of abelian groups of order p^n, where p(n) is the number of partitions of n. According to theorem 9.3.8, these are all non-isomorphic abelian groups of order p^n. If G is an abelian group of order p^n, then its invariants $m_1 \geq m_2 \geq .....\geq m_t > 0$ (say) also a partition of n and this group is isomorphic to one of the p(n) abelian groups, which corresponds to the partition $\{m_1,m_2,\ldots,m_t\}$ of n. Thus there are exactly p(n) number of non isomorphic abelian groups of order p^n.

9.4.2. Self Assessment Question: How many non-isomorphic abelian groups of order 81 are there? List all these.

9.4.3. Corollary: Let $p_1, p_2, \ldots, p_t$ be distinct primes and $n_1, n_2, \ldots, n_t$ be positive integers. Then the number of non-isomorphic abelian groups of order $p_1^{n_1}.p_2^{n_1}\ldots.p_t^{n_t}$ is equal to the product $p(n_1).p(n_2)\ldots.p(n_t)$, where $p(n_i)$ is the number of partitions of n_i.

Proof. Let G be an abelian group of order $p_1^{n_1}.p_2^{n_1}\ldots.p_t^{n_t}$. Since G is abelian, G has unique p_i-Sylow subgroup p_i of order $p_i^{n_i}$, $1\le i\le t$. Moreover $G = p_1.p_2.\ldots.p_t$, an internal direct product of its normal subgroups $p_1, p_2, \ldots, p_t$. (see 8.3.7).

Also, we have that if G_1 and G_2 are abelian groups of same order and $G_1=H_1\ H_2\ \ldots.H_k$, an internal direct product of its Sylow subgroups. $H_1, H_2, .., H_t$ and $G_2 = T_1\ .T_2\ \ldots\ldots.T_k$, an internal direct product of its Sylow subgroups $T_1, T_2, \ldots, T_k$ are isomorphic if and only if $H_i \cong T_i$ for all $1\le i\le t$, that is, the corresponding Sylow subgroups are isomorphic. Therefore, as there are $p(n_i)$ number of non-isomorphic abelian groups of order p_i , $1\le i\le t$, we get that the number of non isomorphic abelian groups of order $p_1^{n_1}.p_2^{n_1}\ldots.p_t^{n_t}$ is $p(n_1).p(n_2)\ldots p(n_t)$.

9.4.4. Self Assessment Question: How many non-isomorphic abelian groups of order 600 are there and make a list of all these.

9.4.5. Describe all the non-isomorphic abelian groups of order 1936.

9.5. MODEL EXAMINATION QUESTIONS:

9.5.1. State and prove the Fundamental theorem on finite abelian groups.

9.5.2. For any prime p, prove that two abelian groups order p^n are isomorphic if and only if they have the same invariants.

9.5.3. For any prime p and any positive integer n, prove that the number of non-isomorphic abelian groups of order p^n is equal to the number of partitions of n.

9.5.4. State and derive a formula for the number of non-isomorphic finite abelian groups of a given order.

9.6. EXERCISE:

9.6.1. Describe all finite abelian groups of order
a) 2^6 b) 11^6 c) 7^5 d)$2^4.3^4$

9.6.2. If G is an abelian group of order p^n, p a prime and $n_1\ge n_2\ge\ldots.\ge n_k > 0$ are the invariants of G, show that the maximal order of any element in G is p^{n_1}.

9.6.3. If a finite abelian group G has subgroups of orders m and n, prove that G has a subgroup whose order is the least common multiple of m and n.

9.6.4. Let G be an abelian group of order p^n with invariants $n_1\ge n_2\ge\ldots.\ge n_k > 0$ and $H \ne \{e\}$ be a subgroup of G. If $h_1\ge h_2\ge\ldots.\ge h_s > 0$ are the invariants of H, then show that $k \ge s$ and $h_i \le n_i$ for i=1,2,…,s.

9.6.5. Let G be a finite abelian group p^n and $\hat{G}$ ibe the set of all homomorphisms of G into the group of nonzero complex numbers under multiplication. Prove that $\hat{G}$ is an abelian group under the operation defined by $(\phi_1.\phi_2)(g) = \phi_1(g)\,\phi_2(g)$ for all $\phi_1, \phi_2 \in \hat{G}$ and $g\in G$.

9.6.6. For any $\phi \in \hat{G}$ and g∈G, show that ϕ(g) is a root of unity, if G is a finite abelian group.

9.6.7. If G is a finite cyclic group, show that $\hat{G}$ is also a cyclic group and O($\hat{G}$) = O(G). Hence G and $\hat{G}$ are isomorphic.

9.6.8. If G is a finite abelian group and x≠y ∈ G, prove that there is a $\phi \in \hat{G}$ with $\phi(x) \neq \phi(y)$.

9.6.9. If G is a finite abelian group and $1 \neq \phi \in \hat{G}$, show that $\sum_{g \in G} \phi(g) = 0$.

9.7 SUMMARY:

In this lesson, you have learnt the fundamental theorem on finite abelian groups which states that any finite abelian group is a product of cyclic groups. We have introduced the notion of invariants of an abelian group of order p^n, where p is a prime, and proved that two such groups are isomorphic if and only if they have the same invariants. Also, we have proved that the number of non-isomorphic abelian groups of order p^n is equal to the number of partitions of n, and using this we have derived a formula for the number of non-isomorphic abelian groups of a given order.

9.8 TECHNICAL TERMS:

- Abelian group
- Fundamental theorem
- Cyclic group
- Invariants
- Partition

9.9 ANSWERS TO SELF ASSESSMENT QUESTIONS:

9.2.2. Consider $Z_p \times Z_p \times \ldots\ldots\ldots \times Z_p$ (*n times*)**.** This is an abelian group of order p.p….p (n-times) = p^n and is non-cyclic, since any element, except the identity, is of order p.

9.3.3. O(G) = 4 = 2^2, O(A) = 2, O(B) = 2 and G = AB, an internal direct product of cyclic subgroups A and B. So, the invariants of G are 1, 1, ...

9.3.9. Let G be a cyclic group of order m. Then G = (a) for some a∈ G, whose order is m, and G = {e, a, a^2,....., a^{m-1}}. It is easy to verify that i $\longmapsto$ a^i is an isomorphism of Z_n onto G. Therefore $G \cong Z$. If H is another cyclic group of order m, then $G \cong Z_m \cong H$ and hence $G \cong H$.

9.4.2: 81 is of the form p^n where p =3 is a prime and n =4 is a positive integer. By theorem 9.4.1, the number of non-isomorphic abelian groups of order 3^4 is equal to the number of partitions of 4. But the number of partitions of 4 is 5. The partitions of 4 and the corresponding groups of order 3^4 are given below.

{1,1,1,1}	$Z_3 \times Z_3 \times Z_3 \times Z_3$
{1,1,2}	$Z_3 \times Z_3 \times Z_{3^2}$
{1,3}	$Z_3 \times Z_{3^3}$
{2,2}	$Z_{3^2} \times Z_{3^2}$

{4} Z_{3^4}, which is cyclic of order $3^4=81$

9.4.4: Observe that $600 = 2^3 .5^2 .3^1$. Now p (3) = 3 and p(2) = 2. So, by theorem 9.4.3, the number of non-isomorphic abelian groups of order 600 is p(3).p(2).p(1) = 3.2.1 = 6. To list all these six groups, we have to determine groups of orders 2^3, 5^2 and 3^1 and take products as below:

Partitions of 3 **Groups of order 2^3**

{1,1,1} $Z_2\times Z_2\times Z_2$

{1,2} $Z_2\times Z_{2^2}$

{3} Z_{2^3}

The partitions of 2 are {1, 1} and {2} and hence $Z_5\times Z_5$ and Z_{5^2} are the only groups of order 5^2. Now, we can list all the abelian groups of order $2^3.5^2.3^1(=600)$

$Z_2\times Z_2\times Z_2\times Z_5\times Z_5\times Z_3(\cong Z_2\times Z_{100}\times Z_3\cong Z_6\times Z_{10}\times Z_{10})$

$Z_2\times Z_2\times Z_2\times Z_{5^2} Z_3(\cong Z_6\times Z_2\times Z_{50})$

$Z_2\times Z_{2^2}\times Z_5\times Z_5\times Z_3(\cong Z_{10}\times Z_{20}\times Z_3\cong Z_{30}\times Z_{20})$

$Z_2\times Z_{2^2}\times Z_{5^2}\times Z_3(\cong Z_{50}\times Z_{12}\cong Z_4\times Z_{150})$

$Z_{2^3}\times Z_5\times Z_5\times Z_3$ $(\cong Z_{40}\times Z_{15}\cong Z_{24}\times Z_5\times Z_5)$

$Z_{2^3}\times Z_{5^2}\times Z_3(\cong Z_{24}\times Z_{25}\cong Z_8\times Z_{75})$

9.4.5. We have $1936 = 2^4.11^2$. Now p(4) = 5 and p(2) =2. The numberof non-isomorphic abelian groups of order 1936 is p(4).p(2) = 5.2 =10.

Partition of 4	**Partition of 2**	**Groups of order $2^4.11^2$**
{1,1,1,1}	{1,1}	$Z_2\times Z_2\times Z_2\times Z_2\times Z_{11}\times Z_{11}$
{1,1,1,1}	{2}	$Z_2\times Z_2\times Z_2\times Z_2\times Z_{121}$
{1,1,2}	{1,1}	$Z_2\times Z_2\times Z_{2^2}\times Z_{11}\times Z_{11}$
{1,1,2}	{2}	$Z_2\times Z_2\times Z_{2^2}\times Z_{11^2}$
{1,3}	{1,1}	$Z_2\times Z_{2^3}\times Z_{11}\times Z_{11}$
{1,3}	{2}	$Z_2\times Z_{2^3}\times Z_{11^2}$
{2,2}	{1,1}	$Z_{2^2}\times Z_{2^2}\times Z_{11}\times Z_{11}$
{2,2}	{2}	$Z_{2^2}\times Z_{2^2}\times Z_{11^2}$
{4}	{1,1}	$Z_{2^4}\times Z_{11}\times Z_{11}$

{4} {2} $Z_{2^4} \times Z_{11^2}$

9.10 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. K. SIVA PRASAD

LESSON -10

DEFINITIONS, EXAMPLES AND SOME SIMPLE REUSLTS OF RING THEORY

OBJECTIVES:

The objectives of this lesson are to

- Introduce the concepts like ring, commutative ring, field, division ring.
- Discuss some examples of rings.
- Prove some fundamental results related to the known concepts.
- Understand the relation between the concepts field and integral domain.

STRUCTURE:

10.1. INTRODUCTION:

Ring is a fundamental abstract concept in the study of algebra. A group is equipped with only one binary operation where as a ring is equipped with two binary operations connected by some inter relations. We shall give an axiomatic definition of ring and study some of its elementary properties.

Despite the differences, the analysis of rings will follow the pattern already laid out for groups. Study of rings serves as one of the fundamental building blocks for the abstract algebra.

It is clear that the definition of a ring is an abstraction of the ring of integers. Although rings are a direct generalization of the integers, certain arithmetic facts to which we have become accustomed in the ring of integers need not hold in general rings. For instance, we know that the product of two non-zero integers is non-zero, but this may no longer be true in a general ring. In the ring of 2 x 2 matrices, we will come across the situation that $\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$. Thus even though both $\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$ and $\begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$ are non zero, their product is zero in the ring of 2 x 2 matrices. This leads to the study ofsome special class of rings. Integral domains, division rings and fields. Also westate the pigeon hole principle which is useful in proving the theorem that statesthat ‘a finite integral domain is a field’.

10.2. SOME DEFINITIONS AND EXAMPLES:

10.2.1. Definition. A non - empty set R is said to be an associative ring if in R there are defined two operations, denoted by $+$ and $\bullet$ respectively, such that for all a, b, c in R.

(i) a + b is in R
(ii) a + b = b + a
(iii) (a + b) + c = a + (b + c)
(iv) There is an element 0 in R such that a + 0 = a for every a in R.
(v) There exists an element $-a$ in R such that $a + (-a) = 0$.
(vi) a.b is in R
(vii) a.(b.c) = (a.b).c
(viii) a.(b+c) = a.b +a.c and
(ix) (b+c).a = b.a + c.a

Axioms (i) through (v) merely state that R is an abelian group under the operation +, which we call addition. Axioms (vi) and (vii) insist that R be closed under an associative operation; which we call multiplication. Axioms (viii) and (ix) Serves to inter relate the two operations of R.

10.2.2. Definition. Let (R, +, $\bullet$) be a ring. If there is an element 1 in R such that a.1 = 1.a = a for every a in R then R is said to be a ring with unit element. If the multiplication of R is such that a.b = b.a for every a, b in R then we call R a commutative ring.

10.2.3. Example. Let R be the set of integers, positive, negative, and 0; + is the usual addition and the usual multiplication of integers. Then R is a commutative ring with unit element.

10.2.4. Example. Let R be the set of even integers under the usual operations of addition and multiplication. Then R is a commutative ring but has no unit element.

10.2.5. Example. Let R be the set of rational numbers under the usual addition and multiplication of rational numbers. Then R is a commutative ring with unit element.

10.2.6. Self Assessment questions.

Find the multiplicative inverse of a given non-zero rational number.

10.2.7. Definition. A ring in which the non-zero elements form a group is called a division ring or skew-field.

10.3. INTEGRAL DOMAINS AND FIELDS:

10.3.1. Definition. If R is a commutative ring, then $0 \neq a \in R$ is said to be a zero divisor if there exists $b \in R$, $b \neq 0$, such that ab = 0.

10.3.2. Definition. A commutative ring is an integral domain if it has no zero divisors.

10.3.3. Definition. A ring is said to be a division ring if its non-zero elements form a group under multiplication.

10.3.4. Example. The ring of integers is an integral domain.

10.3.5. Example. The ring of all real numbers with usual addition and multiplication is a division ring as well as field.

10.3.6. Lemma. If R is a ring, them for all a, $b \in R$
(i) a 0 = 0 a = 0
(ii) a(–b) = (–a)(b) = –(ab)

(iii) (–a)(–b) = ab

If, in addition, R has a unit element 1, then

(iv) (–1) a = –a

(v) (–1)(–1) =1

Proof. Assume that R is a ring and let a, b $\in$ R

(i) a 0 = a(0 + 0) = a0 + a0

Now, 0 + a0 = a0 = a0 + a0

$\Rightarrow$ a0 = 0 (by the right cancellation law)

similarly, 0a + 0 = 0a = (0+0)a = 0a+0a

$\Rightarrow$ 0a = 0 (by the left cancellation law)

(ii) By (i) 0 = a0

= a (b + (–b))

= ab + a(–b)

$\Rightarrow$ a(–b) = –(ab)

Also 0 = 0b = (a + –a)b

= ab + (–a)b

$\Rightarrow$ (–a)b = –(ab)

Therefore, a(–b) = (–a)b = – (ab)

(iii) (–a)(–b) = –(a(–b)) (by (ii))

= – (–(ab)) (by (ii))

= ab

(iv) Suppose that R has a unit element '1'

consider (–1)a = –(1a) (by ii)

= –a

Therefore, (–1) a = –a

(v) Consider (–1)(–1) = – ((1)(-1)) by (ii)

= –(–(1.1) by (ii)

= 1.1 =1

((or) by (iii) (–1)(–1) = 1.1 =1.

10.3.7. The Pigeonhole Principle

If n objects are distributed over m places, and if n > m, then some places receives at least two objects.

10.3.8. Lemma. A finite integral domain is a field.

Proof. Let R be a finite integral domain. Then R is a commutative ring which has no zero divisors.

To prove R is a field it is enough to prove that every non-zero element has multiplicative

inverse. Now we show.

(i) There exists $1 \in 0$ such that $a1 = a \ \forall\ a \in R$

(ii) For every $0 \neq a \in R$ there exists $b \in R$ such that $ab = 1$

Let $R = \{x_1, x_2, \ldots, x_n\}$ and $0 \neq a \in R$

Now, we claim that $x_1a, x_2a, \ldots, x_na$ are distinct elements in R

For, $x_ia = x_ja$ for some $i \neq j$

$\Rightarrow (x_i - x_j)\, a = 0$

$\Rightarrow x_i - x_j = 0$ (since R is integral domain and $a \neq 0$)

$\Rightarrow x_i = x_j$

This is a contradiction to $i \neq j$

Thus $x_1a, x_2a, \ldots, x_na$ are distinct elements in R.

Therefore $R = \{x_1a, x_2a, \ldots, x_na\}$

Since $a \in R$, $a = x_ka$ for some $1 \leq k \leq n$

This implies $a = x_ka = ax_k$ ($\because$ R is commutative)

Now we show that x_k is the identity element in R.

Let $r \in R$

Then $r = x_l\, a$ for some $1 \leq l \leq n$

Consider $r\, x_k = (x_la)x_k$

$= x_l\, (a\, x_k)$

$= x_l\, a = r$

Therefore, $r\, x_k = x_k\, r = r$, $\forall r \in R$

This shows that x_k is the identity element in R. Let us denote $x_k = 1$.

Also $x_k = x_ja$ for some, $1 \leq j \leq n$ ($\therefore x_k \in R$, $x_k = x_ja$ for some j)

Since R is commutative,

$x_k = x_j a = a\, x_j$ for some $1 \leq j \leq n$

This shows that x_j is the multiplicative inverse of a in R.

Hence R is a field.

10.3.9.Corollary. If p is a prime number then J_p, the ring of integers mod p, is a field.

Proof. By the lemma 10.2.8 it is enough to prove that J_p is an integral domain, since it only has a finite number of elements. We know that $J_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{p-1}\}$ is a commutative ring with respect to addition and multiplication modulo p.

Let $\bar{a}, \bar{b} \in J_p$ and suppose that $\bar{a}\,\bar{b} = \bar{0}$

Now $\bar{a}\,\bar{b} = \bar{0} \Rightarrow ab \equiv 0 \pmod p$

$\Rightarrow$ ab–0 is divisible by p

$\Rightarrow p \mid ab$

$\Rightarrow$ p|a or p|b

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

$\Rightarrow \bar{a}\,\bar{b} = 0$ or $\bar{b} = 0$

Therefore, $\bar{a}\,\bar{b} = 0 \Rightarrow$ either $\bar{a} = 0$ *or* $\bar{b} = 0$

so, J_p in a finite integral domain
Thus J_p is a field.

10.3.10. Definition. An integral domain D is said to be of characteristic 0 if the relation ma = 0, where $a \neq 0$ is in D, and m is an integer, can hold only if m = 0.

10.3.11. Definition. An integral domain D is said to be of finite characteristic if there exists a positive integer m such that ma = 0 for all $a \in D$.

10.3.12. Definition. A ring in which $x^2 = x$ for all elements is called a Boolean ring.

10.3.13. Examples.

(i) **$(Z, +, \bullet)$** is an integral domain with characteristic 0.
(ii) **$(Z_p, +, \bullet)$** is an integral domain with characteristic p.
(iii) **$(Z_6, +, \bullet)$** is a commutative ring but not an integral domain.

10.4 SOME PRELIMINARY RESULTS ON RINGS:

10.4.1. Problem. If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative.

Solution. We are given that $x^2 = x \ \forall\, x \in R$. So, for all x, $x^2=0 \Rightarrow x=0$ (since $x^2 = x$)

Now for all x, y ∈ R , consider $(xy–xyx)^2 = (xy–xyx)(xy–xyx)$,

$= xyxy–xyxyx–xyx^2y+xyx^2yx$
$= xyxy–xyxyx–xyxy+xyxyx$ (since $x^2=x$)
$= 0$

$\Rightarrow (xy – xyx)^2 = 0$
$\Rightarrow xy – xyx = 0$ (since $x^2=0 \Rightarrow x=0$)
$\Rightarrow xy = xyx \quad \rightarrow (1)$

Similarly, we can see that $(yx–xyx)^2 = 0$
Therefore $yx–xyx = 0$
$\Rightarrow yx = xyx \quad \rightarrow (2)$

from (1) & (2) , $xyx = xy = yx \quad \forall x, y \in R$
i.e., $xy = yx \quad \forall x, y \in R$
Hence R is commutative.

10.4.2. Problem. Prove that if $a,b \in R$ and n,m are integers, then (na)(mb) = (nm) (ab)

Solution. Let R be a ring and $a,b \in R$

consider $(na)(mb) = (\underbrace{a + a + \ldots + a}_{n \text{ times}})(\underbrace{b + b + \ldots + b}_{m \text{ times}})$

$= \underbrace{ab + ab + \ldots + ab}_{mn \text{ times}}$

$= (mn)(ab)$

10.4.3. Problem. If D is an integral domain and if na =0 for some $0 \neq a$ in D and someinteger n $\neq 0$, prove that D is of finite characteristic.

Solution. Assume that D is an integral domain without loss of generality, wemay assume that n is a positive integer.
We are given that na =0 for some $0 \neq a \in D$ and $n \in N$For all
$x \in D$ we have
(na)x = 0

$$\Rightarrow (\underbrace{a + a + ...+ a}_{n \text{ times}})x = 0$$

$$\Rightarrow \underbrace{ax + ax + \ldots + ax}_{n \text{ times}} = 0$$

$$\Rightarrow a(\underbrace{x + x + ...+ x}_{n \text{ times}}) = 0$$

$$\Rightarrow a(nx) = 0$$

Since D is an integral domain and $a \neq 0$ we must have nx = 0 $\forall x \in D$
Then D is of finite characteristic.

10.4.4. Problem. Show that the commutative ring D is an integral domain if and only if for a, b, c $\in$ D with $a \neq 0$ the relation ab = ac implies that b = c.

Solution. Suppose D is an integral domain. Let a, b, c $\in$ D with $a \neq 0$
Assume that ab = ac

$\Rightarrow$ ab – ac = 0
$\Rightarrow$ a (b – c) = 0
$\Rightarrow$ b – c =0 ($\because 0 \neq a \in D$ & D is an integral domain)
$\Rightarrow$ b = c

Conversely assume that ab = ac $\Rightarrow$ b=c

10.4.5. Self Assessment Question. If a, b, c, d $\in$ R and R is a ring then evaluate(a + b)(c + d).

10.4.6. Self Assessment Question. Prove that if a, b $\in$ R, then $(a + b)^2 = a^2 + ab + b^2$, where$x^2$ = xx.

10.4.7. Self Assessment Question. Find out two examples for an integral domain which are not fields.

10.5. MODEL EXAMINATION QUESTIONS:

10.5.1. Define a ring, commutative ring. Give two examples of each. Give an exampleof a ring which is not commutative.

10.5.2. Prove that every field is an integral domain.

10.5.3. If R is a ring and a,b$\in$R, then show that (–a)(–b) = ab.

10.5.4. Prove that every finite integral domain is a field.

10.5.5. Show that the characteristic of an integral domain is a prime number if D is offinite characteristic

10.6 SUMMARY:

The abstract algebraic concepts. Ring, ring with unit element, commutative ring, integral domain, division ring, field were introduced. The set of integers and the set of rational numbers with usual addition and multiplication of numbers form commutative ring with unit element. The set of even integers under the usual operations of addition and multiplication forms a commutative ring without unit element. The set of integers modulo n (where $n \in \mathbb{Z}^+$, $n \geq 2$) forms a finite commutative ring.

A finite integral domain is a field. For any prime number p, the set of integers modulo p forms a field. An integral domain D is of finite characteristic if there exists a positive integer m such that ma = 0 for all a $\in$ D. If D is of finite characteristic then the smallest positive integer p with pa = 0 for all a $\in$ D, is called the characteristic of the integral domain D. This p is a prime number.

10.7 TECHNICAL TERMS:

Ring with unit element.	Let $(R,+,\cdot)$ be a ring. If $1 \in R$ such that a.1 = 1.a =a for every a $\in$ R, then we say that R is a ring with unit element
Commutative ring.	If a.b = b. a $\forall$ $a, b \in R$, then R is said to be a commutative ring.
Division ring.	A ring R is said to be a division ring if R-{0} is a group.
Integral Domain.	A commutative ring is said to be an integral domainif it has no zero divisors.
Field.	A division ring is said to be a field if it is commutative.
The pigeon hole principle.	If n objects are distributed over m places and if n>m then some place receives at least two objects.
Finite Characteristic.	An integral domain D is said to be of finite characteristic if there exists a positive integer m such that ma = 0 $\forall$ a $\in$ D.
Characteristic.	If D is of finite characteristic then we define the characteristic of D to be the smallest positive integer p such that pa = 0 for all a $\in$ D.

10.8 ANSWERS TO SELF ASSESSMENT QUESTIONS:

10.2.6. Let Q be the set of all rational numbers and $0 \neq q \in Q$. Then $q = \frac{a}{b}$ where a, b $\in$ Z with

$b \neq 0$. Since $q \neq 0$ we have that $a \neq 0$. Now $\frac{b}{a} \in Q$ such that $\frac{b}{a}.q = \frac{b}{a}\frac{a}{b} = 1$. Thus $\frac{b}{a}$ is the inverse of the given non-zero element $q = \frac{a}{b} \in Q$

10.4.5. Let R be a ring and let a, b, c, d $\in$ R
consider (a+b) (c+d) = a(c+d) +b (c+d) (by the distributive law)
= ac + ad + bc + bd

10.4.6. Let R be a ring and a, b $\in$ R

Consider $(a + b)^2$ = (a + b) (a + b)
= a(a + b) + b(a + b)
= aa + ab + ba + bb
= a^2 + ab + ba + b^2

10.4.7. (i) The set of integers forms an integral domain which is not a field.
(ii) The set of real quaternions forms an integral domain which is not a field.

10.9 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr. T. Srinivasa Rao

LESSON -11

HOMOMORPHISMS – IDEALS AND QUOTIENT RINGS

OBJECTIVES:

The objectives of this lesson are to

- Introduce the concepts like homomorphism, kernel and isomorphism.
- Discuss some examples for homomorphism and kernel.
- Introduce the concepts like ideal, quotient ring.
- Discuss some examples of ideals.
- Know how to construct a quotient ring R/I for a given ideal I

STRUCTURE:

11.1. INTRODUCTION:

The notion of homomorphism is one of the central ideas that are common to all aspects of modern algebra. By this, one means a mapping from one algebraic system to a like algebraic system which preserves the structure.

Next we define ideal of a given ring R and construct the quotient ring of Rwith respect to a given ideal in a natural way. Ideals play an important role in thestudy of rings.

11.2. RING HOMOMORPHISM'S:

11.2.1. Definition. A mapping ϕ from the ring R into the ring R^1 is said to be a homomorphism if

(i) $(a+b) = \phi(a) + \phi(b)$

(ii) $(ab) = \phi(a)\ \phi(b)$. for all $a,b \in R$

11.2.2. Lemma. If ϕ is a homomorphism of R into R^1, then

(i) $(0) = 0$

(ii) $(-a) = -\phi(a)$ for every $a \in R$

Proof. (i) Consider $\phi(0) = \phi(0+0)$

$$= \phi(o) + \phi(0)$$

$\Rightarrow 0 + \phi(0) = \phi(0) + \phi(0)$

$\Rightarrow 0 = \phi(0)$

Therefore, $\phi(0) = 0$

(ii) Let $a \in R$

Consider $\phi(a+(-a)) = \phi(a) + \phi(-a)$

$\Rightarrow \phi(0) = \phi(a) + \phi(-a)$

$\Rightarrow 0 = \phi(a) + \phi(-a)$ (by (i))

$\Rightarrow \phi(-a) = -\phi(a)$.

11.2.3. Note: If both R and R^1 have the respective unit elements 1 and 1^1 for their multiplications it need not follow that $\phi(1) = 1^1$. However, if R^1 is an integral domain, or if R^1 is arbitrary but ϕ is onto then $\phi(1) = 1^1$.

11.2.4. Self assessment question: Consider Z, the ring of integers, and the ring $J(\sqrt{2}) = \{m+n\sqrt{2} / m,n \in Z\}$. Define $\phi: J(\sqrt{2}) \rightarrow J(\sqrt{2})$ By $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$. Show that ϕ is an isomorphism.

11.3. KERNEL OF A HOMOMORPHISM:

11.3.1. Definition. If ϕ is a homomorphism of R into R^1 then the Kernel of ϕ , $I(\phi)$ is the set of all elements $a \in R$ such that $\phi(a) = 0$, the zero element of R^1.

11.3.2. Lemma. If ϕ is a homomorphism of R into R^1 with kernel $I(\phi)$ then

(i) $I(\phi)$ is a subgroup of R under addition.

(ii) If $a \in I(\phi)$ and $r \in R$ then both ar and ra are in $I(\phi)$.

Proof. Assume that $\phi : R \rightarrow R^1$ be a homomorphism with kernel, $I(\phi)$.

i.e, $I(\phi) = \{a \in R / \phi(a) = 0$,the zero element $R^1\}$.

Since $0 \in I(\phi)$, $I(\phi)$ is non-empty

clearly, $I(\phi) \subseteq R$

(i) We have to prove that $I(\phi)$ is a subgroup of R under addition.

Let $x, y \in I(\phi)$

Then $\phi(x) = 0$ and $\phi(y) = 0$

Now $\phi(a+(-b)) = \phi(a) + \phi(-b)$ ($\because \phi$ is a homo morphism)

$= \phi(a) - \phi(b)$ ($\because \phi(-b) = -\phi(b)$)

$\Rightarrow \phi(a - b) = \phi(a) - \phi(b)$

$= 0 - 0$

$= 0$

$\Rightarrow a - b \in I(\phi)$

Therefore, I(ϕ) is a subgroup of R under addition.

(ii) Let $a \in I(\phi)$ and $r \in R$
consider $\phi(ra) = \phi(a)\,\phi(r) = 0$ ($\because \phi$ is a homomorphism)
$\phi(r) = 0 \Rightarrow ar \in I(\phi)$
Also consider $\phi(ar) = \phi(r)\,\phi(a)$ ($\because \phi$ is homomorphism)
$= \phi(r)0$
$= 0$
$\Rightarrow ar \in I(\phi)$
Let $y \in I(\phi)$

Then $\phi(y) = 0$

$\Rightarrow \phi(y) = \phi(0)$

$\Rightarrow y = 0$ ($\because \phi$ is one – to – one)

Therefore, Kernel of ϕ, $I(\phi) = \{0\}$

Conversely, suppose that $I(\phi) = \{0\}$

We have to prove that ϕ is one -to- one

Let $a,b \in R$ ə $\phi(a) = \phi(b)$

$\Rightarrow \phi(a) - \phi(b) = 0$

$\Rightarrow \phi(a-b) = 0$ ($\because \phi$ is a homomorphism)

$\Rightarrow a - b \in I(\phi) = \{0\}$

$\Rightarrow a - b = 0$

$\Rightarrow a = b$

Therefore, ϕ is one – to – one

Thus ϕ is an isomorphism from R into R^1

11.4. IDEALS:

11.4.1. Definition. A non empty subset U of a ring R is said to be an ideal of R of if

(i) U is a subgroup of R under addition.
(ii) For every $u \in U$ and $r \in R$, both ur and ru are in U.

11.4.2. Lemma. If ϕ is a homomorphism of R into R^1 with kernel $I(\phi)$, then $I(\phi)$ is an ideal of R.

Proof. By lemma 11.3.2, $I(\phi)$ is an ideal of R.

11.4.3. Problem. If U is an ideal of R and $1 \in U$, prove that U = R

Sol. Assume that U is an ideal of R and $1 \in U$ clearly $U \subseteq R$
Let $r \in R$
Since U is an ideal of R we have that $r \in R$ and $1 \in U$ implies $r.1 \in U$. So, $r \in U$.
Therefore, $R \subseteq U$
Hence U = R

11.4.4. Problem. If F is a field, prove that its only ideals are {0} and F itself

Sol. Suppose that F is a field
We know that {0} and F are ideals of F
Let U be an ideal of F such that $U \neq \{0\}$
Since $U \neq \{0\}$, $\exists$ an element $y \in U \ni y \neq 0$
But F being a field and $y \neq 0$, $\exists\ y^{-1} \in F$.
Since U is an ideal of F, $yy^{-1} \in U$. But $yy^{-1} = 1 \in U$
By 11.4.3, U = F.

11.4.5. Problem. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.

Sol. Let F_1 , F_2 be two fields and ϕ is a homomorphism from F_1 into F_2 .
If $\phi(x) = 0\ \forall x \in F_1$ then $\phi = 0$
Now suppose that $\phi = 0$
Then $\exists\ a \in F_1 \ni \phi(a) \neq 0$
We know that $I(\phi)$ is an ideal of F_1 .
By 11.4.4, either $I(\phi) = \{0\}$ or $I(\phi) = F_1$
If $I(\phi) = F_1$ then $\phi(x) = 0\ \forall x \in F_1$ so that $\phi = 0$.
Which is a contradiction to $\phi \neq 0$.
Therefore, $I(\phi) = \{0\}$
By 11.3.2, ϕ is an isomorphism.

11.4.6. Self Assessment question. If R is a commutative ring and $a \in R$,
(i) Show that $aR = \{ar / r \in R\}$ is an ideal of R.
(ii) Show by an example that this may be false if R is not commutative.

11.4.7. Self assessment question. If U, V are ideal of R,
Let $U+V = \{u+v / u \in U, v \in V\}$. Prove that U +V is also an ideal.

11.4.8. Definition. Let R be a ring. A subset I of R is called a left ideal of R if
(i) I is a subgroup of R under addition.
(ii) $r \in R$, $a \in I$ implies $ra \in I$.

11.4.9. Definition. Let R be a Ring. A subset I of R is called a right ideal of R if
(i) I is a subgroup of R under addition.
(ii) $r \in R$, $a \in I$ implies $ar \in I$.

11.4.10. Problem. If U,V are ideals of R let UV be the set of all elements that can be written as finite sums of elements of the form uv, where $u \in U$ and $v \in V$. Prove that UV is ideal of R.

Solution. Suppose that U,V are ideals of R

$UV = \{\sum_{i=1}^{n} u_i v_i / u_i \in U, v_i \in V \text{ for } 1 \leq i \leq n, n \text{ is a positive integer}\}$
Let $x,y \in UV$
Then $x \sum_{i=1}^{n} u_i v_i$ and $y = \sum_{i=1}^{n} w_i z_i$ for some $u_i, w_i \in U, v_i, z_i \in V$ for each admissible values of i.

Now, $x-y = \sum_{i=1}^{n} u_i v_i - \sum_{i=1}^{n} w_i z_i$

$= \sum_{i=1}^{n} u_i v_i + \sum_{i=1}^{n} (-w_i z_i) \in UV$ (by the definition of UV)

So, x–y ∈UV
Therefore, UV is a subgroup of R under addition.
Let r ∈R

Consider xr = $(\sum_{i=1}^{n} u_i v_i)\, r$
$= \sum_{i=1}^{n} (u_i v_i) r$
$= \sum_{i=1}^{n} u_i (v_i r) \in UV$ (∵ Vis an ideal, v_i r∈V)
$\Rightarrow$ xr ∈UV
similarly, we can prove that ru∈UV
Therefore, UV is an ideal of R.

11.4.11. Self Assessment question. If U, V are ideals of a ring R, prove that UV $\subseteq$ U $\cap$ V.

11.4.12. Problem. If R is a ring and a ∈ R let r(a) = {x ∈ R / ax = 0}. Prove that r(a) is a right ideal of R.

Solution. Suppose that R is a ring and a ∈ R
Let r(a) = {x ∈ R / ax = 0}
Suppose x, y ∈ r(a)
Then ax = 0 and ay = 0
Consider a(x – y) = ax – ay = 0–0 =0
So, x – y ∈ r(a)
Thus r(a) is a subgroup of R under addition.
Next if x ∈ r(a) and r∈R, we have a(xr) = (ax)r = 0r = 0
So, xr ∈ r(a) for all x∈r(a) and r ∈ R
Hence r(a) is a right ideal of R.

11.4.13. Problem. If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R^1 . Prove that ϕ (1) is the unit element of R^1

Solution. Assume that R is a ring with unit element 1 and ϕ: R→ R^1 is an onto homomorphism.
Let y∈ R^1
Since ϕ is onto, ∃ x∈R ϶ ϕ (x) = y.
Now yϕ (1) = ϕ (x) ϕ (1)
= ϕ (x.1) (∵ ϕ is homomorphism)
= ϕ (x)
= y
Similarly, ϕ (1) y = y
Hence ϕ (1) is the unit element of R^1.

11.5. QUOTIENT RINGS.

11.5.1. Lemma. If U is an ideal of the ring R, the R/U is a ring and is a homomorphic image of R.

Proof. Let R be a ring and U is an ideal of R define a relation '~' on R as follows.
a ~ b iff a – b∈R for all a, b∈R
Now we prove that '~' is an equivalence relation on R.
Since a – a = 0 ∈ R, ∀a ∈ R, a ~ a, ∀a∈R.

So, the relation '~' is reflexive
suppose $a \sim b$, $a, b \in R$
$\Rightarrow a - b \in U$
$\Rightarrow b - a \in U$ ($\because$ U is an ideal of R)
$\Rightarrow b \sim a$
So, the relation '~' is symmetric.
Suppose $a \sim b$, $b \sim c$, $a, b, c \in R$
$\Rightarrow a - b \in U$ and $b - c \in U$
$\Rightarrow (a - b) + (b - c) \in U$
$\Rightarrow a - c \in U$
$\Rightarrow a \sim c$
So, the relation '~' is transitive.
Hence the relation '~' is an equivalence relation on R.
Now, the set of all equivalence classes under the relation '~' denoted by R/U is given by
$R/U = \{a+U / a \in R\}$
We define '+' and ' • ' on R/U as follows.
(i) $(a + U) + (b + U) = (a + b) + U$
(ii) $(a + U).(b + U) = ab + U$ for all $a, b \in R$.
First we show that the operations defined above are well defined.
Suppose $a + U = a^1 + U$ and $b + U = b^1 + U$, where $a, a^1, b, b^1 \in R$.
$\Rightarrow a - a^1 \in U$ and $b - b^1 \in U$
$\Rightarrow (a - a^1) + (b - b^1) \in U$
$\Rightarrow (a + b) - (a^1 + b^1) \in U$
$\Rightarrow (a + b) + U = (a^1 + b^1) + U$
$\Rightarrow (a + U) + (b + U) = (a^1 + U) + (b^1 + U)$
So '+' is well defined
Suppose $a + U = a^1 + U$ and $b + U = b^1 + U$, where $a, a^1, b, b^1 \in R$
$\Rightarrow a - a^1 \in U$ and $b - b^1 \in U$
$\Rightarrow a - a^1 = u_1$ and $b - b^1 = u_2$ for some $u_1, u_2 \in U$
$\Rightarrow a = a^1 + u_1$ and $b = b^1 + u_2$
consider $ab = (a^1 + u_1)(b^1 + u_2)$
$= a^1 (b^1 + u_2) + u_1 (b^1 + u_2)$
$= a^1 b^1 + a^1 u_2 + u_1 b^1 + u_1 u_2$
Since U is an ideal of R, we have that
$a^1u_2 + u_1b^1 + u_1u_2 \in U$ ($\because a^1 u_2 \in U$, $u_1 b^1 \in U$ and $u_1u_2 \in U$)
put $u_3 = a^1u_2 + u_1b^1 + u_1u_2$
Then $ab = a^1b^1 + u_3$
So, $ab + U = (a^1b^1 + u_3) + U$
$= a^1 b^1 + (u_3 + U)$ ($\therefore u_3 \in U$, $u_3 + U = U$)
$= a^1 b^1 + U$
i.e; $(a + U)(b + U) = (a^1+U)(b^1+U)$
Thus ' • ' is well defined.
Now, we show that $(R/U, +, \bullet)$ is a ring
Let $a + U, b + U, c + U \in R/U$.

(i) Consider $(a + U) + [(b + U) + (c + U)] = (a + U) + [(b + c) + U]$
$= (a + (b + c)) + U$
$= ((a + b) + c) + U$
$= [(a + b) + U] + (c + U)$

$= [(a + U) + (b + U)] + (c + U)$

Thus '+' is associative in R/U

(ii) Now $(a + U) + (b + U) = (a + b) + U$
$= (b + a) + U$
$= (b + U) + (a + U)$

This '+' is commutative in R/U

(iii) Clearly $0 + U \in R/U$

For any $a + U \in R/U$, $(a + U) + (0 + U) = (a + 0) + U = a + U$

So, $0 + U$ is the additive identity in R/U.

(iv) Let $a + U \in R/U$

Since $a \in R$, $-a \in R$

Clearly $-a + U \in R/U$

Consider $(a + U) + (-a + U) = (a + (-a)) + U$
$= 0 + U$
$= U$

So, $-a + U$ is the additive inverse of $a + U$

Hence $(R/U, +, \bullet)$ is an abelian group.

(v) $(a + U)[(b + U)(c + U)] = (a + U)(bc + U)$
$= (a(bc) + U)$
$= ((ab)c + U)$
$= (ab + U)(c + U)$
$= [(a + U)(b + U)](c + U)$

So, $(R/U, +, \bullet)$ is associative.

(vi) Consider $(a + U)[(b + U) + (c + U)] = (a + U)[(b + c) + U]$
$= a(b + c) + U$
$= (ab + ac) + U$
$= (ab + U) + (ac + U)$
$= (a + U)(b + U) + (a + U)(c + U)$

Similarly, we can prove that

$[(a + U) + (b + U)](c + U) = (a + U)(c + U) + (b + U)(c + U)$

So, distributive laws are satisfied in R/U

Hence $(R/U, +, \bullet)$ is a ring.

Define $\phi : R \to R / U$ by $\phi(a) = a + U \ \forall \ a \in R$

Now, we show that ϕ is a homomorphism.

Let $a, b \in R$

$\phi(a + b) = (a + b) + U$ (by the definition of ϕ)
$= (a + U) + (b + U)$
$= \phi(a) + \phi(b)\ \phi(ab)$
$= (a + b) + U$
$= (a + U) + (b + U)$
$= \phi(a) + \phi(b)$

Therefore, ϕ is a homomorphism from R_1 into R/U

Now, we prove that ϕ is onto

Let $x + U \in R/U$ where $x \in R$

By the definition, $\phi(x) = x + U$

i.e; for any $x + U \in R/U$, $\exists\ x \in R \ni \phi(x) = x + U$

So, ϕ is onto
Thus R/U is the homomorphic image of R.

11.5.2. Definition. The ring (R/U, +, •) is called the quotient ring of the ring R by the given ideal U.

11.5.3. Note. If R is a commutative ring so is R/U
For any $a + U, b + U \in R/U$
$(a + U)(b + U) = ab + U$
$= ba + U$
$= (b + U)(a + U)$
So, R/U is commutative

11.5.4. Result. If $\phi: R \to R/U$ then the kernel of ϕ, $I(\phi) = U$.
Proof. Suppose $\phi : R \to R/U$ is an onto homomorphism.
Let $x \in I(\phi)$
Now $x \in I(\phi) \Leftrightarrow \phi(x) = 0$ in R/U
$\Leftrightarrow x+U = 0+U$
$\Leftrightarrow x \in U$
Then $I(\phi) = U$

11.5.5. Theorem. Let R, R^1 be rings ϕ is a homomorphism of R onto R^1 with kernel U. Then R^1 is isomorphic to R/U. Moreover there is a one-to-one correspondence between the set of ideals of R^1 and the set of ideals of R which contain U. This correspondence can be achieved by associating with an ideal W^1 in R^1 the ideal W in R defined by $W = \{x \in R/\phi(x) = W^1\}$. With W so defined, R/W is isomorphic to R^1/W^1 .

Proof. Suppose that $\phi: R \to R^1$ be an onto homomorphism with kernel U.
Then $\phi(R) = \{\phi(x) / x \in R\} = R^1$ and $I(\phi)=U$

(i) We have to prove that R1 is isomorphic to R/U
Define $\Psi : R/U \to R^1$ by $\Psi(a + U) = \phi(a), \forall a \in R$
Let $a, b \in R$.
Ψ is well defined and one - to - one.
now $a + U = b + U \Leftrightarrow a - b \in U$
$\Leftrightarrow \phi(a - b) = 0 \quad (\because I(\phi) = U)$
$\Leftrightarrow \phi(a) = \phi(b)$
$\Leftrightarrow \Psi(a + U) = \Psi(b + U)$
So, Ψ is well defined and one- to- one
Ψ is onto.
Let $r^1 \in R^1$
Since ϕ is onto, $\exists\ r \in R$ ə $\phi(r) = r^1$
clearly, $r + U \in R/U$ and by the definition of Ψ, $\Psi(r + U) = \phi(r) = r^1$
Ψ is homomorphism.
Consider $\Psi[(a + U) + (b + U)] = \Psi[(a + b) + U)]$
$= \phi(a + b)$
$= \phi(a) + \phi(b)$
$= \Psi(a + U) + \Psi(b + U)$
also $\Psi[(a + U)(b + U)] = \Psi(ab + U)$
$= \phi(ab)$

$= \phi(a)\,\phi(b)$
$= \Psi(a + U)\,\Psi(b + U)$

So, Ψ is a homomorphism.
Hence R/U is isomorphic to R^1

(ii) Let A = { J/J is an ideal of R containing R^1}
and B = {W^1 / W^1 is an ideal of R^1}
Define f : A$\rightarrow$ B as follows.
Let J$\in$ A
We have to prove that ϕ(J) is an ideal of R^1.
Let $a^1, b^1 \in \phi(J)$
Then $a^1 = \phi(a)$ and $b^1 = \phi(b)$ for some a, b $\in$ J
Now, $a^1 - b^1 = \phi(a) - \phi(b)$
$= \phi(a - b)$ ($\because$ ϕ is homomorphism)
Since J is an ideal of R and a, b$\in$ J
$\phi(a - b) \in \phi(J)$ and hence $a^1 - b^1 \in \phi(J)$
Let $r^1 \in R^1$
Since ϕ is onto, $\exists\ r \in R$ ə $\phi(r) = r^1$.
Now $a^1 r^1 = \phi(a)\,\phi(r)$
$= \phi(ar) \in \phi(J)$ ($\because$ ϕ is homo and J is an ideal of R)
So, $a^1r^1 \in \phi(J)$
similarly, $r^1a^1 \in \phi(J)$
Thus ϕ(J) is an ideal of R^1 and hence $\phi(J) \in B$
Now, we show the one- to -one correspondence between A and B.
Define f(J) = ϕ (J)
f is one - to - one.
Suppose $f(J_1) = f(J_2)$ where $J_1, J_2 \in A$
$\Rightarrow \phi(J_1) = \phi(J_2)$
We have to prove that $J_1 = J_2$
Let x$\in$ J_1
$\Rightarrow \phi(x) \in \phi(J_1) = \phi(J_2)$
$\Rightarrow \phi(x) = \phi(y)$ for some $y \in J_2$
$\Rightarrow \phi(x-y) = 0$ in R1
$\Rightarrow x - y \in I(\phi) = U \subseteq J_2$
$\Rightarrow x - y \in J_2$
Since $y \in J_2$ and $x - y \in J_2$ and J_2 is an ideal of R, $(x - y) + y \in J_2$
Clearly $x = x - y + y \in J_2$
$\Rightarrow x \in J_2$
So, $J_1 \subseteq J_2$. Similarly, we can prove that $J_2 \subseteq J_1$
Hence $J_1 = J_2$
Then f is one - to - one
f is onto.
Let $W^1 \in B$
Define $W = \phi^{-1}W^1$
$= \{x \in R / \phi(x) \in W^1\}$
Now we claim that W is an ideal of R
Let a, b$\in$ W
Then $\phi(a), \phi(b) \in W^1$

$\Rightarrow \phi(a-b) = \phi(a) - \phi(b) \in W^1$ $(\because W^1$ is an ideal)

$\Rightarrow a - b \in W$

Let $r \in R$

Consider $\phi(ar) = \phi(a)\,\phi(r) \in W^1$ $(\because \phi(a) \in W^1, \phi(r) \in R^1$ and W^1 is an ideal)

$\Rightarrow ar \in W$

Similarly, we can prove that $ra \in W$

Hence W is an ideal of R

Also, note that $U = I(\phi) \subseteq \phi^{-1}(W^1) = W$

So, $U \subseteq W$

i.e, for each $W^1 \in B$, $\exists\, W \in A$ ə $f(W) = \phi(W) = W^1$

Thus f is onto

Hence there is a one - to - one correspondence between the set of ideals of R^1 and the set of ideals of R which contain U.

(iii) Finally, we have to prove that R/W is isomorphic to R^1 / W^1

Consider the natural onto homomorphism $\pi: R^1 \to R^1 / W^1$ defined by $\pi(r^1) = r^1 + W^1$ for all $r^1 \in R^1$

Put $h = \pi \circ \phi$. By the composition of mappings, h is a mapping from R into R^1.

Since ϕ and π are onto and homomorphism, $h = \pi \circ \phi$ is also an onto homomorphism. Let $x \in R$

Now, $x \in \ker h \Leftrightarrow h(x) = 0$

$\Leftrightarrow (\pi \circ \phi)(x) = 0$

$\Leftrightarrow \pi(\phi(x)) = 0$

$\Leftrightarrow \phi(x) + W^1 = 0 + W^1$

$\Leftrightarrow \phi(x) \in W^1$

$\Leftrightarrow x \in W$

This shows that ker h=W

By the fundamental theorem of homomorphism

$R/\ker h \cong R^1 / W^1$

i.e $R/W \cong R^1 / W^1$

11.6. MODEL EXAMINATION QUESTIONS.

11.6.1. If $\phi: R \to R^1$ is ring homomorphism, then show that kerϕ is a subgroup of (R, +).

11.6.2. If $\phi: R \to R^1$ is ring homomorphism with ker $\phi = 0 \Leftrightarrow \phi$ is a one-to-one mapping.

11.6.3. The homomorphism ϕ of R into R^1 is an isomorphism iff $I(\phi) = \{0\}$

11.6.4. If U is an ideal of the ring R, then R/U is a ring and is a homomorphic image of R.

11.6.5. If F is a field, prove that its only ideals are (0) and F itself.

11.6.6. If R is a ring and $a \in R$. Let $r(a) = \{x \in R / ax = 0\}$. Prove that r(a) is a right ideal of R.

11.7 SUMMARY:

* A mapping ϕ from a ring R into a ring R^1 is said to be a ring homomorphism if it satisfies (i) $\phi(a+b) = \phi(a) + \phi(b)$ and (ii)$\phi(ab) = \phi(a)\,\phi(b)$, for all $a,b \in R$.

* If $\phi : R \to R1$ is a homomorphism then $\phi(0)=0$ and $\phi(-a) = -\phi(a)$, for all $a \in R$.

* The set $\{x \in R / \phi(x) = 0\}$ is called the kernel of ϕ and is denoted by $I(\phi)$ or ker ϕ.

* A mapping $\phi: R \to R^1$ is one- to-one $\Leftrightarrow$ ker $\phi = \{0\}$.

* A non empty set U of a ring R is said to be an ideal of R if

(i) U is subgroup of R under addition

(ii) $ar \in U$ and $ra \in U$ for any $a \in U$ and $r \in R$.

* If ϕ: R$\rightarrow$ R^1 is homomorphism then ker ϕ is an ideal of R.
* If U is an ideal of R then R/U = {r+U/r$\in$R} is a ring called the quotient ring. Also R/U is a homomorphic image of R.

11.8 TECHNICAL TERMS:

- Homomorphism
- Kernel
- Isomorphism
- Left ideal
- Right ideal
- Ideal

11.9 ANSWERS TO SELF ASSESSMENT QUESTION:

11.2.4. Let $m + n\sqrt{2}, p + q\sqrt{2} \in J\sqrt{2}$)

$$(\phi(m + n\sqrt{2}) + (p + q\sqrt{2})) = \phi((m + p) + (n + q)\sqrt{2})$$
$$= (m + p) - (n + q)\sqrt{2}$$
$$= m + p - n\sqrt{2} - q\sqrt{2}$$
$$= (m - n\sqrt{2}) + (p - q\sqrt{2})$$
$$= \phi(m + n\sqrt{2}) + \phi(p + q\sqrt{2})$$

So, $(x + y) = \phi(x) + \phi(y)$ for all x, y $\in J(\sqrt{2})$

$$\phi((m + n\sqrt{2})(p + q\sqrt{2})) = \phi(mp + mq\sqrt{2} + np\sqrt{2} + nq\sqrt{2}\sqrt{2})$$
$$= (mp + 2nq + (mq + np)\sqrt{2}$$
$$= (mp + 2nq) - (mq + np)\sqrt{2}$$

Consider $\phi((m + n\sqrt{2})(p + q\sqrt{2})) = (mp + 2nq) - (mq + np)\sqrt{2}$
$$= (m - n\sqrt{2})(p - q\sqrt{2})$$
$$= \phi((m + n\sqrt{2})(p + q\sqrt{2}))$$

This proves that ϕ is a homomorphism

Suppose $(m + n\sqrt{2}) = 0$
$$\Rightarrow m - n\sqrt{2} = 0$$
$\Rightarrow$ m = 0 and n = 0
$\Rightarrow$ m+ n$\sqrt{2}$ =0

So, ϕ is one - to - one mapping

For $m + n\sqrt{2} \in (\sqrt{2})$, the element $m - n\sqrt{2} \in J(\sqrt{2}) \ni \phi(m + n\sqrt{2}) = m - n\sqrt{2}$

So ϕ is onto.

Hence ϕ is an isomorphism.

11.4.6. a) First we will show that aR is a sub group of R.

Suppose x, y $\in$ aR . Then x = ar$_1$ and y = ar$_2$ for some r$_1$, r$_2$ $\in$ R

But x – y = ar$_1$ – a r$_2$ = a(r$_1$ – r$_2$) = ar$_3$ for some r$_3\in$R.

So, x – y $\in$aR.

Thus aR is a subgroup of R under addition.

Next if some x$\in$aR and r$\in$R, Then we have x = ar$_4$ for some r$_4\in$R.

Also rx = xr ($\because$ R is a commutative ring)
= (ar$_4$)r
= a(r$_4$r)

$= ar_5$ for some $r_5 \in R$.
So, for all $x \in aR$ and $r \in R$ we have $rx, xr \in aR$
Thus aR is an ideal of R.

(b) Consider $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a,b,c,d \in R \right\}$
Then R is a ring but not commutative.
Since $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac+0 & ad+0 \\ 0 & 0 \end{pmatrix}$
And $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ca+0 & cb+0 \\ 0 & 0 \end{pmatrix}$
So, R is not a commutative ring.
Let $a = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$
Then $aR = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix}$
$= \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$ where $\alpha = a + c \in R \text{ and } \beta = b + d \in R$
But aR is not a two sided ideal
For, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in aR \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in R$
We have $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin R$

There is a non-commutative ring R, aR need not be an ideal

11.4.7. Let $x, y \in U + V$
Then $x = u + v$ and $y = w + z$ for some $u, w \in U$ and $v, z \in V$
now, $x - y = (u + v) - (w + z)$
$= (u - w) + (v - z) \in U+V$
$\therefore$ U + V is subgroup of (R, +)
(Since: U is an ideal, $u - w \in U$ and since V is an ideal, $v - z \in V$)
Let $r \in R$ and $x \in U+V$
Consider $xr = (u + v)r$
$= ur + vr \in U + V$
$\therefore$ U + V is a right ideal of R
Similarly, we can prove that U + V is a left ideal of R.

11.4.11. Let $x \in UV$
Then $x = \sum_{i=1}^{n} u_i v_i$ for some positive integer n, $u_i \in V \text{ and } v_i \in V$ for all $1 \leq i \leq n$.
Since $u_i \in U$, $v_i \in V \subset R$ and U is a right ideal of R, we have that $u_i v_i \in U$ for all $1 \leq i \leq n$.
Since U is a subgroup of (R,+), we have $\sum_{i=1}^{n} u_i v_i$. So, $x \in U$
Similarly, we can prove that $x \in V$
Hence $x \in U \cap V$
$\therefore UV \subseteq U \cap V$

11.10 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer- Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.T.Srinivasa Rao

LESSON -12

MORE IDEALS AND QUOTIENT RINGS

OBJECTIVES:

The objectives of this lesson are to

- Define a maximal ideal of a ring R.
- Give some examples of maximal ideals in some concrete rings.
- Get a necessary and sufficient condition for R/M to be a field.

STRUCTURE:

12.1 INTRODUCTION:

We continue the discussion of ideals and quotient rings of the previous lesson. We have seen that some properties of a ring R are carried over to the quotient ring R/M, for instance the commutative property and the existence of unit element. Also there are some properties which are valid in a ring but not valid in the quotient ring. For example, Z is an integral domain but $Z_4=Z_{42}$is not an integral domain.

In this lesson, we will prove when a commutative ring with unit element will become a field. Also we will prove the necessary and sufficient condition for R/M to be a field, where M is an ideal of R.

12.2 MAXIMAL IDEAL:

12.2.1 Definition. An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subset U \subset R$, then either R=U or M=U.

12.2.2. Lemma. Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.

Proof. Let R be a commutative ring with unit element whose only ideals are (0) and R itself. To prove R is a field, it is enough to show that every non-zero element has a multiplicative inverse in R.
Let $0 \neq a \in R$.
Consider the set $Ra=\{xa / x \in R\}$

Now we claim that Ra is an ideal of R
Let $u, v \in Ra$, then $u = r_1a$, $v = r_2 a$ for some $r_1, r_2 \in R$.

So, $u + v = r_1a + r_2a$
$= (r_1+r_2) a \in Ra$

Similarly, $-u = -r_1a = (-r_1)a \in Ra$

Hence Ra is an additive subgroup of R

Moreover if $r \in R$, $ru = r(r_1a) = (rr_1)a \in Ra$

Thus Ra is an ideal of R

Since R has the only ideals (0) and R itself either Ra = (0) or Ra = R

As $0 \neq a = 1.a \in Ra$, $Ra \neq (0)$

So, Ra=R.

Then there exists an element $b \in R$ such that ab = 1

This shows that b is the inverse of a in R

Hence R is a field.

12.2.3. Problem. Let R be the ring of all the real valued, continuous functions on the closed unit interval [0,1]. Let $M = \{f(x) \in R / f(\frac{1}{2}) = 0\}$. Then M is a maximal ideal of R.

Sol. First we prove that M is an ideal of R.

Let $f(x), g(x) \in M$

Then $f(\frac{1}{2}) = g(\frac{1}{2}) = 0$ (by the definition of M)

Clearly, $f(\frac{1}{2}) - g(\frac{1}{2}) = 0-0=0$

$\Rightarrow f(x) - g(x) \in M$ $(\because f(x) \in M \Leftrightarrow f(\frac{1}{2}) = 0)$

So, M is an additive subgroup of R.

Let $f(x) \in R$, $g(x) \in M$

Then $g(\frac{1}{2})=0$

Now $f(\frac{1}{2})\, g(\frac{1}{2}) = f(\frac{1}{2})\, 0 = 0$

and $g(\frac{1}{2})\, f(\frac{1}{2}) = 0\, f(\frac{1}{2}) = 0$

Thus $f(x)\, g(x) \in M$.....(1)

$\therefore$ M is an ideal of R.

Now we prove that M is a maximal ideal of R. Suppose there is an ideal U of R such that $M \subset U$ and $M \neq U$

Then there is a function $g(x) \in U$ and $g(x) \notin M$

So that $g(\frac{1}{2}) = a \neq 0$

Write $f(x) = g(x) - a$ .....(2)

Then $f(\frac{1}{2}) = g(\frac{1}{2}) - a$

$= a-a = 0$

So, $f(x) \in M \subset U$

$\Rightarrow f(x) \in U$

Now $f(x) \in U$ and $g(x) \in U$ implies that $g(x) - f(x) \in U$ ($\because$ U is an ideal of R)

But $a = g(x) - f(x) \in U$ (by 2)

Since R is the ring of all the real-valued, continuous functions on [0,1] and $a \neq 0$, there is a function $l(x) \in R$ such that $l(x) = 1/a$ for all $x \in [0,1]$.

Since U is an ideal, $1 = a.1/a = g(x)\, l(x) \in U$.

That is $1 \in U$. So, U=R

$\therefore$ M is a maximal ideal of R.

12.2.4. Problem. Let Z be the ring of integers with respect to usual addition and multiplication of numbers and let M be an ideal of Z. Then M is a maximal ideal of Z if and only if M = (n) = p Z for some prime number p.

Sol. We know that for any $n \in Z$, (n) = nZ is an ideal of Z in of this form….(1)
Let M be an ideal of Z. Suppose that M is a maximal ideal of Z
By (1), M = p Z for some positive integer $p \in Z$.
Now, we show that p is a prime number. If possible assume that p is not a prime number.
Then p = ab with $1< a < p$ and $1< b < p$.
Write U = aZ
Then U is an ideal of Z.
Claim: $M \subseteq U$
Let $n \in M= pZ$
$\Rightarrow n = px$ for some $x \in Z$
Now, $n = px = (ab)x = a(bx) \in aZ=U$.
$\Rightarrow n \in U$
Then $M \subseteq U$

Since M is a maximal ideal of Z and $M \subseteq U \subseteq Z$, we have either U = M or U= Z.
If U=Z, then aZ = Z. So, a =1.Which is a contradiction.
Suppose U = M
Since U = aZ, $a = a.1 \in a Z = U$
clearly $a \in M = pZ$
$\Rightarrow yb=1$
$\Rightarrow y=1$or b =1
$\Rightarrow$ b=1 or a=p
Which is a contradiction.
$\therefore$ p is a prime number
Conversely, suppose that p is a prime number. We will show that M = pZ is a maximal ideal of Z.
Suppose that N is an ideal of Z such that $M \subseteq N \subseteq U \subseteq Z$ and $M \neq N$.
Claim. M=Z
By (1), N= NZ for some positive integer n.
Now $p \in pZ=M \subseteq N=NZ$
$\Rightarrow p=nm$ for some integer m
..... $\Rightarrow$p/m or p/n……..(2)
If p/n then n=ps for $s \in Z$
$\Rightarrow n \in pZ=M$
$\Rightarrow N \subseteq M$
$\Rightarrow N = M$ ($\because M \subseteq N$)
Which is a contradiction to $M \neq N$,
So, p$\nmid$n
From (2), p/m
$\Rightarrow$ m=pr for some $r \in Z$
Now, p = nm = n (pr)= (np)r = (pn)r = p(nr)
$\Rightarrow 1= nr \in nZ = N$
$\Rightarrow 1 \in N$
$\Rightarrow$ N = Z

Hence M = pZ is a maximal ideal of Z.

12.2.5. Self Assessment Question.
A commutative ring with identity is a field iff (0) is a maximal ideal.

12.2.6. Theorem. If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field.

Proof. Assume that R is a commutative ring with unit element and M is an ideal of R. Suppose that R/M is a field. Since R/M is a field, it's only ideals are (0) =M/M and R/M itself.

That is there is no ideal I/M of R/M such that $M/M \subset I/M \subset R/M$……(1)

By the known theorem, there is a one-to-one correspondence between the set of ideals of R/M and the set ideals of R which contain M.

Under this correspondence, the ideal M of R corresponds to the ideal (0), R/M where as the ideal R of R corresponds to the ideal R/M of R/M…..(2).
From (1) & (2), there no ideal I of R such that $M \subset I \subset R$.
Hence M is a maximal ideal of R.
Conversely suppose that M is a maximal ideal of R.

As R is a commutative ring with unit element, R/M is also a commutative ring with unit element. Since M is maximal ideal of R, we have that the only ideals of R which contain M are M and R itself. That is there exists no ideal I of R. Such that $M \subset I \subset R$

So, by the same correspondence, there is no ideal I/M of R/M such that $M/M \subset I/M \subset R/M$.

Thus the only ideals of R/M are (0) = M/M and R/M itself.
By the known lemma, R/M is a field.

12.2.7. Problem: Let R be a ring with unit element, R not necessarily commutative, such that the only right ideals of R are (0) and R. Prove that R is a division ring

Solution: Let R be a ring with unit element. To prove R is a division ring it is enough to prove that every non-zero element of R has a multiplicative inverse in R.
Let $0 \neq a \in R$
Clearly, $aR = \{ax / x \in R\}$
Now, we prove that a R is a right ideal of R
Let $u,v \in aR$
Then $u = ar_1$ and $v = ar_2$ for some $r_1, r_2 \in R$
Now, $u - v = ar_1 - ar_2$
$= a(r_1 - r_2) \in R$
Let $s \in R$
Consider $us = (ar_1)s$
$= a(r_1 s) \in aR$
$\therefore$ a R is a right ideal of R
But, the only right ideals of R are (0) and R itself.
So, either ar = (0) or aR=R
Since $0 \neq a \in R$, $aR \neq (0)$ ($\because 0 \neq a.1 \in aR$)

$\therefore$ aR=R…….(1)
Since1$\in$ R, there exists b$\in$R such that 1=ab
Clearly b$\neq$ 0
Now bR is a non-zero right ideal of R
Then bR = R
$\Rightarrow$1= bc for c $\in$ R

consider $a = a.1$
= a(bc)
= (ab)c
= 1.c
= c

$\therefore$ ab =1= ba
This shows that b is the inverse of a in R
Thus every non-zero element of R has a multiplicative inverse in R
Hence R is a division ring.

12.2.8. Problem: Let J be the ring of integers, p a prime number, and (p) the ideal of J consisting of all multiples of p. Prove

(i) J/(p) is isomorphic to J_p, the ring of integers mod p.

(ii) J_p is a field.

Solution: Clearly, $J_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots \ldots \overline{p-1}\}$

(i) Define $\phi : J \to J_p$ by $\phi(n) = \overline{n}$ for every n $\in$ J,
Where $\overline{n}$ is the equivalence class containing n under the relation modulo p.
Now, we prove that ϕ is an onto homomorphism.
For any $n_1, n_2 \in$ J
$\phi(n_1+n_2) = \overline{n_1 + n_2}$
$= \overline{n_1} + \overline{n_2}$
$= \phi(n_1) + \phi(n_2)$ and
$\phi(n_1 n_2) = \overline{n_1 n_2}$
$= \overline{n_1} \cdot \overline{n_2}$
$= \phi(n_1)\,\phi(n_2)$
$\therefore \phi$ is a ring homomorphism
Let $\overline{m} \in J_p$ then m is an integer and $0 \leq m \leq p-1$
Now m $\in$ J and ϕ(m) = $\overline{m}$

$\therefore \phi$ is onto
By the known theorem, we have
$J / \ker\phi \cong J_p$ …..(1)
Claim: $\ker\phi = (p) = pZ$
Let x $\in$ J

Now $x \in \ker\phi \Rightarrow \phi(x) = 0$

$\Rightarrow \bar{x} = \bar{0}$

$\Rightarrow$ x– 0 is divisible by p

$\Rightarrow$ x=py for some $y \in Z$

$\Rightarrow x \in pZ$

$\therefore \ker\emptyset \subseteq pZ$

Let $r \in pZ \Rightarrow$ r = pu for some $u \in Z$

$\Rightarrow$ r – 0 is divisible by p

$\Rightarrow r \equiv 0 (\text{mod } p)$

$\Rightarrow \phi(r) = \bar{0}$

$\Rightarrow \bar{r} = \bar{0}$

$\Rightarrow r \in \ker\phi$

$\therefore pZ \subseteq \ker\phi$

Hence $\ker\phi = pZ$……..(2)

From (1) & (2) $J/(p) \cong J_p$

(ii) Since p is a prime number, we have that (p) is a maximal ideal of J

By the known theorem, J/(p) is a field

As $J/(p) \cong J_p$, J_p is a field.

12.3. MODEL EXAMINATION QUESTIONS:

12.3.1. Define the term maximal ideal. If F is a field, then prove that $(_0)$ is the maximal ideal of F.

12.3.2. Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then prove that R is a field.

12.3.3. If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field.

12.3.4. Let R be a ring with unit element, R is not necessarily commutative, such that the only right ideals of R are $(_0)$ and R. Prove that R is a division ring.

12.4 SUMMARY:

The Concept of maximal ideal of a ring is introduced. Some maximal ideals in some concrete rings were given. We proved that a commutative ring R with unit element whose only ideals are (0) and R itself then R is a field. Also we proved that an ideal M of a commutative ring with unit element is maximal if and only if R/M is a field

12.5 TECHNICAL TERMS:

Maximal ideal Definition. 12.2.1

12.6 ANSWERS TO SELF ASSESSMENT QUESTIONS:

12.2.4. Let R be a commutative ring with identity.

By 12.2.6,M is a maximal ideal of R iff R/M in a field

Taking M=(0), we get that (0) is a maximal ideal of R iff R/(0) is a field. But, R/(0) = R.

So, R is field.

12.7 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.T.Srinivasa Rao

LESSON -13

THE FIELD OF QUOTIENT'S OF AN INTEGRAL DOMAIN

OBJECTIVES:

The Objectives of this lesson are to

- Define imbedding of a ring in another ring.
- Define field of quotients of an integral domain
- Define equivalence relation and equivalence classes
- Prove a theorem namely, Every integral domain can be imbedded in a field.

STRUCTURE:

13.1. INTRODUCTION:

In this lesson we start with the integers Z and then build the rationals by taking all quotients of integers (avoiding division by zero). We start with an integral domain and build a field which contains all quotients of elements of theintegral domain. So, we are extending an integral domain to a field.

13.2. IMBEDDINGS:

13.2.1. Definition: A ring R can be imbedded in a ring R^1 if there is an isomorphism of R into R^1. If R and R^1 have unit elements 1 and 1^1 respectively, we insist that this isomorphism takes 1 into 1^1.

13.2.2. Definition: A ring R^1 will be called an over ring or extension of R if R can be imbedded in R^1.

13.2.3. Theorem: Every integral domain can be imbedded in a field.

Proof: Let D be an integral domain
Let $M = \{(a,b)/a,b \in D \text{ and } b \neq 0\}$

Here think of (a, b) as a/b
In M define a relation ~ as follows.

$(a,b) \sim (c,d)$ if and only if $ad = bc$……..(1)

We claim that this defines an equivalence relation on M.

(i) Let $(a,b) \in M$

Then a, b $\in$ D (by this definition of M)

Since D is an integral domain

we have that ab = ba
so, by (1) (a,b) ~ (a,b)

$\therefore$ The relation '~' is reflexive.

(ii) Let (a,b), (c,d) $\in$M and (a,b) ~ (c,d)

Then by (1), we have ad = bc
$\Rightarrow$ bc = ad
$\Rightarrow$ cb = da
$\Rightarrow$ (c, d) ~ (a,b)

$\therefore$ the relation '~' is symmetric

(iii) Let (a,b), (c,d), (e,f)$\in$M and

(a,b) ~ (c,d) and (c,d) ~ (e,f)
$\Rightarrow$ ad = bc and cf = de

$\Rightarrow$ adf = bcf and bcf = bde

$\Rightarrow$ adf = bde
$\Rightarrow$ afd = bed (by commutative law)
$\Rightarrow$ af = be (by the cancellation law)

$\Rightarrow$ (a,b) ~ (e,f)

$\therefore$ the relation '~' is transitive

Hence the relation '~' is an equivalence relation.

For any (a,b)$\in$M, let us denote the equivalence class containing (a,b) as

[a,b] write F = {[a,b]/(a,b) $\in$M}

We define the addition and multiplication on F as follows;

For any [a,b], [c,d] $\in$F, [a,b]+[c,d] = [ad + bc, bd]
and [a,b].[c,d] = [ac, bd]

Now, we prove that the operations additions and multiplication are well defined.

Suppose [a,b] = [a^1,b^1] and [c,d]=[c^1,d^1]
$\Rightarrow$ (a,b)~(a^1,b^1) and (c,d)~(c^1,d^1)

$\Rightarrow$ ab^1 =ba^1 and cd^1 =dc^1 ·····(2)

Claim: [a,b] + [c,d] = [a^1,b^1]+[c^1,d^1]

i.e., [ad+bc,bd] = [a^1d^1+b^1c^1, b^1d^1]

i.e., (ad+bc, bd) ~ (a^1d^1+b^1c^1,b^1d^1)

i.e., $(ad+bc)b^1d^1$ = $bd(a^1d^1+b^1c^1)$

Consider $(ad+bc)b^1d^1$ = $adb^1d^1+bcb^1d^1$

= $ab^1dd^1+bcd^1b^1$
= ba^1dd^1 +bdc^1b^1 (by (2))

$= bda^1d^1 + bdb^1c^1$

$= bd\,(a^1d^1 + b^1c^1)$

$\therefore$ addition is well defined on F

Claim: $[a,b].[c,d] = [a^1,b^1].[c^1,d^1]$

i.e $[ac, bd] = [a^1c^1, b^1d^1]$

i.e $(ac, bd) \sim (a^1c^1, b^1d^1)$

i.e $ac\ b^1d^1 = bda^1c^1$

Consider $acb^1d^1 = ab^1cd^1$

$= ab^1dc^1$ (by (2)

$= bda^1c^1$

$\therefore$ multiplication is well defined on f

Claim: addition is associative

let $[a,b],[c,d],[e,f] \in F$

Consider $([a,b] + [c,d]) + [e,f]$

$= [ad + bc, bd] + [e,f]$

$= [(ad)f + (bc)f + (bd)e, (bd)f]$

$= [a(df) + b(cf) + b(de), (bd)\,f]$

$= [a(df) + b(cf + de), b(df)]$

$= [a,b] + [cf + de, df]$

$= [a.b] + ([c,d] + [e,f])$

Claim: addition is commutative

Let $[a,b],[c,d] \in F$

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

$= [bc + ad, db]$

$= [cb + da, db]$

$= [c,d] + [a,b]$

Claim: Existence of zero element.

For any $0 \neq x \in D$, $[0,x] \in F$ and $[a,b] \in F$

Consider $[a,b] + [0,x] = [ax + b, bx]$

$= [ax, bx]$

$= [a,b]$ ($\because (a, b) \sim (ax, bx)$)

$\therefore$ $[0,x]$ is the additive identity

Claim: Existence of additive inverse.

For any $[a,b] \in F$, $[-a,b] \in F$ ($\because -a \in D$)

Consider $[a,b] + [-a,b] = [ab + b(-a), bb]$

$= [ab - ab, b^2]$

$= [0, b^2]$

$= [0,y]\ (b^2=y)$

$\because$ [–a, b] is the additive inverse of [a,b]

Claim: multiplication is associative

For any [a,b],[c,d],[e,f] $\in F$

Consider ([a,b][c,d][e,f]) = [ac,bd][e,f]

= [(ac)e, (bd)f)]

= [a(ce), b(df)]

= [ab],[(ce,df)]

= [a,b] ([c,d].[e,f])

Claim: multiplication is commutative

For any [a,b] ,[c,d] $\in F$

Consider [a,b].[c,d] = [ac,bd]

= [ca,db]

= [c,d].[a,b]

Claim: Existence of multiplicative identity.

For any $0 \neq d \in D$, [d,d] acts as a multiplicative identity. Let $[a,b] \in F$

Consider [a,b][d,d] = [ad,bd]

= [a,b]

Claim: Existence of multiplicative inverse

Let [a,b] be a non zero element in F.

So, $a \neq 0$ and $b \neq 0$. Clearly $[b,a] \in F$

Consider [a,b].[b,a] = [ab, ba]

= [ab, ab]

= [d,d] (where d = ab)

Then [b,a] is the multiplicative inverse of [a,b]

Claim: Multiplication is distributive over addition

For any [a,b],[c,d],[e,f] $\in F$

Consider [a,b].([c,d]+[e,f])

= [a,b].[cf+de,df]

= [a(cf+de),b(df)]

= [a(cf) + a(de), b(df)]

=[(a(cf) + a(ed)b,b(df)b]

= [((ac)f+(ae)d)b,bd(fb)]

= [(ac)fb+(ae)db,bd(bf)]

= [(ac)bf+bd(ae), bd(bf)]

= [ac, bd]+[ae, bf]

= [a,b].[c,d] + [a,b]. [e,f]

Similarly, we can prove that
([a,b]+[c,d]).[e.f] = [a,b].[e,f]+[c,d].[e,f]
Hence (F,+,•) is a field
i.e, F is a commutative division ring
Fix $0 \neq x \in D$
Define $\phi : D \to F$ by $\phi(a) = [ax, x]$
Clearly, ϕ is well - defined $\forall a \in D$
Claim : ϕ is one-to one

Suppose a,b $\in$D such that $\phi(a) = \phi(b)$

Now, $\phi(a) = \phi(b) \Rightarrow [ax,x]=[bx,x]$

$\Rightarrow (ax,x)\sim(bx,x)$

$\Rightarrow ax^2=xbx=bxx$

$\Rightarrow ax^2 = bx^2$

$\Rightarrow$ a = b (by cancellation laws)

$\therefore \phi$ is one-to-one

Claim: ϕ is a homomorphism
Let a,b$\in$D

Consider $\phi(a+b) = [(a+b)x,x]$

$= [ax+bx,x]$

$= [(ax+bx)x,xx]$

$= [axx+bxx,xx]$

$= [axx+xbx,xx]$

$= [ax,x]+[bx,x]$

$= \phi(a)+ \phi(b)$ and

$\phi(ab) = [(ab)x,x]$

$= [(ab)xx,xx]$

$= [a(bx)x,xx]$

$= [a(xb)x,xx]$

$= [(a\ x)bx,xx]$

$= [ax,x].[bx,x]$

$= \phi(a)+ \phi(b)$

$\therefore \phi$ is a homomorphism

Hence $\phi : D \to F$, defined by $\phi(a) =[ax, x]\ \forall a \in D$.

Where $0 \neq x \in D$ be a fixed element, is an isomorphism of D into F.

Thus D can be imbedded in F.

13.2.4. Note. The field constructed in the above theorem is called the field of quotients of D. We may verify that if D = Z then F = Q.

13.2.5. Self Assessment Question.

Prove that the mapping $\phi : D \to F$ defined by $\phi(a) = [a,1]$ is an isomorphism of D into F.

13.2.6. Self Assessment Question.

Let R be an integral domain and F is the field of quotients of R. Then prove that F is the smallest field containing R.

13.3. MODEL EXAMINATION QUESTIONS:

13.3.1. Define the term imbedding. Show that every integral domain can be imbedded in a field.

13.3.2. Prove that the mapping $\phi: D \to F$ defined by $\phi(a) = [a,1]$ is an isomorphism of D into F

13.4 SUMMARY:

We learn that the ring of integers can be enlarged to the set of rational numbers which is a field. After defining imbedding, we have proved that every integral domain can be imbedded in a field. The field F constructed is called the field of quotients of the integral domain D.

13.5 TECHNICAL TERMS:

Imbedded. A ring R is said to be imbedded in a ring R^1 if there exists an isomorphism $\phi : R \to R^1$. Moreover, if R and R1 are rings with unit elements 1 and 1^1 respectively. We insist that $\phi(1) = 1^1$

13.6 ANSWERS TO SELF ASSESSMENT QUESTIONS:

13.2.5. First we prove that ϕ is well defined

Let $a,b \in D$ such that $a = b$
Then $a.1.1 = b.1.1$ ($\because 1 \in D$)

$\Rightarrow$ $a.1.1 = 1.b.1$

$\Rightarrow (a.1,1) \sim (b.1,1)$

$\Rightarrow [a.1,1]=[b.1,1]$

$\Rightarrow [a,1] = [b,1]$

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

$\therefore$ ϕ is well defined

Also $\phi(a+b) = [a+b,1]$
$= [a.1+1.b, 1.1]$
$= [a,1] + [b,1]$
$= \phi(a) + \phi(b)$

and $\phi(a,b) = [ab,1]$
$= [ab,1.1]$

$= [a,1].[b,1]$

$= \phi(a).\ \phi(b)$

$\therefore \phi$ is a ring homomorphism

now we prove that ϕ is one- to- one
Suppose $\phi(a) = \phi(b)$

$\Rightarrow [a,1] = [b,1]$

$\Rightarrow (a,1) \sim (b,1)$

$\Rightarrow a.1 = 1.b$

$\Rightarrow a = b$

$\therefore \phi$ is one - to -one

Hence ϕ is an one - to - one isomorphism

13.2.6. Let R be an integral domain and F be the field of quotients of R. Let F^1 be any field containing R. Then for any $x \in F$, $x = ab^{-1}$; $a,b \in R$; $b \neq 0$.
Since $R \subset F^1$, $a, b \in F^1$ and since F^1 is a field, it follows that $x = ab^{-1} \in F^1$. Thus $F \subset F^1$. This shows that F is the smallest field containing R.

(Let R be an integral domain and F is the field of quotients of R. Then every element $x \in F$ can be expressed as $x = ab^{-1}$ for some elements $a,b \in R$ with $b \neq 0$)

13.7 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.T.Srinivasa Rao

LESSON -14

EUCLIDEAN RINGS

OBJECTIVES:

The objectives of this lesson are to

- Define Euclidean ring, principal ideal ring, division ring, greatest common divisor, unit, associates, prime element and relatively prime elements.
- Prove some basic lemmas and theorems on the concepts defined.
- Deduce that a Euclidean ring is a principal ideal ring.
- Understand the difference between a unit and a unit element.
- Prove the unique factorization theorem for Euclidean rings.
- Determine all maximal ideals in an Euclidean ring.
- Defining the domain of Gaussian integers J[i].
- Study the ring of Gaussian integers, a particular Euclidean ring
- Prove Fermat's theorem.

STRUCTURE:

14.1. INTRODUCTIONS:

We now formulate the concepts like divisibility, factorization, prime elements, greatest common divisor etc for a general commutative ring. In this lesson, we study some types of rings which possess the property similar to the property of division algorithm in the ring Z of integers. We prove that any ideal A in an Euclidean ring R is of the form A = (a_o). Where $(a_o) = \{xa_0 / x \in R\}$. We also prove the unique factorization theorem. We give a simple, precise answer to the question, what conditions improved on an ideal A = (a_o) to ensure that A is a maximal ideal of R? In the last part of this lesson, we are about to particularize the notion of Euclidean ring to a concrete ring. The ring of Gaussian integers. Wedefine the set of Gaussian integers and observed that the set of Gaussian integersforms an Euclidean ring. Finally, we prove the Fermat's theorem.

14.2. EUCLIDEAN RINGS:

14.2.1. Definition. An integral domain R is said to be Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer d(a) such that

(i) For all $a,b \in R$, both nonzero, $d(a) \leq d(ab)$

(ii) For any $a,b \in R$, both non zero, there exist $t,r \in R$ such that $a = tb + r$ where either $r =$

0 or d(r) < d(b)

14.2.2. Example: The ring Z of integers is a Euclidean ring. Define d(a) = |a| for $a \in Z-\{0\}$

14.2.3. Theorem. Let R be a Euclidean ring and let A be an ideal of R. Then there an element $a_o \in A$ such that A consists exactly of all $a_o x$ as x rangers over R.

Proof. If $A = \{0\}$, then $a_0 = 0$ and hence $A = 0R = a_oR$
Thus we may assume that $A \neq \{0\}$. Hence there is an element $a \neq 0$ in A.
Consider the set $\{d(x)/0 \neq x \in A\}$ which is a nonempty set of non-negative integers.
Choose an element $a_0 \in A$ such that $d(a_o)$ is minimum

i.e., $d(a_o) = \min \{d(x)/0 \neq x \in A\}$
Since A is an ideal of R and $a_o \in A$ we have that $a_oR = \{ a_ox/x \in R\} \subseteq A$……..(1)
Claim: $A \subseteq a_oR$
Let $b \in A$. Clearly $a_o \neq 0$ and $b \neq 0$
Since R is an Euclidean ring there exists $t, r \in R$ such that $b = t a_o + r$ where r = 0 or $d(r) < d(a_0)$

Since $a_o \in A$ and A is an ideal of R, $t a_o \in A$ also since $b \in A$ and $ta_o \in A$ and A is an ideal we have $b - ta_o \in A$. But $r = b - ta_o \in A$. If $r \neq 0$ then $d(r) < d(a_o)$, which is a contradiction to the minimal of $d(a_o)$. Consequently r = 0 and hence $b = ta_o = a_ot$.
So, $b \in \{ a_ox/x \in R\}$

$\therefore A \subseteq \{a_ox/x \in R\}$……(2)

from (1) and (2) we have

$A = \{ a_ox/x \in R\} = a_oR$

14.2.4. Remark :

(i) In a commutative ring R with unit 1 for any $a \in R$, we know that aR = Ra is an ideal.

(ii) If A is an ideal of R such that $a \in A$. Then $aR \subseteq A$.

Therefore Ra = aR is the smallest ideal of R containing a and is denoted by (a)

14.2.5. Definition: An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form A = (a) for some $a \in R$.

14.2.6. Corollary. A Euclidean ring possesses a unit element.

Proof. Let R be a Euclidean ring.
Since R is an ideal of R itself by 14.2.3 we may conclude that $R = (u_0) = u_0R$ for some $u_0 \in R$.
Thus every element in R is a multiple of u_0. In Particular, $u_0 = u_0c$ for some $c \in R$.
If $a \in R$ then $a = xu_0$ for some $x \in R$
Now consider $ac = (xu_0)c$
$= x(u_0c)$
$= xu_0$
$= a$
This is true for any $x \in R$. Since R is commutative ac = a = ca for all $a \in R$

Hence c is the unit element in R
Thus R possesses a unit element.

14.3. PRINCIPLE IDEAL RINGS:

14.3.1. Definition. An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form A = (a) for some $a \in R$.

The smallest ideal containing a is denoted by (a) and is called the ideal generated by 'a'.

14.3.2. Corollary. Every Euclidean ring is a principal ideal ring.

Proof. Let R be a Euclidean ring by 14.2.6, R contains a unit element. Also
14.2.3, every ideal A of R is of the form A = aR for some $a \in R$.
Finally, by 14.2.4, if follows that A = aR = (a)
This shows that R is a principal ideal ring.

14.3.3. Definition. If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exists $c \in R$ such that b = ac. We shall denote a divides b by a/b & a does not divide b by $a \nmid b$.

14.3.4. Remark. Let R be a commutative ring and let $a,b,c \in R$. Then the following facts can be verified easily.

(i) If a | b and b | c then a | c

(ii) If a | b and a | c then a | (b ± c)

(iii) If a | b and a | bx for all $x \in R$

14.3.5. Definition. If $a,b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

(i) d/a and d/b

(ii) whenever c | a and c | b then c | d
The g c d of a and b is denoted by (a, b) = d

14.3.6. Lemma. Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof. Let R be a Euclidean ring. By 14.2.6, R has a unit element.

Let $a,b \in R$
Write $A = \{ra + sb / r,s \in R\}$

We claim that A is an ideal of R
For this, take $x,y \in A$.
Therefore $x = r_1a + s_1b$, $y = r_2a + s_2b$ for some $r_1, r_2, s_1, s_2 \in R$
Then $x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2)b \in A$
For any $u \in R$, $ux = u(r_1a + s_1b)$
$= (ur_1)a + (us_1)b \in A$
Since R is commutative , $xu \in A$

Thus A is an ideal of R.
by 14.2.3, there exists an element $d \in A$ such that $A = dR = (d)$
By the construction of A, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$
Also $a = 1.a + 0.b \in A$ and
$b = 0.a + 1.b \in A$
So, $a = da_1$ and $b = da_2$ for some $a_1, a_2 \in R$

$\Rightarrow$ d | a and d | b

i.e., d is a common divisor a and b
Let $c \in R$ such that c | a and c | b
By 14.3.4 (iii), c | λa and c | μb
Again by 14.3.4(ii), c|($\lambda a + \mu b$) But
$\lambda a + \mu b = d$. Therefore c | d
Thus d is a greatest common divisor of a and b and $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

14.3.7. Definition. Let R be a commutative ring with unit element. An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that ab = 1.

14.3.8. Note. Do not confuse a unit with a unit element! A unit in a ring is an element whose inverse is also in the ring.

14.3.9. Lemma. Let R be an integral domain with unit element and suppose that for $a,b \in R$ both a | b and b | a are true. Then a = ub, where u is a unit in R.

Proof. Let R be an integral domain with unit element and suppose that for $a,b \in R$ both a | b and b | a are true.

Since a | b , b = xa for some $x \in R$ and since b | a, a = yb for some $y \in R$

Then b = xa

= x(yb)

= (xy)b

$\Rightarrow$ b = (xy)b

$\Rightarrow$ 1.b = (xy)b

$\Rightarrow$ 1= (xy) (by cancellation laws)

$\Rightarrow$ xy = 1

$\Rightarrow$ yx =1($\therefore$ R us a commutative ring)

By the definition, y is a unit in R.
Hence a = yb where y is a unit in R
If we take u = y then a = ub where u is a unit in R.

14.3.10. Definition. Let R be a commutative ring with unit element. Two elements and b in R are said to be associates if b = ua for some unit u in R.

14.3.11. Problem. In a commutative ring with unit element prove that the relation a is an associative of b is an equivalence relation.

Solution. Let R be a commutative ring with unit element.

For a,b∈R, define a~b iff a is an associate of b.
That is a~b $\Leftrightarrow$ b = ua for some unit u∈R.

Since a = 1.a and 1 is a unit element, a is an associate of a itself.

That is a ~ a.Therefore the relation '~' is reflexive
Suppose a~b. So, b = ua for some unit u in R
Since u is a unit, there exists w∈R such that wu =1
Now wb = w(ua) = (wu)a = 1.a =a

$\Rightarrow$ wb = a and w is a unit

$\Rightarrow$ a = wb and w is a unit

$\Rightarrow$ b ~ a

Therefore the relation '~'is symmetric
suppose a~b and b~c

$\Rightarrow$ b=ua and c= wb for some units u, w in R since u and w are units, there exists v,z∈R such that uv=1 and wz =1.
As (uw) (zv) = u(wz)v = u.1.v=uv=1, uw is also a unit.
Now c =wb=w(ua) =(wu)a = (uw)a and uw is a unit. That c=(uw)a, uw is a unit in R.
This implies a~c.
Therefore the relation '~' is transitive.
Thus the relation '~' is an equivalence relation.

14.3.12. Problem. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.

Solution. Let d_1, d_2 be two greatest common divisors of a and b. Since d_1 is common divisor of a and b and d_2 is a g.c.d of a and b by 14.3.5, $d_1|d_2$.
Similarly, since d_2 is a common divisor of a and b and d_1 is a g.c.d of a and b by 14.3.5 $d_2|d_1$.
Since $d_1|d_2$ and $d_2|d_1$, 14.3.9, we have $d_1=ud_2$ for some unit u in R.Thus d_1, d_2 are associates.

14.3.13. Lemma. Let R be a Euclidean ring and a ≠ 0, b∈R. If b ≠ 0 is not a unit in R,then d(a) < d (ab).

Proof. Let R be a Euclidean ring and let a,b∈R where a ≠ 0.
Assume that b ≠ 0 is not a unit in R. Since a∈R, A = (a) = {xa/x∈R} in an ideal of R. For any y∈A we have y = xa for some x∈R.
Since R is a Euclidean ring by 14.2.1, we have d(a) ≤ d(xa) for all 0 ≠ x∈R.
That is d(a) ≤ d(y) for all 0 ≠ y∈A.
This shows that d(a) = min {d(y)/0 ≠ y∈A}……(1)
As a∈A and b∈R, ab∈A and hence d(a) ≤ d(ab)
If possible assume that d(a) = d(ab) ……(2)
From (1) and (2) we have
d(ab) = d(a) = min{ d(y)/0 ≠ y∈A}
Since ab∈A and A is an ideal of R it follows that (ab)R ⊆ A. Now we prove that A ⊆ (ab)R
Let 0 ≠ x∈A

Since R is an Euclidean ring, for x and ab, there exists t, r $\in$ R $\ni$ x = (ab)t +r
where r = 0 or d(r) < d(ab)…..…..(3)
Now r = x –(ab)t$\in$A
It r $\neq$ 0 then from (3), d(r) < d(ab) which is a contradiction to our assumption d(a) = d(ab).
Therefore r =0

$\Rightarrow$ x–(ab)t = 0

$\Rightarrow$ x = (ab)t $\in$(ab) R Therefore A $\subseteq$ (ab)R

Hence A = (ab) R
Now 0 $\neq$ a$\in$A = (ab) R

$\Rightarrow$ a = (ab)y for some y$\in$R

$\Rightarrow$ a – (ab)y = 0

$\Rightarrow$ a(1–by) =0

$\Rightarrow$ 1–by = 0 ($\because$ a $\neq$ 0 and R is an integral domain)

$\Rightarrow$ by =1

$\Rightarrow$ b is a unit

Which is a contradiction to the fact that b is not a unit.

$\therefore$ d(a) < d(ab)

14.3.14. Self Assessment Question.

Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that d(a) = d(1).

14.4. PRIME ELEMENTS:

14.4.1. Definition. In the Euclidean ring R a non unit π is said to be a prime elementof R if whenever π = ab, where a,b are in R then one of a or b is a unit in R.

A prime element is an element in R which cannot be factored in R in a non-trivial way.

14.4.2. Lemma. Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Proof. Let R be a Euclidean ring and let a$\in$R. Here the proof is by induction ond(a). Since d(1) $\leq$ d(1.x) = d(x)
for all 0 $\neq$ x$\in$R, we have d(1) = min{d(x)/0 $\neq$ x$\in$R}

If d(a) =d(1) then by 14.3.14, we get that a is a unit.
Assume that the result is true for all x$\in$R such that d(x) <d(a).
If a is a prime element then there is nothing to prove.
So, suppose that a is not a prime element.
Then a = bc, where neither b nor c is a unit in R.
By 14.3.13, d(b) < d(bc) = d(a) and also d(c) < d(bc) = d(a)
Thus by over induction hypothesis, we get that b = $\pi_1 \pi_2 \ldots \pi_n$ and

c= $\pi_1^1 \pi_2^1 \ldots\ldots \pi_m^1$ where π_i, 1$\leq$ i $\leq$ m and π_j^1, 1$\leq$ i $\leq$ m are prime elements of R.

Now a=bc = $(\pi_1 \pi_2 \ldots\ldots\ldots\ldots..\pi_n)(\pi_1^1 \pi_2^1 \ldots\ldots.\pi_m^1)$

$\Rightarrow$ a = $\pi_1 \pi_2 \ldots\ldots\ldots\ldots..\pi_n \pi_1^1 \pi_2^1 \ldots\ldots.\pi_m^1$

Hence the lemma.

14.4.3. Definition: In the Euclidean ring R, a and b are said to be relatively prime if their greatest common divisor is a unit of R.

14.4.4. Lemma. Let R be a Euclidean ring. Suppose that for a,b,c $\in$R, a |bc but (a,b) =1. Then a|c.

Proof. Let R be a Euclidean ring

Suppose that a,b,c$\in$R such that a |bc and (a,b) =1.By 14.3.6, the g.c.d 1 can be written as

1 = $\lambda a + \mu b$ for some $\lambda, \mu \in R$

$\Rightarrow$ c.1 = c ($\lambda a + \mu b$)

$\Rightarrow$ c = $c\lambda a + c\mu b$

Since a | bc, a | c μb also since a | c λa we have a | ($c\mu b + c\lambda a$)

That is a | c.

14.4.5. Lemma. If π is a prime element in the Euclidean ring R and π /ab where a,b$\in$R then π divides at least one of a or b.

Proof. Let R be a Euclidean ring. Assume that π is a prime element in R such that π /ab where a,b$\in$R

Suppose that $\pi \nmid$ a

we now show that π /b

write d = (π ,a) where d$\in$R

Then d|π and d/a…….(1)

Since d/π and π is a prime element, either d= π or d is a unit

If d = π then by (1), π /R

Which is a contradiction to our supposition. In the other case, we have that (π, a) =1

Since (π, a) =1 and π /ab by 14.4.4, π /b.

14.4.6. Corollary. If π is a prime element in the Euclidean ring R and π | a_1, a_2,...,a_n then π divides at least one a_1,a_2,……,a_n.

Proof. Let R be a Euclidean ring and let π be a prime element in R such that

π | a_1,a_2,...,a_n where a_1,a_2,….$a_n \in$R.

We will prove this by using induction on n. If n =1 then π | a_1

Suppose the result is true for n–1

That is π |a_1,a_2,…….a_{n-1}

Given π |a_1,a_2……$a_{n-1}a_n$

If π /b_n then the proof is over

suppose $\pi \nmid b_n$.

By 14.4.5, we conclude that π|a_1, a_2 .....a_{n-1}.

Now by induction hypothesis, if follows that π /a_i for some i.

14.4.7. Theorem. (Unique Factorization Theorem). Let R be a Euclidean ring and $a \neq 0$ a non-unit in R. Suppose that $a= \pi_1 \pi_2 \ldots\ldots\ldots\pi_n = \pi_1^1 \pi_2^1 \ldots\ldots\pi_m^1$ where the π_i and π_j^1 are prime elements of R. Then n = m and each π_i, $1 \leq i \leq n$ is an associate of some π_j^1, $1 \leq j \leq m$ and conversely each π_k^1 is an associate of some πq.

Proof. Let R be a Euclidean ring and $a \neq 0$ be a non-unit in R.
Given that $a= \pi_1 \pi_2 \ldots\ldots\ldots\pi_n = \pi_1^1 \pi_2^1 \ldots\pi_m^1$ where the π_i's and π_j^1 are prime elements of R……(1)
Since $\pi_1 | a$, $\pi_1 | \pi_1^1 \pi_2^1 \ldots\pi_m^1$ ($\because a=\pi_1^1 \pi_2^1 \ldots\pi_m^1$) By 14.4.6, $\pi_1 | \pi_j^1$ *for some* $1 \leq j \leq m$
Without loss of generality, we may assume j =1
Then $\pi_1 | \pi_1^1 \Rightarrow \pi_1^1 = u_1\pi_1$ for some $u_1 \in$ R. Since π_1^1 is prime, either u_1 is a unit or π_1 is a unit.
As π_1 is a prime element, u_1 is a unit.
This shows that π_1 is an associate π_1^1
From (1), $\pi_1 \pi_2 \ldots\ldots\ldots\pi_n = u1\pi_1 \pi_2^1 \ldots\pi_m^1$

$\Rightarrow \pi_1 \pi_2 \ldots\ldots\ldots\pi_n = \pi_1 u_1 \pi_2^1 \ldots\pi_m^1$

$\Rightarrow \pi_2 \ldots\ldots\ldots\pi_n = u_1 \pi_2^1 \ldots\pi_m^1$ (by cancellation laws)……..(2)

Since $\pi_2 | \pi_2 \ldots\ldots\ldots\pi_n$, $\pi_2 | u_1 \pi_2^1 \ldots\pi_m^1$ (by (2))
Again 14.4.6, $\pi_2 | \pi_j^1$ for some $2 \leq j \leq m$

Without loss of generality, we may assume that j =2

Then $\pi_2 | \pi_2^1 \Rightarrow \pi_2^1 = u_2\pi_2$ some unit u_2 in R
From (2), we have

$\pi_2 \ldots\ldots\ldots\pi_n = u_1u_2 \pi_2 \ldots\pi_m^1$

$\Rightarrow \pi_2 \ldots\ldots\ldots\pi_n = \pi_2 u_1u_2 \ldots\pi_m^1$ (by cancellation law)

$\Rightarrow \pi_3 \ldots\ldots\ldots\pi_n = u_1u_2 \ldots\pi_m^1$ (by cancellation law)

By repeating the above argument upto n steps, the left hand side becomes 1 and the right hand side becomes $u_1u_2.....u_n \pi_{n+1}\ldots\pi_m^1$
Therefore $n \leq m$ ($\because \pi_j^1$'s are non-units)
Similarly, we can prove then $m \leq n$
Thus n = m
In the above process we proved that each π_i, $1 \leq i \leq n$ is an associate of some π_j^1, $1 \leq j \leq m$ and each π_k^1, $1 \leq k \leq m$ is an associate of π_q^1, $1 \leq q \leq n$.

14.4.8. Result. Every non-zero element in a Euclidean ring R can be uniquely written(up to association) as a product of prime elements or is a unit in R.

Proof. Write the proofs 14.4.2 and 14.4.7

14.4.9. Lemma. The ideal $A =(a_0)$ is a maximal ideal of the Euclidean ring R if and only if a_0 is a prime element of R.
Proof. Let R be a Euclidean ring
Assume that $A = (a_0)$ is a maximal ideal of R. We have to prove that a_0 is a primeelement of R
If possible, suppose that a_0 is not a prime element of R. Then a_0= bc for some nonunit b and c of R.

Write B = (b). Then B is an ideal of R.
Now a_o = bc $\in$ (b) $\subseteq$ B.
$\Rightarrow a_o \in B$
$\Rightarrow A = (a_o) \subseteq B$
Therefore B is an ideal of R and A $\subseteq$ B$\subseteq$ R.
Now we claim that B $\neq$ A and B $\neq$ R.
If possible suppose that A = B
Then b $\in$ B = A = (a_0)
$\Rightarrow$ b= x a_0 for some x$\in$R
$\Rightarrow$ b= xbc for some x$\in$R
$\Rightarrow$ b= bxc for some x$\in$R
$\Rightarrow$1= xc for some x$\in$R
$\Rightarrow$ 'c' is a unit in R
This is a contradiction to the fact that c is not a unit.
$\therefore$ A $\neq$ B
Again, if possible suppose that B = R
$\Rightarrow$1$\in$B =(b)
$\Rightarrow$ 1= yb for some y$\in$R
$\Rightarrow$ b is a unit in R
This is contradiction to the fact that b is not a unit
$\therefore$ B $\neq$ R
Thus we get an ideal B of R such that $A \subseteq B \subseteq R$. This is a contradiction to A is a maximal ideal of R.
Thus a_0 is a prime element of R.
Conversely, Assume that a_0 is a prime element of R.
We have to prove that A = (a_0) is a maximal ideal of R.
Let U be an ideal of r such that A $\subseteq$ U $\subseteq$ R.
Since R is a Euclidean ring there exists u$\in$U such that U = (u)
Clearly $a_0 \in A \subseteq$ U = (u)
$\Rightarrow$ a_0= tu for some t$\in$R
Since a_0 is a prime element of R either t is a unit or u is a unit in R.
If u is a unit in R then Ru = R and hence U = Ru =R. That is u = R
If t is a unit in R then a_0= tu implies u= t^{-1} $a_0 \in (a_0)$ = A . That is u$\in$A.
Now U = (u) $\subseteq$ A and hence U = A.
Thus A is a maximal ideal of R.

14.4.10. Self Assessment Question.

Prove that if an ideal U of a ring R contains a unit of R, Then U = R

14.5. A PARTICULAR EUCLIDEAN RING:

14.5.1. Note. (i) Let J[i] denote the set of all complex numbers of the form a+bi wherea and b are integers. Under the usual addition and multiplication of complex numbers J[i] forms an integral domain called the domain of Gaussian integers.
(ii) For 0 $\neq$ x$\in$ J[i], d(x) is a non negative integer. i.e if x = a+ ib where a,b $\in$Z, d(x) = a^2+b^2 $\geq$ 1.

(iii) For any two non zero Gaussian integers, $x= a_1+ib_1$ and $x_2= a_2+ib_2$ we have

$d(xy) = d[(a_1+ib_1)(a_2+ib_2)]$

$= d[(a_1a_2-b_1b_2)+i(a_1b_2+b_1a_2)]$

$= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$

$= (a_1a_2)^2 + (b_1b_2)^2 - 2\, a_1a_2b_1b_2 + (a_1b_2)^2 + (b_1a_2)^2 + (a_1b_2 + 2\, a_1a_2b_1b_2$

$= a_1^2a_2^2 + b_1^2b_2^2 + a_1^2b_2^2 + b_1^2 a_2^2$

$= (a_1^2 + b_1^2)(a_2^2 + b_2^2)$

$= d(x)d(y)$

Therefore $d(xy) = d(x)\, d(y)$ for any two Gaussian integers.

(iv) Let $x,y \in J[i]$ such that $x \neq 0$, $y \neq 0$. Then by (ii), we get that $d(x) \geq 1$ and $d(y) \geq 1$

Also $d(x) = d(x).1 \leq d(x)\, d(y) = d(xy)$

$\Rightarrow d(x) \leq d(x,y)$

(v) Let $u,v \in J[i]$ there exist $t,r \in J[i]$ such that $v = tu+r$.

Where $r = 0$ or $d(r) < d(u), |r| \leq n/2$

14.5.2. Theorem. J[i] is a Euclidean ring.

Proof. We know that J[i] is an integral domain with unity with respect to the usual addition and multiplication of complex numbers.

For each $0 \neq x \in J[i]$ where $x = a+ib$, define $d(x) = a^2+b^2$ and clearly $d(x) \geq 1$.

Also by 14.5.1 (ii), for any $0 \neq x$, $0 \neq y$ in J[i], $d(x) \leq d(xy)$

Let $x,y \in J[i]$ such that $x \neq 0$

Case(i). Suppose that $y = a+ib$ is an arbitrary element in J[i] and $x = n = n+i0$ where n is a positive integer.

By the division algorithm for the ring of integers we can find integers u, v such that $a = un + u_1$ and $b= vn+v_1$ where u_1 and v_1 are integers satisfying $|u_1| \leq n/2$ and $|v_1| \leq n/2$. Let $t=u+iv$ and $r=u_1+iv_1$

then $y = a+ib = (un+u_1)+i(vn+v_1) = n(u+iv) + (u_1+iv_1) = nt + r = tx + r$ ($\because x = n$)

If $r \neq 0$ then $d(r) = d(u_1+iv_1)$

$= u_1^2 + v_2^2$

$< (n/2)^2 + (n/2)^2$

$= 2\,(n^2/4)$

$= (n/2)^2 < n^2$

$= d(n+i0)$

$= d(x)$

Thus there exists two elements, $t,r \in J[i]$ such that $y = tx + r$ where either $r = 0$ or $d(r) < d(x)$

Case (ii). Let $0 \neq x$ and $y \in J[i]$

Write $m = x\bar{x}$.

Clearly m is a positive integer and $\bar{x}$ is the complex conjugates of x.

Observe that $y\bar{x} \in J[i]$ ($\because y \in J[i]$, $\bar{x} \in J[i]$ and J[i] is an integral domain)

by case (i) , $\exists\ t_o, r_o \in J[i]$ such that $y\bar{x} = t_o m + r_o$ where either $r_0=0$ or $d(r_o)<d(m)$.

If $r_0=0$ then $y\bar{x} = t_0 m = t_0 x\bar{x}$ and so $y = t_0 x$ (by the cancellation laws)

So, $y = t_0\ x + 0 = t_0 x + r_0$.

Suppose $d(r_0) < d(m)$.

Then we have $y\bar{x} = t_0 m + r_0$

$\Rightarrow y\bar{x} - t_o m = r_0$

$\Rightarrow d(y\bar{x} - t_0 m) = d(r_o) < d(m) = d(x\bar{x})$

$\Rightarrow d(y\bar{x} - t_0 x\bar{x}) < d(x\bar{x})$

$\Rightarrow d(y - t_0 x)\, d(\bar{x}) < d(x)\, d(\bar{x})$

$\Rightarrow d((y - t_0 x)(\bar{x})) < d(x) d(\bar{x})$

$\Rightarrow d(y - t_0 x) <$

$d(x)$ Let $r^1 = y - t_0 x$

Then $y = t_0 x + r^1$ and $d(r^1) < d(x)$

Hence J[i] is an Euclidean ring.

14.5.3. Lemma. Let p be a prime integer and suppose that for some integer c relatively prime to p we 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 Z is a sub ring of J[i].

Part (i) In this part, we show that p is not a prime element of J[i].

If possible, suppose that p is a prime element of J[i].

Since $cp = x^2+y^2 = (x+iy)(x-iy)$, 14.4.5, $p \mid (x+iy)$ or $p \mid (x-iy)$ in J[i].

$p|(x+iy)$ then $(x+iy) = p(u+iw)$

so, $x = pu$ and $y = pw$

since $p \mid pu$ and $p \mid pw$, $p\ |(pu - ipw) \Rightarrow p|(x-iy)$

Therefore $p^2 \mid (x+iy)(x-iy)$

$\Rightarrow p^2 \mid (x^2+y^2)$

$\Rightarrow p^2 \mid cp$

$\Rightarrow P \mid c$

Which is a contradiction to p and c are relatively prime.

In a similar way, if $p|\ (x-iy)$ then we will get a contradictionThus p is not a prime element in J[i]

Part(ii) . Since p is not a prime element in J[i],

we have that $p = (a+ib)(g+id)$ for some non units $a+ib, g+id \in J[i]$

Since a+ib , g +id are non units, by 14.5.1 (ii), we have $a^2+b^2 > 1$ and $g^2+d^2 >1$.

Since $p = (a+ib)(g+id)$ is an integer it follows easily that $p = (a-ib)(g-id)$

Thus $p^2 = p.p = (a+ib)(g+id)(a-ib)(g-id)$

$= (a^2+b^2)(g^2+d^2)$

$\Rightarrow (a^2+b^2) \mid p^2$

$\Rightarrow a^2+b^2 = 1$ or p or p^2 ($\because$ p is prime)

we know that $a^2+b^2 \neq 1$
If $a^2+b^2 = p^2 = (a^2+b^2)(g^2+d^2)$ then $g^2+d^2=1$
Which is a contradiction.
Hence $a^2+b^2 = p$
Hence the lemma.

14.5.4. Lemma. If p is a prime number of the form 4n+1, then we can solve the congruence

$x^2 \equiv -1 \bmod p$.

Proof. Assume that p is a prime number of the 4n+1
i.e., p = 4n+1
$\Rightarrow$ p –1 = 4n
$\Rightarrow \frac{p-1}{2} = 2n$……(1)
Let $x=1.2.3\ldots\ldots.\frac{p-1}{2} = (\frac{p-1}{2})!$

Then x = (2n)! (By (1)), which is a product of an even number of terms

Therefore we can write of terms

$x= (-1)(-2)(-3) \ldots\ldots. (-\frac{p-1}{2})$

Also we know that for any integers k,
$(p–k) \equiv (–k) \bmod p$
$\Rightarrow \quad – k \equiv (p–k) \bmod p$
For k =1, $–1 \equiv (p–1) \bmod p$
For k = 2, $–2 \equiv (p–2) \bmod p$ and so on
Consider $x^2 = x \cdot x$

$= (1.2.3\ldots\ldots. \frac{p-1}{2}) ((-1)(-2)(-3) \ldots\ldots. (-\frac{p-1}{2}))$
$= (1.2.3\ldots\ldots. \frac{p-1}{2})((p-1)(p-2)(p-3) \ldots\ldots. (\frac{p-1}{2})$
$= (1.2.3\ldots\ldots. \frac{p-1}{2})((p-1)(p-2)(p-3) \ldots\ldots. (p - \frac{p-1}{2})$

$= (1.2.3\ldots\ldots. \frac{p-1}{2})((\frac{p+1}{2}) \ldots\ldots.)(p-2)(p-1))$
$= (p –1)!$
$x^2 \equiv –1 \bmod p$
(by willson's theorem , if p is a prime number the $(p–1)! \equiv –1 \bmod p$)

14.5.5. Lemma (Fermat). If p is a prime number of the form 4n+1, then $p = a^2+b^2$ forsome integers a, b.

Proof. First we show that there exists an integer x with $0< x \leq p–1$ such that
$x^2 \equiv –1(\bmod p)$
By 14.5.4, there exists y such that $y\ 2 \equiv –1(\bmod p)$…..(1)
By the division algorithm for y, p there exists two integers a and x such thaty = ap+x where x = 0 or $0<x\leq p–1$.

If x = 0 then $y = ap+0 \equiv 0(\bmod p)$ and so $0 \equiv y^2 \equiv –1(\bmod p) \Rightarrow 0 \equiv –1(\bmod p)$.

That is 1 is divisible by p. Which is a contradiction to p is prime. So, $x \neq 0$.

Therefore the inequality $0 < x < p$ holds
consider $y^2 = (ap+x)^2 = a^2p^2+x^2+2apx$

$\Rightarrow y^2 - x^2 = a^2p^2+2apx$

$= p(a^2p+2ax)$

$\Rightarrow y^2 - x^2$ is divisible by p

..... $\Rightarrow y^2 \equiv x^2 \pmod p$……..(2)

from (1) and (2),

we get $x^2 \equiv y^2 \equiv -1 \pmod p$
Therefore there exists $0 < x \leq p-1$ such that $x^2 \equiv -1 \pmod p$……(3)

Part(ii): Now we will find a number such that
$|s| < \frac{p}{2}$ and $s^2 \equiv -1 \pmod p$

If $|x| < \frac{p}{2}$ then s = x will do

Otherwise $x > p/2 \Rightarrow -x < -(p/2)$
Write $s = p - x$
now $s = p - x < p - (p/2) = (p/2)$

Consider $s^2 = (p-x)(p-x) = p^2-2px+x^2$

$\Rightarrow s^2 - x^2 = p(p-2x)$

$\Rightarrow p \mid s^2 - x^2$

..... $\Rightarrow s^2 \equiv x^2 \bmod p$…….(4)

Thus there exists an integer's' such that $|s| < p/2$ and $s^2 \equiv -1 \pmod p$
Part (iii). We have $s^2 \equiv -1 \pmod p$

$\Rightarrow s^2+1$ is divisible by p
$\Rightarrow s^2+1 = tp$ for some integer t

Consider $tp = s^2+1 \leq (p/2)^2 + 1 = p^2+4/4 < p^2$

$\Rightarrow tp < p^2 \Rightarrow t < p$

Since p is prime and $t < p$, we have that t and p are relatively prime
by 14.5.3, $p = a^2 + b^2$ for some integers a & b

14.5.6. Problem. Find all the units of J[i]
Solution. Since J[i] is a Euclidean ring, an element u is a unit of j[i] if and only if $d(u) = d(1)$
Let $u = a + ib$
Then u is a unit iff $d(u) = a^2+b^2 = d(1) = 1^2+0^2$
i.e, $a^2 + b^2 = 1$
But the integral solutions of $a^2+b^2 = 1$ are $a = 0, b = \pm 1$ and $a = \pm 1, b = 0$
Thus i, –i, 1, –1 are the only units J[i].

14.5.7. Self Assessment question. If a+ib is not a unit of J[i], prove $a^2+b^2 > 1$

14.6. MODEL EXAMINATION QUESTIONS:

14.6.1. Prove that a Euclidean ring possess a unit element.

14.6.2. State and prove unique factorization theorem.
14.6.3. Prove that J[i] is a Euclidean ring.
14.6.4. If p is a prime number of the form 4n+1 then $p = a^2+b^2$ for some integers a, b

14.7 SUMMARY:

The abstract algebraic concepts like Euclidean ring, principal ideal ring, division, g.c.d, unit, associate, prime element, relatively, prime were introduced. We have established that a Euclidean ring has a unit element. Every Euclidean ring is a principle ideal ring. The relation of being associates is an equivalence relation. In an Euclidean ring any two greatest common divisors of two given elements are associates. We proved the unique factorization theorem. Every non-zero element in an Euclidean ring R is either unit in R or it can be uniquely written (upto associates) as a product of prime elements. An ideal $A = (a_0)$ of a Eulidean ring R is a maximal ideal of $R \Leftrightarrow a_0$ is a prime element of R.

Later, we have defined the domain of Gaussian integers J[i]. We have proved that J[i] is Euclidean ring. The odd prime numbers can be divided into two classes. And those which have a remainder of 3 on division by 4. We showed that every prime number of the first kind can be written as the sum of two squares.

14.8 TECHNICAL TERMS:

Euclidean ring Definition. An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer d(a) such that

(i) For all $a,b \in R$, both nonzero, $d(a) \leq d(ab)$

(ii) For any $a,b \in R$, both non zero, there exist $t,r \in R$ such that $a = tb = r$ whereeither $r = 0$ or $d(a) < d(b)$.

Principal ideal ring Definition. An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form A = (a) for some $a \in R$.

Greatest common divisor Definition. If $a,b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

(i) d/a and d/b (ii) whenever c | a and c | b then c | d

The g c d of a and b is denoted by (a,b) = d

Unit. Let R be a commutative ring with unit element. An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that ab = 1.

Relatively Prime Definition; In the Euclidean ring R, a and b are said to be relatively prime if their greatest common divisor is a unit of R.

14.9 ANSWERS TO SELF ASSESSMENT QUESTIONS:

14.3.14. If a is a unit then there exists $b \in R$. Such that ab = 1
Now $d(a) \leq d(ab) = d(1)$
Also $d(1) \leq d(1.a) = da$
Hence d(a) = d(1)
Conversely, suppose d(a) = d(1)
If a is not a unit then by 14.3.13, we have that $d(1) < d(1.a) = d(a)$, which is

contradiction.
Hence a is a unit.

14.5.7. Since $a + ib \neq 0$ we have that $a \neq 0$ or $b \neq 0$
If $a \neq 0$ then $a^2+b^2 \geq a^2 \geq 1$
If $b \neq 0$ then $a^2+b^2 \geq b^2 \geq 1$
Therefore in any case, $a^2+b^2 \geq 1$
If $a^2+b^2 = 1$ then $a + ib$ is a unit, which is a contradiction
Hence $a^2+b^2>1$

14.10 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

Dr.T.Srinivasa Rao

LESSON - 15

POLYNOMIAL RINGS

OBJECTIVES

The objectives of this lesson are to

- Define polynomials, equality, addition, multiplication, degree, irreducibility of polynomials and the ring of polynomial $F[x]$ over a field F.
- Prove $F[x]$ is an integral domain.
- Understand and prove the division algorithm for polynomials.
- Apply the division algorithm to solve some problems and further theorems.
- Prove $F[x]$ is a principal ideal ring.

STRUCTURE

15.1. INTRODUCTION

Consider expressions of the type x^2-4x+3 or $x^4+\frac{1}{4}x^3-\frac{1}{2}x^2+\frac{1}{8}$. These are called polynomial expressions. The first expression x^2-4x+3 is called as a polynomial with integer coefficients and the second expression $x^4+\frac{1}{4}x^3-\frac{1}{2}x^2+\frac{1}{8}$ is called as a polynomial with rational coefficients. We are familiar with their properties like factorization, nature of roots etc. In this lesson, we shall consider the set $R[x]$ of all polynomial expressions with coefficients from a given commutative ring R with unit element. We shall define addition and multiplication on $R[x]$ forms a ring with respect to these operations. This ring will be a Euclidean ring when R is a field. So we can apply the results already obtained for Euclidean rings to this ring $R[x]$ when R is a field. We state and prove the division algorithm in $R[x]$.

15.2. POLYNOMIAL RINGS:

15.2.1. Definition: Let F be a field, the ring of polynomials in the indeterminate x denoted by $F[x]$ and is defined as the set of all symbols $a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n$, where n can be any non-negative integer and the coefficients $a_0, a_1, a_2, a_3, \ldots, a_n$ are all elements of F, i.e.,

$F[x]=\{\, a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n \mid n \text{ is a non-negative integer}, a_i \in F, 1 \le i \le n\}$

Every element of $F[x]$ is a polynomial with coefficients from F or polynomial over F.

15.2.2. Definition: Let F be a field and x be an indeterminate. If $p(x), q(x) \in F[x]$, then $p(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_mx^m$, for some m is non-negative integer,

$a_i \in F,\ 1 \le i \le m$ and $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n$, for some n is non-negative integer, $b_i \in F, 1 \le i \le n$.

(i) $p(x),\ q(x)$ are said to be equal if their corresponding coefficients are equal.

$i.e.\ p(x) = q(x)$ iff $a_i = b_i$ for all $i \ge 0$.

(ii) Addition of two polynomials $p(x)$ and $q(x)$ in $F[x]$ is defined as

$p(x) + q(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots + c_tx^t,$

$where\ c_i = a_i + b_i,$ for all i. Here + is commutative.

(iii)Multiplication of two polynomials $p(x)$ and $q(x)$ in $F[x]$ is defined as

$p(x).q(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots + c_tx^t,$

$where\ c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t.$

Clearly $(F[x],\ \cdot)$ is a semi group with identity $1 = 1 + 0x + 0x^2 + \cdots$

15.2.3. Example: Consider the polynomials $p(x) = 1 + x - x^2, q(x) = 2 + x^2 + x^3$ in $F[x]$. Calculate $p(x) + q(x)$ and $p(x).q(x)$

Solution: Given $p(x) = 1 + x - x^2, q(x) = 2 + x^2 + x^3$ in F[x].

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

$= (0 + 1)x^3 + (-1 + 1)x^2 + (1 + 0)x + (1 + 2)$

$= x^3 + x + 3$

Now compare $p(x)$ and $q(x)$ with $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m$ and $b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n$ respectively.

So we have $a_0 = 1, a_1 = 1, a_2 = -1, a_3 = a_4 = \cdots = 0,$ $b_0 = 2,\ b_1 = 0, b_2 = 1, b_3 = 1, and\ b_4 = b_5 = \cdots = 0.$

Now $c_0 = a_0b_0 = 1 \cdot 2 = 2$

$c_1 = a_1b_0 + a_0b_1 = 1 \cdot 2 + 1 \cdot 0 = 2$

$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = (-1)(2) + 1 \cdot 0 + 1 \cdot 1 = -2 + 1 = -1$

$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = 0 \cdot 2 + (-1) \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 2$

$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 0 \cdot 2 + 0 \cdot 0 + (-1) \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 0$

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5$

$= 0 \cdot 2 + 0 \cdot 0 + 0 \cdot 1 + (-1) \cdot 1 + 1 \cdot 0 + 0 \cdot 0 = -1$

$c_6 = a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6$

$= 0 \cdot 2 + 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + (-1) \cdot 0 + 1 \cdot 0 + 1 \cdot 0 = 0$

$c_7 = c_8 = \cdots = 0.$

$\therefore p(x).q(x) = (1 + x - x^2)(2 + x^2 + x^3) = c_0 + c_1x + c_2x^2 + \cdots$

$= 2 + 2x - x^2 + 2x^3 - x^5$

We define $0(x) = 0$, then $0(x)$ is the additive identity or zero element of $F[x]$

i.e, $0(x) + p(x) = 0 + 0x + 0x^2 + \cdots + 0x^n + a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m$

$= a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m$

$\therefore 0(x) + p(x) = p(x) = p(x) + O(x), \forall\ p(x) \in F[x]$

Consider a polynomial $-p(x) = -a_0 + (-a_1)x + (-a_2)x^2 + (-a_3)x^3 + \cdots + (-a_m)x^m$ in $F[x]$.

Now $p(x) + \big(-p(x)\big) = 0(x) = \big(-p(x)\big) + p(x)$. Then $-p(x)$ is the additive inverse polynomial of $p(x)$ in $F[x]$.

Hence $(F[x],+)$ is an abelian group.

By a routine verification, we can understand that the distributive laws hold good. Therefore $(F[x],+,\cdot)$ is a ring. This ring is called the ring of polynomials in the indeterminate x over the given field F.

15.2.4. Self Assessment Question: Consider the ring $R=\{a+b\sqrt{-5}\mid a,b\in Z\}$, two polynomials $f(x)=x^2+(1+\sqrt{-5})x+2+3\sqrt{-5}$ and $g(x)=x^3-(3+7\sqrt{-5})x+(2-3\sqrt{-5})$ over R. Calculate $(f+g)(x)$ and $(fg)(x)$

15.2.5. Definition: If a polynomial $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n$ in $F[x]$ with $a_n\neq 0$ then we say that the degree of $f(x)$ is n written as $deg(f(x))$, is n.
i.e., the degree of $f(x)$ is the largest integer i for which the i^{th} coefficient of $f(x)$ is not 0.

We do not define the degree of the zero polynomial.

A polynomial is said to be constant if its degree is zero.

15.2.6. Definition: A polynomial $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n$ is said to be monic if $a_n=1$.

15.2.7. Lemma: If $f(x),\ g(x)$ are two non-zero elements of $F[x]$ then $deg(f(x)g(x))=deg\ (f(x))+deg\ (g(x))$

Proof: Let $f(x),g(x)$ are two non-zero elements of $F[x]$.
Then $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_mx^m$, for some $a_i\in F,\ 1\leq i\leq m$, m is a non-negative integer with $a_m\neq 0$ and $g(x)=b_0+b_1x+b_2x^2+b_3x^3+\cdots+b_nx^n$, for some $b_i\in F,\ 1\leq i\leq n$, n is a non-negative integer with $b_n\neq 0$.
Therefore $deg\ (f(x))=m$ and $deg\ (g(x))=n$.
By definition $f(x).g(x)=c_0+c_1x+c_2x^2+c_3x^3+\cdots+c_tx^t$,
where $c_t=a_tb_0+a_{t-1}b_1+a_{t-2}b_2+\cdots+a_0b_t$.
Now $c_{m+n}=a_{m+n}b_0+a_{m+n-1}b_1+\cdots+a_mb_n+\cdots+a_0b_{m+n}$
Since $a_m\neq 0$ and $b_n\neq 0$, we have $a_mb_n\neq 0$.

$\Rightarrow c_{m+n}\neq 0$
$\Rightarrow deg(f(x)g(x))=\ c_{m+n}=\deg\ (f(x))+deg(g(x))$
$\therefore deg(f(x)g(x))=\deg\ (f(x))+deg(g(x))$

15.2.8. Corollary: If $f(x),g(x)$ are two non-zero elements in $F[x]$ then $deg\ (f(x))\leq deg\ (f(x)).deg\ (g(x))$

Proof: By the above lemma, we have $deg(f(x)g(x))=\deg\ (f(x))+deg(g(x))$
Then $deg\ (f(x))\leq deg\ (f(x))+deg\ (g(x))=deg(f(x)).deg\ (g(x))$
$\therefore deg\ (f(x))\leq deg\ (f(x)).deg\ (g(x))$

15.2.9. Corollary: $F[x]$ is an integral domain.

Proof: Clearly $F[x]$ is a commutative ring.
Claim: $F[x]$ is an integral domain, *i.e.* it has no non zero divisors.
Consider the polynomials $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots+a_mx^m$, for some $a_i\in F,\ 1\leq i\leq m$, m is a non-negative integer with $a_m\neq 0$ and

$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n$, for some $b_i \in F, 1 \leq i \leq n$, n is a non-negative integer with $b_n \neq 0$.
$\Rightarrow f(x)g(x) \neq 0 \Rightarrow F[x]$ has no non zero divisors.
$\Rightarrow F[x]$ is an integral domain.

15.2.10. Definition: Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. We say that $g(x)$ divides $f(x)$ if there exists $a(x) \in F[x]$ such that $f(x) = a(x)g(x)$. $g(x)$ divides $f(x)$ written as $g(x)/f(x)$.

15.2.11. Note: Let F be a field. By the above corollary, it follows that $F[x]$ is an integral domain. The field F^* of quotients of $F[x]$ is called the field of rational functions in x over F.

15.2.12. Lemma: (**The division algorithm**) Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)t(x) + r(x)$ where $r(x) = 0$ or $deg\ (r(x)) < deg\ (g(x))$.

Proof: Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m$ with $a_m \neq 0$ and $g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n$ with $b_n \neq 0$. Then $deg\ (f(x)) = m$ and $deg\ (g(x)) = n$.
If $m < n$ or $f(x) = 0$, there is nothing to prove.
Suppose $m \geq n$.
Let $f_1(x) = f(x) - \left(\frac{a_m}{b_n}\right)x^{m-n}g(x)$
Then
$f_1(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m - \left(\frac{a_m}{b_n}\right)x^{m-n}(b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n)$

$\therefore deg\ f_1(x) \leq m - 1$
Then by induction on the degree of $f(x)$, we can assume that
$f_1(x) = t_1(x)g(x) + r(x)$, where $r(x) = 0$ or $deg\ (r(x)) < deg\ (g(x))$
$\Rightarrow f(x) - \left(\frac{a_m}{b_n}\right)x^{m-n}g(x) = t_1(x)g(x) + r(x)$
$\Rightarrow f(x) = \left(\frac{a_m}{b_n}\right)x^{m-n}g(x) + t_1(x)g(x) + r(x)$
$\Rightarrow f(x) = \left(\left(\frac{a_m}{b_n}\right)x^{m-n} + t_1(x)\right)g(x) + r(x)$
Here $r(x) = 0$ or $deg\ (r(x)) < deg\ (g(x))$

15.2.13. Theorem: $F[x]$ is a Euclidean ring

Proof: By the corollary 15.2.9, we have that $F[x]$ is an integral domain.
Let $f(x) \in F[x]$ with $f(x) \neq 0$
Take $deg\ (f(x)) = d(f(x))$

(i) Clearly, $d(f(x)) \geq 0$, for all non-zero polynomial $f(x)$ in $F[x]$
(ii) $d(f(x)) \leq d(f(x)g(x))$, for all non-zero polynomial $g(x)$ in $F[x]$
(iii) Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$

Then by the division algorithm, there exists two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)t(x) + r(x)$, where $r(x) = 0$ or $deg\ (r(x)) < deg\ (g(x))$.

$\therefore F[x]$ is an Euclidean ring.

15.2.14. Lemma: $F[x]$ is a principal ideal ring.

Proof: We have that every Euclidean ring is a principal ideal ring.
Hence $F[x]$ is a principal ideal ring.

15.2.15. Definition: Consider any two polynomials $f(x)$ and $g(x)$ in $F[x]$ not both zero. We say that the non zero polynomial $d(x) \in F[x]$ is the greatest common divisor of $f(x)$ and $g(x)$ if

(i) $d(x)/f(x)$ and $d(x)/g(x)$
(ii) If $h(x)/f(x)$ and $h(x)/g(x)$ then $h(x)/d(x)$

15.2.16. Lemma: Given two polynomials $f(x), g(x)$ in $F[x]$ they have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x)f(x) + \mu(x)g(x)$

Proof: We have $F[x]$ is an Euclidean ring.
Let R be an Euclidean ring. Then any two elements $a, b \in R$ have a greatest common divisor d. Moreover the gcd is of the form $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.
Hence the gcd of $f(x), g(x)$ is of the form $d(x) = \lambda(x)f(x) + \mu(x)g(x)$, for some $\lambda(x), \mu(x) \in F[x]$.

15.3. IRREDUCIBLE POLYNOMIALS:

15.3.1. Definition: A polynomial $p(x)$ in $F[x]$ is said to be irreducible over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0. (i.e. it is constant).

15.3.2. Example: Consider $x^2 + 1 = (x + i)(x - i)$ (Here $i^2 = -1$)
Then $x = a$ or $x = b$ is a root of $x^2 + 1$
$a^2 + 1 = 0$ or $b^2 + 1 = 0 \Rightarrow a^2 = -1$ or $b^2 = -1$
This can not be true for any real numbers $a, b \in R$.
$\therefore x^2 + 1$ is irreducible over R.
In the set C of complex numbers, consider $x^2 + 1 = (x + i)(x - i)$.
Then $deg(x + i) = 1 \neq 0$ and $deg(x - i) = 1 \neq 0$
Therefore $x^2 + 1$ is not an irreducible polynomial over C.

15.3.3. Lemma: Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.

Proof: Let $f(x) \in F[x]$
Suppose $f(x)$ is a unit polynomial.
Then $f(x)$ is an irreducible polynomial.
Hence $f(x)$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.
Suppose $f(x)$ is not unit polynomial.
By unique factorization theorem, $f(x)$ can be written as a product of prime elements in a unique way.

Since every prime element is an irreducible element. We have that $f(x)$ can be written as product of irreducible elements in a unique manner.

15.3.4. Lemma: The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.

Proof: Assume that $A = (p(x))$ is a maximal ideal of $F[x]$.
Now we prove that $p(x)$ is irreducible over F
Suppose that $p(x)$ is not irreducible over F.
$i.e. p(x) = a(x)b(x)$, where $a(x), b(x) \in F[x]$ and $deg\ (a(x)) > 0$ and $deg\ (b(x)) > 0$.
Take $B = (b(x))$
Clearly, we have that $(p(x)) \subseteq (b(x)) \subseteq F[x]$
If $(p(x)) = (b(x))$, then $b(x) \in (p(x))$
$\Rightarrow b(x) = p(x)g(x)$, for some $g(x) \in F[x]$
$\Rightarrow a(x).b(x) = a(x).p(x)g(x)$
$\Rightarrow a(x).g(x) = 1$, which is a contradiction
$\therefore (p(x)) \neq (b(x))$
Clearly, every constant polynomial of $F[x]$ is not in $(b(x))$
$\therefore (p(x)) \subset (b(x)) \subset F[x]$, which is a contradiction
$\therefore p(x)$ is irreducible polynomial over F.
Conversely, assume that $p(x)$ is irreducible polynomial over F
We prove that $(p(x)) = A$ is maximal.
Let $(u(x))$ be any ideal of $F[x]$ with $(p(x)) \subseteq (u(x))$
Then $p(x) \in (u(x))$
$\Rightarrow p(x) = u(x)u'(x)$, for some $u'(x) \in F[x]$
Since $p(x)$ is irreducible, we get that $deg\ (u(x)) = 0$ or $deg\ (u'(x)) = 0$
Suppose $\deg\ (u(x)) = 0$.
i.e. $u(x)$ is a constant polynomial of $F[x]$.
Then $1 \in (u(x))$
$\Rightarrow q(x)\ 1 \in (u(x)),\ \forall\ q(x) \in F[x]$ (Since $u(x)$ is an identity of $F[x]$)
$\Rightarrow q(x) \in (u(x)), \quad \forall q(x) \in F[x]$
Hence $(u(x)) = F[x]$
Therefore $(p(x))$ is maximal.
Suppose $\deg(u'(x)) = 0$.
Now $p(x) = u(x)u'(x)$
$p(x) = u(x)a$, where take $u'(x) = a$
$\Rightarrow p(x) = a.u(x)$
$\Rightarrow a^{-1}p(x) = u(x)$
$\Rightarrow u(x) \in (p(x))$
$\Rightarrow (u(x)) \subseteq (p(x))$
$\Rightarrow (u(x)) = (p(x))$
Hence $(p(x))$ is a maximal ideal of $F[x]$.

15.3.5. Self Assessment Question: (i) If $p(x)$ is an irreducible element in $F[x]$, then show that $p(x)$ is either a unit or a prime element in the Euclidean domain $F[x]$.
(ii). Observe that every prime element is an irreducible element.

15.4. MODEL EXAMINATION QUESTIONS:

15.4.1. Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$ where F is a field. Then prove that there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

15.4.2. Suppose that F is a field and $p(x) \in F[x]$. Then the ideal generated by $p(x)$, that is, $(p(x))$ in $F[x]$ is a maximal ideal of $F[x] \Leftrightarrow p(x)$ is irreducible in $F[x]$.

15.5 SUMMARY:

The abstract algebraic concepts and operations like polynomials, equality of polynomials, multiplication, degree, irreducibility and the ring of polynomials are introduced. We proved that $F[x]$, the ring of polynomials over a field F, is an integral domain. We deduced the division algorithm. $F[x]$ is a Euclidean ring. $F[x]$ is also a principal ideal domain ring. The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.

15.6 TECHNICAL TERMS:

Polynomial: Let F be a field, x an intermediate. Write
$F[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \mid n \text{ is a positive integer}, a_i \in F, 1 \le i \le n \right\}$. Each element of $F[x]$ is called polynomial with coefficients from F.

Constant polynomial: A polynomial with zero degree is called a constant polynomial.

Division Algorithm: Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

Irreducible polynomial: A polynomial $p(x) \in F[x]$ is irreducible if $p(x)$ is of positive degree and given any polynomial $f(x)$ in $F[x]$, then either $p(x) \setminus f(x)$ or $p(x)$ is relatively prime to $f(x)$.

15.7 ANSWERS TO SELF ASSESSMENT QUESTIONS:

15.2.4.

(i) $(f+g)(x) = \{x^2 + (1+\sqrt{-5})x + 2 + 3\sqrt{-5}\} + \{x^3 - (3+7\sqrt{-5})x + (2-3\sqrt{-5})\}$
$= x^3 + x^2 - (2+6\sqrt{-5})x + 4$

(ii) $(fg)(x) = \{x^2 + (1+\sqrt{-5})x + 2 + 3\sqrt{-5}\}\{x^3 - (3+7\sqrt{-5})x + (2-3\sqrt{-5})\}$
$= x^5 + (1+\sqrt{-5})x^4 - (1+4\sqrt{-5})x^3 + (34-13\sqrt{-5})x^2 + (116-24\sqrt{-5})x + 49.$

15.3.5. (i) Suppose that $p(x)$ is an irreducible element in $F[x]$ which is not a unit. We have to show that $p(x)$ is a prime element in $F[x]$. For this, suppose that $p(x) = a(x)b(x)$. Since $p(x)$ is irreducible, we have that either $deg(a(x)) = 0$ or $deg(b(x)) = 0$. This implies that either $a(x)$ is constant or $b(x)$ is constant, and so either $a(x)$ is a unit or $b(x)$ is unit. This shows that every irreducible element in $F[x]$ is either a unit or a prime element.

(ii) From the definitions of prime element and irreducible element, it is clear that every prime element is an irreducible element.

15.8 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-Dr. Noorbhasha Rafi

LESSON -16

POLYNOMIALS OVER THE RATIONAL FIELD

OBJECTIVES:

The objectives of this lesson are to

- Define primitive polynomial, content of a polynomial, integer monic polynomial
- State and prove Gauss lemma.

STRUCTURE:

16.1. INTRODUCTION:

We define the concepts: primitive polynomial, content of a polynomial and integer monic polynomial. We state and prove Gauss lemma.

16.2. POLYNOMIALS OVER THE RATIONAL FIELD

16.2.1. Definition: The polynomial $f(x) = a_0 + a_1x+\ldots+a_nx^n$, where $a_0, a_1, \ldots, a_n$ are integers is said to be primitive if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

16.2.2. Lemma: If $f(x)$ and $g(x)$ are primitive polynomials then $f(x)g(x)$ is a primitive polynomial.

Proof: Consider the polynomials $f(x) = a_0 + a_1x+\ldots+a_nx^n$ and $g(x) = b_0x+\ldots+b_nx^n$.
Suppose $f(x)$ and $g(x)$ are primitive polynomials.
Then gcd$\{a_0, a_1, \ldots, a_n\}$=1 and gcd$\{b_0, b_1, \ldots, b_n\}$=1.
Now $f(x)g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k$, where $c_k = a_kb_0 + a_{k-1}b_1+\ldots+a_0b_k$
Now we prove that gcd$\{c_0, c_1, \ldots, c_k\}$=1
Suppose gcd$\{c_0, c_1, \ldots, c_k\} \neq 1$. Then choose a prime number p >1 such that gcd$\{c_0, c_1, \ldots, c_k\}$ = p. Then p/c_i, for $0 \le i \le k$.
Suppose p/a_i, for $0 \le i \le n$, we get gcd$\{a_0, a_1, \ldots, a_n\}$=1, which is a contradiction.
$\therefore p \nmid a_j$, for some $j, 0 \le j \le n$.
By similar argument, we get $p \nmid b_k$, for some $k, 0 \le k \le m$
$\Rightarrow p \nmid a_jb_k$.
Now $c_{j+k} = a_{j+k}b_0 + a_{j+k-1}b_1 + a_{j+k-2}b_2 + \ldots + a_jb_k + \ldots + a_0b_{j+k}$
Since $p \nmid a_jb_k$, we get $p \nmid c_{j+k}$, which is a contradiction to p/c_i for $0 \le i \le k$.
$\therefore \ gcd\{c_0, c_1, \ldots, c_k\} = 1$
Hence $f(x)g(x)$ is a primitive polynomial.

16.2.3. Definition: The content of the polynomial $(x) = a_0 + a_1x + \cdots + a_nx^n$, where the $a_i's$ are integers, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

16.2.4. NOTE: 1. Any polynomial $p(x)$ with integer coefficients can be written as $p(x) = dq(x)$, where d is the content of $p(x)$ and $q(x)$ is a primitive polynomial.
2. The content of every primitive polynomial is 1.

16.2.5. Theorem (Gauss Lemma): If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.

Proof: Assume that the primitive polynomial $f(x)$ can be factored as the product of two polynomials $u(x)$ and $v(x)$ having rational coefficients.
i.e $f(x) = u(x)v(x)$, where $u(x)$ and $v(x)$ have rational coefficients.

The coefficients of $u(x)$ and $v(x)$ can be written as $u(x) = \frac{a_1}{b_1}\lambda(x)$ and $v(x) = \frac{a_2}{b_2}\mu(x)$, where $\lambda(x)$ and $\mu(x)$ are primitive polynomials with integer coefficients.

Now $f(x) = \frac{a_1}{b_1}\lambda(x)\frac{a_2}{b_2}\mu(x) = \frac{a_1a_2}{b_1b_2}\lambda(x)\mu(x)$

Take $a = a_1a_2$ and $b = b_1b_2$. So $f(x) = \frac{a}{b}\lambda(x)\mu(x) \Rightarrow bf(x) = a\lambda(x)\mu(x)$

Since $f(x)$ is primitive, the content of $f(x)$ is 1 and hence the content of $bf(x)$ is b.
By known result, $\lambda(x)\mu(x)$ is primitive.
$\Rightarrow$ the content of $\lambda(x)\mu(x)$ is 1 and the content of $a\,\lambda(x)\mu(x)$ is a.
Therefore $a = b$ and hence $f(x) = \lambda(x)\mu(x)$, where $\lambda(x)$ and $\mu(x)$ having integer coefficients.

16.2.6. Definition: A polynomial is said to be integer monic if all its coefficients are integers and it's highest is 1.

16.2.7. Note: Every integer monic polynomial is primitive but converse is not true.

16.2.8. Corollary: If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.

Proof: By the above note, the Gauss lemma is valid to this corollary.

16.2.9. Self assessment Question: Prove that the polynomial $x^3 - 9$ is an irreducible polynomial over the field $Z_{31} = \{0,1, \ldots, 30\}$ of the integers modulo 31.

16.3. MODEL EXAMINATION QUESTIONS:

16.3.1. Define the term 'primitive polynomial'. If $f(x)$ and $g(x)$ are primitive polynomials then show that $f(x)g(x)$ is also a primitive polynomial.
16.3.2. State and prove Gauss Lemma
16.3.3. Prove that $x^2 + x + 1$ is an irreducible polynomial over the field of integers modulo 2.
16.3.4. Prove that the polynomial $x^3 - 9$ is an irreducible polynomial over the field $Z_{31}$of integers modulo 31.

16.4 SUMMARY:

We introduced some concepts like primitive polynomial, content of a polynomial, integer monic polynomial. We proved that the product of two primitive polynomials is also a primitive. Gauss lemma was proved.

16.5 TECHNICAL TERMS:

Primitive polynomial: A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $a_0, a_1, \ldots, a_n$ are integers, is said to be primitive if g.c.d$\{a_0, a_1, \ldots, a_n\} = 1$.

Content: If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $a_0, a_1, \ldots, a_n$ are integers, then the g.c.d of $a_0, a_1, \ldots, a_n$ is called the content of $f(x)$.

Monic polynomial: A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is said to be monic if $a_n = 1$.

Integer Monic: A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is said to be integer monic if $a_0, a_1, \ldots, a_n$ are integers and $a_n = 1$.

16.6 ANSWERS TO SELF ASSESSMENT QUESTIONS:

16.2.9. In a contrary way, suppose that the polynomial $x^3 - 9$ is not an irreducible polynomial over the field $Z_{31} = \{0,1,2, \ldots,30\}$. Then $x^3 - 9 = f(x)g(x)$ for some polynomials $f(x)$ and $g(x)$ over Z_{31}. Now either $f(x)$ or $g(x)$ is of degree 1. Suppose $deg(f(x)) = 1$. Since $f(x) = x - \alpha$ is a factor of $x^3 - 9$, the polynomial $x^3 - 9$ has root in Z_{31}. For some $0 < x < 31$, we have $x^3 - 9 = 0 \Rightarrow x^3 \equiv 9(mod\ 31)$ for some $0 < x < 31$. Since 31 is a prime number, the number of integers lies between 0 and 31, which are relatively prime to 31 is 30. So $\phi(31) = 30$ (Euler's function ϕ is used here). [Recall the statement of the Euler's theorem: If a is relatively prime to n, then $a^{\phi(n)} \equiv 1(mod\ n)$ where $\phi(n)$ is the number of non-negative integers $< n$ that are relatively prime to n]. Now 31 is a prime number and $0 < x < 31 \Rightarrow x$ is relatively prime to 31 $\Rightarrow x^{\phi(31)} \equiv 1(mod\ 31) \Rightarrow x^{30} \equiv 1(mod\ 31)$. Already we have $x^3 \equiv 9(mod\ 31) \Rightarrow x^{30} \equiv 9^{10}(mod\ 31)$. By transitive property we get $9^{10} \equiv 1\ (mod\ 31) \Rightarrow 3^{20} \equiv 1(mod\ 31)$. Since 3 is relatively prime to 31 we have $3^{30} \equiv 1(mod\ 31)$ (by Euler theorem). Now $3^{20} \equiv 1, (mod\ 31) 3^{30} \equiv 1\ (mod\ 31) \Rightarrow 3^{30} \equiv 3^{20}(mod\ 31)$ (by transitive) $\Rightarrow 31 \backslash 3^{20}(3^{10} - 1) \Rightarrow 31 \backslash 3^{20}$ or $31 \backslash (3^{10} - 1)$. Since 31 cannot divide 3^{20} (otherwise 31 \ 3 since 31 is prime), it follows that 31 divides $(3^{10} - 1) = 58049 - 1 = 58048$, a contradiction (since $58048 = (1904)(31) + 24$). This shows that $x^3 - 9$ is irreducible over Z_{31}.

16.7 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-Dr. Noorbhasha Rafi

LESSON - 17

POLYNOMIAL RINGS OVER COMMUTATIVE RINGS

OBJECTIVES:

The objectives of the lesson are to

- state and prove Eisenstein criterion
- apply the Eisenstein criterion to find the irreducibility of a given polynomial.
- define the concepts like: polynomial ring $R[x_1, x_2, \ldots x_n]$ over a given ring R in n-variables, field of rational functions, unique factorization domain.
- find the influence of the structure of R on that of $R[x_1, x_2, \ldots x_n]$
- apply the Gauss lemma to the ring $R[x]$, where R is the unique factorization domain.
- prove some basic theorems and lemmas

STRUCTURE:

17.1. INTRODUCTION:

We continue the study of polynomials. We state and prove Eisenstein criterion. We use the Eisenstein criterion in verifying whether a given polynomial is irreducible. We define $R[x]$, the polynomial ring in x over R. $R[x_1, x_2, \ldots, x_n]$ the ring of polynomials in n variables $x_1, x_2, \ldots, x_n$ over R. We study the influence of the structure of R on that of $R[x_1, x_2, \ldots, x_n]$. We define unique factorization domain. If R is an unique factorization domain then so is $R[x]$. Then we are able to extend this to $R[x_1, x_2, \ldots, x_n]$ by using mathematical induction. Also we prove that if F is a field, then $F[x_1, x_2, \ldots, x_n]$ is a unique factorization domain.

17.2. THE EISENSTEIN CRITERIAN PRINCIPLE

17.2.1. Theorem (The Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p, $p \nmid a_n$, p / a_1, $p / a_2, \ldots$, p / a_0, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over the rationals.

Proof: Suppose there is a prime number p such that $p \nmid a_n$, p / a_1, $p / a_2, \ldots$, p / a_0 and $p^2 \nmid a_0$.
Without loss of generality, we can assume that $f(x)$ is a primitive polynomial.
By Gauss Lemma, $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.
We prove that $f(x)$ is irreducible over the rationals.
If f(x) is reducible, then $f(x) = g(x)h(x)$, where $g(x) = b_0 + b_1x + \ldots + b_rx^r$,

$h(x) = c_0 + c_1x + ... + c_sx^s$ and $deg\ g(x) > 0$ and $deg\ h(x) > 0$, where b's and c's are integers.

Here $a_0 = b_0c_0$

Since p / a_0, we get p / b_0c_0.

Since p is prime, we get either p / b_0 or p / c_0 or both.

If p / b_0 and p / c_0, then p^2 / b_0c_0

$\Rightarrow p^2 / a_0$, which is a contradiction to $p^2 \nmid a_0$

$\Rightarrow$ either $p \nmid b_0$ or $p \nmid c_0$

Suppose p / b_0 and $p \nmid c_0$.

Since $f(x)$ is primitive, we get that $g(x)$ is primitive.

$\Rightarrow p \nmid b_k$, for some $k, 1 \le k \le r$

We have that $a_k = b_kc_0 + b_{k-1}c_1 + ... + b_0c_k$.

Since $p \nmid c_0$ and $p \nmid b_k$, we get $p \nmid b_kc_0$

$\Rightarrow p \nmid a_k$, which is a contradiction to p / a_k.

$\therefore f(x)$ is irreducible over rationals.

Suppose p / c_0 and $p \nmid b_0$.

Since $f(x)$ is primitive, we get $h(x)$ is primitive.

$\Rightarrow p \nmid c_k$, for some $k, 1 \le k \le s$

We have $a_k = b_kc_0 + b_{k-1}c_1 + ... + b_0c_k$.

Since $p \nmid c_k$ and $p \nmid b_0$, we get $p \nmid b_0c_k$.

$\Rightarrow p \nmid a_k$, which is a contradiction to p / a_k.

$\therefore f(x)$ is irreducible over rationals.

17.2.2. Problem: If p is a prime number, then prove that the polynomial $x^n - p$ is irreducible over the field of rational numbers.

Solution: Suppose $x^n - p = a_0 + a_1x + \cdots + a_nx^n$, where $a_i = 0$ for $1 \le i \le (n-1)$ and $a_n = 1, a_0 = p$. Now p divides a_i for $0 \le i \le n-1; p$ do not divide a_n; and p^2 does not divide a_0. By applying the Theorem 17.2.1(Eisenstein Criterion), we can conclude that the polynomial $x^n - p$ is irreducible over the field of rational numbers.

17.2.3. Problem: Prove that the polynomial $1 + x + \cdots + x^{(p-1)}$, where p is a prime number, is irreducible over the field of rationals.

Solution: Here we consider the polynomial $1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1}$ and use the Eisenstein Criterion.

We know that

$1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1} = 1 + (x+1) + (x^2 + 2x + 1) + \cdots +$

$(x+1)^{p-1} = p + [1 + 2 + \cdots + (p-1)]x + [1 + 3 + \cdots + (p-2)]x^2 + \cdots + x^{(p-1)} =$

$p + \left[\frac{(p-1)p}{2}\right]x + \cdots + x^{(p-1)} = a_0 + a_1x + \cdots + a_{p-1}x^{(p-1)}$

Where $a_0 = p, a_1 = \frac{p(p-1)}{2}, \ldots, a_{p-1} = 1.$

Clearly, $p|a_0$, $p|a_{1,\ldots}$ and p does not divide a_{p-1}. Also p^2 does not divide a_0. Hence by Theorem 17.2.1(Eisenstein Criterion), we conclude that $1+(x+1)+(x+1)^2+\cdots+(x+1)^{p-1}$ is irreducible over the field of rational numbers. Hence $1+x+\cdots+x^{(p-1)}$, where p is a prime number, is irreducible over the field of rationals.

17.3. POLYNOMIAL RINGS OVER COMMUTATIVE RINGS:

17.3.1. Definition: Let R be a commutative ring with unit element 1.

(i) The polynomial ring in x over R is denoted by $R[x]$ and it is defined as

$R[x]=\{a_0+a_1x+\cdots+a_mx^m/a_i\in R, 0\le i\le m\}$.

The equality, addition (+), and multiplication (.) are defined same as in polynomials over fields. Hence it is easy to verify that $(R[x],+,.)$ is a commutative ring with unit element.

(ii) The ring of polynomials in the n variables $x_1,x_2,\ldots,x_n$ over R is denoted by $R[x_1,x_2,\ldots,x_n]$ and defined as follows $R_1=R[x_1],R_2=R_1[x_2],R_3=R_2[x_3],\ldots,R_n=R_{n-1}[x_n]$. R_n is called the ring of polynomials in $x_1,x_2,\ldots,x_n$ over R. Its elements are of the form $\sum a_{i_1i_2\ldots i_n}x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$ where equality and addition are defined coefficient wise and where multiplication is defined by use of the distributive law and the rule of exponents

$\left(x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}\right)\left(x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}\right)=x_1^{i_1+j_1}x_2^{i_2+j_2}\ldots x_n^{i_n+j_n}$

17.3.2. Lemma : (i) If R is a commutative ring with identity, then so is $R[x]$

(ii) If R is an integral domain, then so is $R[x]$

Proof: (i) We have that $R[x]$ is a ring.

Clearly $1=0+0x+\cdots+0x^n$ is the identity element of $R[x]$.

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

Then $f(x)=a_0+a_1x+\cdots+a_nx^n$, where $a_i\in R, 0\le i\le n$

$g(x)=b_0+b_1x+\cdots+b_mx^m$, where $b_j\in R, 0\le j\le m$

We prove that $f(x)g(x)=g(x)f(x)$

$f(x)g(x)=(a_0+a_1x+\cdots+a_nx^n)(b_0+b_1x+\cdots+b_mx^m)$

$=c_0+c_1x+\cdots+c_{m+n}x^{m+n}, where\ c_i=\sum_{t=0}^{i}a_tb_{i-t}$

Now

$g(x)f(x)=(b_0+b_1x+\cdots+b_mx^m)(a_0+a_1x+\cdots+a_nx^n)$

$=d_0+d_1x+\cdots+d_{m+n}x^{m+n}, where\ d_i=\sum_{t=0}^{i}b_ta_{i-t}$

Since R is commutative, we have that

$$d_i=\sum_{t=0}^{i}b_ta_{i-t}=\sum_{t=0}^{i}a_tb_{i-t}=c_i\ for\ all\ 1\le i\le m+n$$

$\therefore f(x)g(x)=g(x)f(x)\ for\ all\ f(x),g(x)\in R[x]$.

Hence $R[x]$ is a commutative ring with identity.

(ii) Let $f(x),g(x)\in R[x]$with $f(x)\neq 0$ and $g(x)\neq 0$

Then $f(x)=a_0+a_1x+\cdots+a_mx^m$, where $a_m\neq 0$

$g(x)=b_0+b_1x+\cdots+b_nx^n$, where $b_n\neq 0$

Now

$$f(x)g(x) = (a_0 + a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_nx^n)$$
$$= c_0 + c_1x + \cdots + c_{m+n}x^{m+n}, where\ c_i = \sum_{t=0}^{k} a_{k-i}b_i$$

Now $c_{m+n} = a_{m+n}b_0 + \cdots + a_mb_n + \cdots + a_0b_{m+n}$

Since $a_m \neq 0$ and $b_n \neq 0$ and R is an integral domain, we get that $a_mb_n \neq 0$ and hence $c_{m+n} \neq 0$

$\therefore f(x)g(x) \neq 0$

Thus $R[x]$ is an integral domain.

17.3.3. Corollary: (i) If R is a commutative ring with identity, then so is $R[x_1, x_2, \ldots, x_n]$

(ii) If R is an integral domain, then so is $R[x_1, x_2, \ldots, x_n]$

Proof: (i) Let R be a commutative ring with identity

Now we prove this by induction on n.

Suppose $n = 1$, then by Lemma 17.3.2, we have that $R[x_1]$ is a commutative ring with identity 1.

Suppose the result is true for $n - 1$

That means $R_{n-1} = R[x_1, x_2, \ldots, x_{n-1}]$ is a commutative ring with identity 1.

Then by Lemma 17.3.2.(i), $R_{n-1}$is a commutative ring with identity 1, we get that $R_n = R_{n-1}[x_n]$ (i.e. $R_n = R[x_1, x_2, \ldots, x_n]$) is a commutative ring with identity 1.

(ii) Let R be an integral domain

We prove this also by induction on n.

Suppose $n = 1$, then by Lemma 17.3.2.(ii), we have that $R[x_1]$ is an integral domain.

Assume the result is true for $n - 1$

That means $R_{n-1} = R[x_1, x_2, \ldots, x_{n-1}]$ is an integral domain

That implies again by Lemma 17.3.2.(ii), we get that $R_n = R_{n-1}[x_n]$ (i.e. $R_n = R[x_1, x_2, \ldots, x_n]$) is an integral domain.

In particular, when F is a field $F[x_1, x_2, \ldots, x_n]$ must be an integral domain. As such we can construct its field of quotients; we call this the field of rational functions in $x_1, x_2, \ldots, x_n$ over the field F and denote it by $F(x_1, x_2, \ldots, x_n)$.

17.3.4. Definition: Let R be an integral domain with unit element 1.

(i) An element $x \in R$ is said to be a unit in R if $xy = 1$, for some $y \in R$.

(ii) Two elements a, b in R are said to be associates if $a = ub$, where u is a unit element in R.

(iii) An element $a \in R$ which is not a unit element of R, will be called irreducible (or a prime element) if , when ever $a = bc$ with b, c both in R, then one of b or c must be a unit element in R.

17.3.5. Definition: An integral domain R with unit element is said to be a unique factorization domain if

(i) Any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R.

(ii) The decomposition in part (i) is unique up to the order and associates of the irreducible elements.

i.e. If $a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$, where $p_i's$ and $q_j's$ are irreducible elements $(1 \le i \le n \text{ and } 1 \le j \le m)$, then $m = n$ and for each i, there corresponds j such that p_i and q_j are associates.

17.3.6. Lemma : If R is a unique factorization domain and if a, b are in R, then a and b have a greatest common divisor (a, b) in R. More over, if a and b are relatively prime $(i.e.(a, b) = 1)$, whenever a/bc then a/c.

Proof: Let R is a unique factorization domain and if a, b are in R
Then we can write $a = p_1p_2 \ldots p_n$, $b = q_1q_2 \ldots q_m$ where $p_i's$ and $q_j's$ are irreducible elements for $1 \le i \le n \text{ and } 1 \le j \le m$.
Without loss of generality we can assume that $n \le m$.
Now we prove this result by using induction on $'n'$
Suppose $n = 1$, then $a = p_1$
If there is j $(1 \le j \le m)$ such that p_1 is an associate of q_j then $(a, b) = p_1$.
If there is no j $(1 \le j \le m)$ such that p_1 is an associate of q_j then $(a, b) = 1$.
Hence the gcd of a and b exists for $n = 1$
Assume the result is true for $n = k - 1$
Now we prove this result is true for $n = k$
Suppose $a = p_1p_2 \ldots p_k$
Take $a' = p_1p_2 \ldots p_{k-1}$. Then $a = p_1p_2 \ldots p_k = a'p_k$.
By the induction hypothesis, the gcd of a' and b exists.
Let $(a', b) = d$
If there is j $(1 \le j \le m)$ such that p_k is an associate of q_j then $(a, b) = dp_k$.
Hence gcd exists for a and b.
Let $a, b, c \in R$ with $(a, b) = 1$ and a/bc.
Since R is a unique factorization domain, we can write
$a = p_1p_2 \ldots p_n$
$b = q_1q_2 \ldots q_m$
$c = r_1r_2 \ldots r_s$, where $p_i's, q_j's$ and $r_k's$ are irreducible elements for $1 \le i \le n$, $1 \le j \le m, 1 \le k \le s$.
Since a/bc, there exists $x \in R$ such that $bc = ax$.
$\Rightarrow (q_1q_2 \ldots q_m)(r_1r_2 \ldots r_s) = (p_1p_2 \ldots p_n)x$
Since R is a unique factorization domain and p_i $(1 \le i \le n)$, we have that p_i is associate of either q_j or r_k, for some $1 \le j \le m$ or $1 \le k \le s$.
Suppose that p_i is associate of $q_{j,}$ then p_i/a and p_i/b
Since $(a, b) = 1$, we get that $p_i = 1$, which is a contradiction to irreducible element p_i.
$\therefore p_i$ is not an associate of q_j, for all $1 \le j \le m$.
Hence p_i is an associate of r_{k_j}, for some $1 \le k_j \le s$

$$\Rightarrow \frac{p_1}{r_{k_1}}\frac{p_2}{r_{k_2}} \ldots \frac{p_n}{r_{k_n}}$$

$$\Rightarrow \frac{a}{r_{k_1}r_{k_2} \ldots r_{k_n}}$$

$$\Rightarrow a/c$$

17.3.7. Corollary: If $a \in R$ is an irreducible element and a/bc then a/b or a/c.

Proof: Let a be an irreducible element of R and a/bc.
We prove that a/b or a/c
Suppose a does not divides b
Since a is irreducible and a does not divides b, we get that $(a,b)=1$
By the above result we get that a/c.

17.3.8. Definition: Let R be a unique factorization domain.

(i) The content of given polynomial $f(x)=a_0+a_1x+\cdots+a_mx^m$ in $R[x]$ is defined to be the gcd of $a_0,a_1,\ldots,a_m$. We denote the content of $f(x)$ by $c(f)$.
(ii) Given polynomial $f(x)=a_0+a_1x+\cdots+a_mx^m$ in $R[x]$ is said to be primitive if $c(f)=1$

17.3.9. Self Assessment Question: Let $f(x)\in R[x]$. Then there exist a primitive polynomial $f_1(x)\in R[x]$ such that $f(x)=af_1(x)$, where $a=c(f)$.

17.3.10. Lemma : If R is a unique factorization domain, then the product of two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$.

Proof: By Lemma 16.2.2, we have the proof.

17.3.11. Corollary: If R is a unique factorization domain and if $f(x),g(x)$ are in $R[x]$, then $c(fg)=c(f)c(g)$

Proof: Let $f(x),g(x)$ be in $R[x]$
We can write $f(x)=af_1(x)$ and $g(x)=bg_1(x)$, where $a=c(f)$ and $b=c(g)$, $f_1(x)$ and $g_1(x)$ are primitive polynomials.
By Lemma 17.3.10, $f_1(x)g_1(x)$ is a primitive polynomial. $\Rightarrow c\big(f_1(x)g_1(x)\big)=1$

Now $c\big(f(x)g(x)\big)=c\big(af_1(x)bg_1(x)\big)$
$=c(ab\,f_1(x)\,g_1(x))$
$=ab\,c(f_1(x)g_1(x))$
$=ab.1$
$=ab$
$=c\big(f(x)\big)c(g(x))$.

17.3.12. Self Assessment Question: If R is a unique factorization domain and if $f_i(x)\in R[x], 1\le i\le k$, then $c(f_1f_2\ldots f_k)=c(f_1)c(f_2)\ldots c(f_k)$

17.3.13. Notation: Hence forth, we consider R to be a unique factorization domain. Since it is an integral domain, we have that R can be embedded in a field F (called the field of quotients of R)

(i) If we take a polynomial $f(x)\in R[x]$ then the coefficients of $f(x)$ are from R. Since $R\subseteq F$, the coefficients of $f(x)$ are from F.
Therefore $f(x)\in F[x]$. Hence $R[x]\subseteq F[x]$
(ii) $R[x],F[x]$ are rings and $R[x]\subseteq F[x]$
$\therefore R[x]$ is a subring of $F[x]$

17.3.14. Self Assessment Question: If $f(x) \in F[x]$ then prove that $f(x) = \frac{1}{a} f_0(x)$, where $f_0(x) \in R[x]$ and $a \in R$.

17.3.15. Lemma : If $f(x)$ in $R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element $f(x)$ in $R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.

Proof: Let $f(x)$ be both primitive and irreducible polynomial of $R[x]$.
Now we prove that $f(x)$ is irreducible as an element of $F[x]$
Suppose $f(x)$ is not irreducible over $F[x]$.
Then $f(x) = g(x)h(x)$, where $g(x), h(x)$ are in $F[x]$ and are of positive degree.
Now $g(x) = \frac{1}{a} g_0(x)$ and $h(x) = \frac{1}{b} h_0(x)$, where $g_0(x), h_0(x) \in R[x]$ and $a, b \in R$
Also $g_0(x) = \alpha g_1(x), h_0(x) = \beta h_1(x)$, where $\alpha = c(g_0)$, $\beta = c(h_0)$ and $g_1(x), h_1(x)$ are primitive in $R[x]$

$$\text{Now } f(x) = g(x)h(x) = \frac{1}{a} g_0(x) \frac{1}{b} h_0(x)$$
$$= \frac{1}{ab} \alpha g_1(x) \beta h_1(x)$$
$$= \frac{\alpha\beta}{ab} g_1(x) h_1(x)$$
$$\Rightarrow abf(x) = \alpha\beta g_1(x) h_1(x)$$

Since $g_1(x), h_1(x)$ are primitive, we have that $g_1(x)h_1(x)$ is primitive and hence the content of the right hand side is $\alpha\beta$.
Since $f(x)$ is primitive, the content of the left hand side is ab.
$\therefore ab = \alpha\beta$
Hence $f(x) = g_1(x)h_1(x)$, which is a contradiction to $f(x)$ is irreducible in $R[x]$
$\therefore f(x)$ is irreducible over $F[x]$.
Conversely, assume that a primitive polynomial $f(x)$ in $R[x]$ is irreducible over $F[x]$.
We prove that $f(x)$ is irreducible over $R[x]$.
Suppose $f(x)$ is not irreducible over $R[x]$.
Then $f(x) = f_1(x)f_2(x)$, where $f_1(x)$, $f_2(x)$ are in $R[x]$ and are of positive degree.
Since $R[x]$ is a subring of $F[x]$ we get that $f(x)$ is not irreducible over $F[x]$, which is a contradiction.
$\therefore f(x)$ is irreducible over $R[x]$.

17.3.16. Lemma : If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$.

Proof: Let R be a unique factorization domain and let $p(x)$ be a primitive polynomial in $R[x]$.
Then $p(x) \in F[x]$. By lemma 15.3.3, we can write $p(x) = p_1(x)p_2(x)\dots p_k(x)$, where $p_1(x), p_2(x), \dots, p_k(x)$ are irreducible polynomials in $F[x]$.
Since $p_i(x) \in F[x]$ for $1 \le i \le k$, we get that $p_i(x) = \frac{1}{a_i} f_i(x)$, where $a_i \in R, f_i(x) \in R[x]$, for $1 \le i \le k$.
Moreover, $f_i(x) = c(f_i)q_i(x)$, where $q_i(x)$ is primitive polynomial in $R[x]$, for $1 \le i \le k$
Now $p(x) = p_1(x)p_2(x)\dots p_k(x)$

$$= \frac{1}{a_1} f_1(x) \frac{1}{a_2} f_2(x) \dots \frac{1}{a_k} f_k(x)$$
$$= \frac{1}{a_1} c(f_1) q_1(x) \frac{1}{a_2} c(f_2) q_2(x) \dots \frac{1}{a_k} c(f_k) q_k(x)$$
$$= \frac{1}{a_1 a_2 \dots a_k} c(f_1) c(f_2) \dots c(f_k)(q_1(x) q_2(x) \dots q_k(x))$$
$$\Rightarrow (a_1 a_2 \dots a_k) p(x) = c(f_1) c(f_2) \dots c(f_k)(q_1(x) q_2(x) \dots q_k(x))$$

By the primitivity of $p(x)$ and of $q_1(x)q_2(x) \dots q_k(x)$, we have the content of left hand side as $a_1 a_2 \dots a_k$ and the content of right hand side as $c(f_1)c(f_2) \dots c(f_k)$ are equal.

$$i.e.\ a_1 a_2 \dots a_k = c(f_1) c(f_2) \dots c(f_k)$$

Hence $p(x) = q_1(x)q_2(x) \dots q_k(x)$, where $q_i(x)$ is irreducible polynomial in $R[x]$.

Uniqueness: Suppose $p(x) = r_1(x)r_2(x) \dots r_m(x)$, where each $r_j(x)$ is irreducible in $R[x]$, for $1 \leq j \leq m$

Since $p(x)$ is primitive, each $r_j(x)$ is primitive in $R[x]$. Since by Lemma 15.3.3, the uniqueness in $F[x]$, we get $q_i(x)$ and $r_j(x)$ are equal (up to associates) in some order.

Hence $p(x)$ has a unique factorization as a product of irreducible in $R[x]$.

17.3.17. Self Assessment Question: Suppose that R is an unique factorization domain. If $a \in R$ is an irreducible element of R, then the constant polynomial defined by $a(x) = a$ is irreducible in $R[x]$.

17.3.18. Theorem: If R is a unique factorization domain then so is $R[x]$.

Proof: Let R is a unique factorization domain.

We prove that $R[x]$ is a unique factorization domain.

Let $f(x) \in R[x]$. We can write $f(x)$ in a unique way as $f(x) = cf_1(x)$, where $c = c(f)$ and $f_1(x)$ is a primitive polynomial in $R[x]$.

By the above lemma, we can decompose $f_1(x)$ in a unique way as $f_1(x) = p_1(x)p_2(x) \dots p_k(x)$, where each $p_i(x)$ is irreducible over $R[x]$, for $1 \leq i \leq k$.

Suppose $c = a_0(x)a_1(x) \dots a_m(x)$ Then

$0 = deg(c) = deg(a_0(x)) + deg(a_1(x)) + \cdots + deg(a_m(x))$

$\Rightarrow deg(a_i(x)) = 0$, for $0 \leq i \leq m$

$\Rightarrow$ each $a_i(x)$ is a constant polynomial, $for\ 0 \leq i \leq m$.

Since $c \in R$ and R is a unique factorization domain. We get that c has a unique factorization.

$\Rightarrow f(x)$ has a unique factorization in $R[x]$.

$\therefore R[x]$ is a unique factorization domain.

17.3.19. Self Assessment Question: If R is a unique factorization domain then so is $R[x_1, x_2, \dots, x_n]$

17.3.20. Self Assessment Question: If F is a field then $F[x_1, x_2, \dots, x_n]$ is a unique factorization domain.

17.4. MODEL EXAMINATION QUESTIONS:

17.4.1. State and prove Eisenstein criterion principle.

17.4.2. Define the concepts 'primitive polynomial' and 'irreducible polynomial'.
If $f(x) \in R[x]$ be a primitive polynomial, then prove that $f(x)$ is irreducible in $R[x] \Leftrightarrow f(x)$ is irreducible in $F[x]$.

17.5 SUMMARY:

We stated and proved the Eisenstein criterion. We used the Eisenstein criterion to find out whether a given polynomial is irreducible. Some abstract algebra concepts like the ring of polynomials in one indeterminate x over a given ring R, the ring of polynomials in the n variables over R, field of rational functions, associates prime element, unique factorization domain, content, primitive are introduced. We proved that if R is an integral domain (respectively, commutative ring with unity 1). Then so is $R[x]$, and we also extended this to $R[x_1, x_2, \dots, x_n]$. If R is a unique factorization domain, then so is $R[x]$, and we also extended this to $R[x_1, x_2, \dots x_n]$. If F is a field, then and we also extended this to $F[x_1, x_2, \dots x_n]$ is a unique factorization domain**.**

17.6 TECHNICAL TERMS:

Field of rational functions: If F is a filed, then $F[x_1, x_2, \dots, x_n]$ is an integral domain. Let $F[x_1, x_2, \dots x_n]$ be the field of quotients of $F[x_1, x_2, \dots, x_n]$. Then $F[x_1, x_2, \dots, x_n]$ is called the field of rational functions in $x_1, x_2, \dots, x_n$ over F.

Unit element: Let R be an integral domain with unit element 1. Then an element $x \in R$ is said to be a unit in R if there corresponds an element $y \in R$ such that $xy = 1$

Associates: Two elements a, b are said to be associates if $a = ub$ for some unit u in R.

Irreducible element: An element $a \in R$ which is not a unit is called irreducible (or a prime element) if whenever $ab = c$ with $b, c \in R$, then either b or c is unit in R.

Unique factorization Domain: An integral domain R with unit element is called a unique factorization domain if

(i) For $0 \neq a \in R, \Rightarrow$ a is a unit, or $a = p_1, p_2, \dots p_n$, where $p_i \in R, 1 \leq i \leq n$ are irreducible elements; and

(ii) If $a = p_1, p_2, \dots, p_n = q_1, q_2, \dots, q_m$ where each p_i and q_i are irreducible elements of R, then $n = m$ and for each $i, (1 \leq i \leq n)$ there corresponds $j, 1 \leq j \leq m$ such that p_i and q_j are associates.

Content: Suppose R is a unique factorization domain. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in R[x]$. The content of $f(x)$ is defined to be a g.c.d. of $a_0, a_1, \dots, a_m$.

Primitive: Suppose R is a unique factorization domain. A polynomial $f(x)$ over R is said to be primitive if $c(f) = 1$.

17.7 ANSWERS TO SELF ASSESSMENT QUESTIONS:

17.3.9: Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$. Since $c(f)$ is a g.c.d of $a_0, a_1, \dots, a_m$, we have that $a_i = c(f).b_i$, for some $b_i \in R$ for $1 \leq i \leq m$, and the g.c.d of $b_0, b_1, \dots, b_m$ is 1.

Now, $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$

$= c(f)b_0 + c(f)b_1x + c(f)b_2x^2 + \cdots + c(f)b_mx^m$

$= c(f)[b_0 + b_1x + b_2x^2 + \cdots + b_mx^m]$

$= a.f_1(x)$ where $f_1(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$

17.3.12: We prove this result by using the principle of mathematical induction on k
If $k = 2$, then the result follows from the corollary 17.3.11.
Now suppose the induction hypothesis that the result is true for $k = n - 1$.
Now consider $c(f_1.f_2.\dots f_n) = c(f_1.f_2.\dots\ f_{n-1}(f_n))$ (by corollary 17.3.11)
$= c(f_1.f_2.\dots\ f_{n-1}).c(f_n)$
$= c(f_1).c(f_2).c(f_3).\dots.c(f_n)$ By induction hypothesis.
This shows that $c(f_1.f_2.\dots f_3) = c(f_1).c(f_2).c(f_3).\dots.c(f_n)$
This completes the proof of the corollary.

17.3.14: Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in F[x]$
We know that $F = \{\frac{p}{q}/p, q \in R \text{ and } q \neq 0\}$
Therefore $a_i = \frac{p_i}{q_i}$ for some $p_i, q_i \in R$ for $1 \leq i \leq n$.
Now $f(x) = \frac{p_0}{q_0} + \frac{p_1}{q_1}.x + \cdots + \frac{p_n}{q_n}x^n$
$= \frac{1}{q_0q_1\dots q_n}[p_0q_1q_2\dots q_n + p_1q_1q_2\dots q_n.x + \cdots + p_nq_1q_2\dots q_nx^n]$
$= \frac{1}{a}f_0(x)$ where $a = q_0q_1q_2\dots q_n \in R$ and
$f_0(x) = p_0q_1q_2\dots q_n + p_1q_1q_2\dots q_n.x + \cdots + p_nq_1q_2\dots q_nx^n \in R[x]$.
This completes the proof.

17.3.17: Suppose that $a(x) = p(x)q(x)$ for two polynomials $p(x)$ and $q(x)$ over R.
Now $0 = \deg(a(x)) = \deg(p(x)) + \deg(q(x)) \Rightarrow \deg(p(x)) = 0 = \deg(q(x)) \Rightarrow p(x)$ and $q(x)$ are constant polynomials.
If $p(x) = p$ and $q(x) = q$, then $a = a(x) = p(x)q(x) = pq$, a contradiction to the fact that a is irreducible in R. Hence $a(x) \in R[x]$ is also irreducible.

17.3.19: We prove this corollary by mathematical induction on n.
If $n = 1$, then by theorem 17.3.18, we get that $R[x_1]$ is an unique factorization domain.
Suppose the induction hypothesis that if R is a unique factorization domain, then R_{n-1} is also a unique factorization domain.
Now by the theorem 17.3.18, we get that $R[x_1, x_2, \dots, x_n] = R_{n-1}[x_n]$ is a unique factorization domain.

17.3.20: Since F is a field, it is an integral domain.
Since every non zero element of F is a unit, we have that F is a unique factorization domain.
Therefore by the self-assessment question 17.3.19, we get that $F[x_1, x_2, \dots, x_n]$ is a unique factorization domain.

17.8 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-Dr. Noorbhasha Rafi

LESSON - 18

VECTOR SPACES-ELEMENTARY BASIC CONCEPTS

OBJECTIVES:

The objectives of this lesson are:

- Define the vector space over the field F, examples, define subspace of a vector space, define homomorphisms on vector spaces properties of vector spaces
- Define kernel of a homomorphism and define linear transformation
- Define quotient of quotient space
- Understand and derive some properties of quotient space
- Define isomorphism on vector space and able to study that every homomorphic image of a vector space is isomorphic to its quotient space

STRUCTURE:

18.1. INTRODUCTION:

In this Lesson we shall denote the set $F[x]$ as the set of all polynomials in x over the field F, and V_n as the set of all polynomials of degree less than n. We prove some important properties on vector spaces and also we derive every homomorphic image of a vector space is isomorphic to its quotient space. Later, we define internal direct sum of vector spaces and prove that internal direct sum of vector space V is isomorphic to external direct sum of V.

18.2. ELEMENTARY BASIC CONCEPTS:

18.2.1. Definition: A non-empty set V is said to be a vector space over a field F if V is an abelian group under an operation which we denote by $+$, and if for every $\alpha \in F, v \in V$ there is defined an element, written αV, in subject to

1. $\alpha(v+w)=\alpha v+\alpha w$
2. $(\alpha+\beta)v=\alpha v+\beta v$
3. $\alpha(\beta v)=(\alpha\beta)v$
4. $1.v=v$, for all $\alpha,\beta \in F; v,w \in V$ where the 1 represents the unit element of F under multiplication.

We shall consistently use the following notations:

a. F will be a field.

b. Lower case Greek letters will be elements of F; we shall often refer to elements of F as scalars.
c. Capital Latin letters will denote vector spaces over F.
d. Lower case Latin letters will denote elements of vector spaces. We shall often call elements of a vector space as vectors.

18.2.2. Example: Let F be a field and let K be a field which contains F as a subfield.

Here K is the set of vectors. Additions of vectors is addition composition in the field K. Since K is a field, we have that $(K,+)$ is an abelian group.

Now the elements of F constitute the set of scalars. The composition of scalar multiplication is the multiplication composition in the field K.

Since K is a field, we have $\alpha v \in K, \forall\, \alpha \in F, v \in K\ (\because \alpha, v \in K)$.

If 1 is the unity element of K, then 1 is also the unity element of the subfield F. Let $\alpha, \beta \in F$ and $v, w \in K$.

(i) $\alpha(v+w) = \alpha v + \alpha w$ ($\because$ By left distributive law in K)

(ii) $(\alpha+\beta)v = \alpha v + \beta v$ ($\because$ By right distributive law in K)

(iii) $(\alpha\beta)v = \alpha(\beta v)$ ($\because$ By associativity of multiplication in K)

(iv) $1.v = v$ and 1 is the unity element of K. Since 1 is the unity element of K, we get $1.v = v \in K$

Therefore, K is a vector space over the field.

18.2.3. Example: Let F be a field and let V be the totality of all ordered n −tuples over F.

$i.e, V = \{(\alpha_1, \alpha_2, ..., \alpha_n) / \alpha_i \in F, 1 \le i \le n\}$

Two elements $(\alpha_1, \alpha_2, ..., \alpha_n)$ and $(\beta_1, \beta_2, ..., \beta_n)$ of V are declared to be equal if and only if $\alpha_i = \beta_i$ for all $i = 1, 2, ..., n$.

Now, we introduce the requisite operators in V to make of it a vector space by defining:

1. $(\alpha_1, \alpha_2, ..., \alpha_n) + (\beta_1, \beta_2, ..., \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, ..., \alpha_n + \beta_n)$
2. $\gamma(\alpha_1, \alpha_2, ..., \alpha_n) = (\gamma\alpha_1, \gamma\alpha_2, ..., \gamma\alpha_n)$, for $\gamma \in F$.

First we prove that $(V,+)$ is an abelian group.

Let $(\alpha_1, \alpha_2, ..., \alpha_n), (\beta_1, \beta_2, ..., \beta_n), (\gamma_1, \gamma_2, ..., \gamma_n) \in V$

Now $\left[(\alpha_1, \alpha_2, ..., \alpha_n) + (\beta_1, \beta_2, ..., \beta_n)\right] + (\gamma_1, \gamma_2, ..., \gamma_n)$

$= (\alpha_1 + \beta_1, \alpha_2 + \beta_2, ..., \alpha_n + \beta_n) + (\gamma_1, \gamma_2, ..., \gamma_n)$

$= ((\alpha_1 + \beta_1) + \gamma_1, (\alpha_2 + \beta_2) + \gamma_2, ..., (\alpha_n + \beta_n) + \gamma_n)$

$= (\alpha_1 + (\beta_1 + \gamma_1), \alpha_2 + (\beta_2 + \gamma_2), ..., \alpha_n + (\beta_n + \gamma_n))$

$= (\alpha_1, \alpha_2, ..., \alpha_n) + (\beta_1 + \gamma_1, \beta_2 + \gamma_2, ..., \beta_n + \gamma_n)$

$= (\alpha_1, \alpha_2, ..., \alpha_n) + \left[(\beta_1, \beta_2, ..., \beta_n) + (\gamma_1, \gamma_2, ..., \gamma_n)\right]$

$\therefore$ Addition is associative in V.

<u>Existence of additive identity</u>: Let $(\alpha_1, \alpha_2, ..., \alpha_n) \in V$

Since $0 \in F$, we have $(0,0,...,0) \in V$

Now $(\alpha_1,\alpha_2,...,\alpha_n)+(0,0,...,0)=(\alpha_1+0,\alpha_2+0,...,\alpha_n+0)$
$=(\alpha_1,\alpha_2,...,\alpha_n)$

$\therefore (0,0,...,0)$ is the additive identity element of V.

Existence of additive inverse: Let $(\alpha_1,\alpha_2,...,\alpha_n) \in V$. Then $(-\alpha_1,-\alpha_2,...,-\alpha_n) \in V$

Now $(\alpha_1,\alpha_2,...,\alpha_n)+(-\alpha_1,-\alpha_2,...,-\alpha_n)=(\alpha_1-\alpha_1,\alpha_2-\alpha_2,...,\alpha_n-\alpha_n)$
$=(0,0,...,0)$

$\therefore (-\alpha_1,-\alpha_2,...,-\alpha_n)$ is the additive inverse element of $(\alpha_1,\alpha_2,...,\alpha_n)$

$\therefore (V,+)$ is a group.

Commutativity of addition: Let $(\alpha_1,\alpha_2,...,\alpha_n),(\beta_1,\beta_2,...,\beta_n) \in V$

Now $(\alpha_1,\alpha_2,...,\alpha_n)+(\beta_1,\beta_2,...,\beta_n)=(\alpha_1+\beta_1,\alpha_2+\beta_2,...,\alpha_n+\beta_n)$
$=(\beta_1+\alpha_1,\beta_2+\alpha_2,...,\beta_n+\alpha_n)$
$=(\beta_1,\beta_2,...,\beta_n)+(\alpha_1,\alpha_2,...,\alpha_n)$

$\therefore$ addition is commutative.

$\therefore (V,+)$ is an abelian group.

Let $(\alpha_1,\alpha_2,...,\alpha_n),(\beta_1,\beta_2,...,\beta_n) \in V$ and $\gamma_1,\gamma_2 \in F$

1. Now $\gamma_1\left[(\alpha_1,\alpha_2,...,\alpha_n)+(\beta_1,\beta_2,...,\beta_n)\right]=\gamma_1(\alpha_1+\beta_1,\alpha_2+\beta_2,...,\alpha_n+\beta_n)$
$=(\gamma_1(\alpha_1+\beta_1),\gamma_1(\alpha_2+\beta_2),...,\gamma_1(\alpha_n+\beta_n))$
$=(\gamma_1\alpha_1+\gamma_1\beta_1,\gamma_1\alpha_2+\gamma_1\beta_2,...,\gamma_1\alpha_n+\gamma_1\beta_n)$
$=(\gamma_1\alpha_1,\gamma_1\alpha_2,...,\gamma_1\alpha_n)+(\gamma_1\beta_1,\gamma_1\beta_2,...,\gamma_1\beta_n)$
$=\gamma_1(\alpha_1,\alpha_2,...,\alpha_n)+\gamma_1(\beta_1,\beta_2,...,\beta_n)$

2. Now $(\gamma_1+\gamma_2)(\alpha_1,\alpha_2,...,\alpha_n)=((\gamma_1+\gamma_2)\alpha_1,(\gamma_1+\gamma_2)\alpha_2,...,(\gamma_1+\gamma_2)\alpha_n)$
$=(\gamma_1\alpha_1+\gamma_2\alpha_1,\gamma_1\alpha_2+\gamma_2\alpha_2,...,\gamma_1\alpha_n+\gamma_2\alpha_n)$
$=(\gamma_1\alpha_1,\gamma_1\alpha_2,...,\gamma_1\alpha_n)+(\gamma_2\alpha_1,\gamma_2\alpha_2,...,\gamma_2\alpha_n)$
$=\gamma_1(\alpha_1,\alpha_2,...,\alpha_n)+\gamma_2(\alpha_1,\alpha_2,...,\alpha_n)$

3. Now $(\gamma_1\gamma_2)(\alpha_1,\alpha_2,...,\alpha_n)=((\gamma_1\gamma_2)\alpha_1,(\gamma_1\gamma_2)\alpha_2,...,(\gamma_1\gamma_2)\alpha_n)$
$=(\gamma_1(\gamma_2\alpha_1),\gamma_1(\gamma_2\alpha_2),...,\gamma_1(\gamma_2\alpha_n))$
$=\gamma_1(\gamma_2\alpha_1,\gamma_2\alpha_2,...,\gamma_2\alpha_n)$
$=\gamma_1(\gamma_2(\alpha_1,\alpha_2,...,\alpha_n))$

4. Let $(\alpha_1,\alpha_2,...,\alpha_n) \in V$ and $1 \in F$

Now $1(\alpha_1,\alpha_2,...,\alpha_n)=(1.\alpha_1,1.\alpha_2,...,1.\alpha_n)=(\alpha_1,\alpha_2,...,\alpha_n)$

$\therefore V$ is a vector space over F.

18.2.4. Example: Let F be any field and let $V = F[x]$, the set of polynomials in x over F.

Then $V = F[x]$ is a vector space over F with respect to addition of two polynomials as a addition of vectors and the product of polynomials by an element of F as a scalar multiplications.

18.2.5. Example: In $F[x]$ let V_n be the set of all polynomials of degree less than n. Using the natural operations for polynomials of addition and multiplication, V_n is a vector space over F.
Here $V_n = \{\alpha_0 + \alpha_1 x + ... + \alpha_{n-1}x^{n-1} / \alpha_1, \alpha_2, ..., \alpha_{n-1} \in F\}$

18.2.6. Definition: Let V be a vector space over F and $W \subset V$. Then W is said to be a subspace of V if W itself is a vector space over F with respect to the operations of vector addition and scalar multiplication in V.
Equivalently, W is a subspace of V whenever $w_1, w_2 \in W; \alpha, \beta \in F$ implies that $\alpha w_1 + \beta w_2 \in W$

18.2.7. Definition: Let U and V be two vector spaces over F. The mapping T of U into V is said to be a homomorphism if

1. $(u_1 + u_2)T = u_1T + u_2T$
2. $(\alpha u_1)T = \alpha(u_1T)$; for all $u_1, u_2 \in U$ and all $\alpha \in F$

If T, in addition, is one-to-one, we call it as an isomorphism.
Define kernel of T as $\{u \in U / uT = 0\}$, where 0 is the identity element of the addition in V.

18.2.8. Self Assessment Question:
Kernel of a homomorphism T is a subspace of U.

18.2.9. Note:

1. The set of all homomorphisms of U into V will be written as $Hom(U, V)$.
2. $Hom(U, V)$ can be shows to be a ring, is called the ring of Linear transformations on U.
3. O represents the zero of the addition in V, 0 represents the zero of the addition in F and $-v$ represents the additive inverse of the element v of V.
4. Kernel of a homomorphism T is (0) if and only if T is an isomorphism.

18.2.10. Lemma: If V is a vector space over F then

1. $\alpha 0 = 0$ for $\alpha \in F$
2. $0v = O$ for $v \in V$
3. $(-\alpha)v = -(\alpha v)$ for $\alpha \in F, v \in V$
4. *if* $v \neq 0$, then $\alpha v = 0$ implies that $\alpha = 0$

Proof: 1. Now $\alpha 0 = \alpha(0+0) = \alpha 0 + \alpha 0$ $(\because 0+0=0)$
$\Rightarrow 0 + \alpha 0 = \alpha 0 + \alpha 0$ $(\because \alpha 0 \in V$ and $0 + \alpha 0 = \alpha 0)$
$\Rightarrow \alpha 0 = 0$ ($\because$ By right cancellation law in V)

2. Now $ov=(0+0)v=0v+0v$ ($\because$ 0+0=0)

$\Rightarrow O+0v=0v+0v$ ($\because 0v\in V$ and $O+0v=0v$)

$\Rightarrow O=0v$ ($\because V$ is an abelian group with respect to addition of vectors and by right cancellation law in V)

3. By (2), we have $O=0v=(\alpha+(-\alpha))v=\alpha v+(-\alpha)v$

$\Rightarrow \alpha v+(-\alpha)v=O$

$\Rightarrow (-\alpha)v$ is the additive inverse of αv

$\Rightarrow (-\alpha)v=-(\alpha v)$

4. Let $v\neq 0$ and $\alpha v=0.$

Suppose $\alpha\neq 0$. Then α^{-1} exists.

Now $\alpha v=0\Rightarrow \alpha^{-1}(\alpha v)=\alpha^{-1}0=0\Rightarrow(\alpha^{-1}\alpha)v=0\Rightarrow 1.v=0\Rightarrow v=0.$

Therefore we get a contradiction that $v\neq 0.$

Hence $\alpha=0.$

Let V be a vector space over F and W be a subspace of V. Considering these merely as a abelian groups construct the quotient group V/W; its elements are the cosets $v+W$, where $v\in V, i.e., V/W=\{v+W/v\in V\}$. Since V is an abelian group, $v+W=W+v$, for all $v\in V.$

18.2.11. Lemma: If V is a vector space over F and if W is a subspace of V, then V/W is a vector space over F, where $v_1+W, v_2+W\in V/W$ and $\alpha\in F$,

1. $(v_1+W)+(v_2+W)=(v_1+v_2)+W$
2. $\alpha(v_1+W)=\alpha v_1+W.$

V/W is called the quotient space of V by W.

Proof: Let V be a vector space over F and W be a subspace of V.

We have that $V/W=\{v+W/v\in V\}$.

Define '+' on V/W as $(v_1+W)+(v_2+W)=(v_1+v_2)+W,$ for all $v_1, v_2\in V.$

We prove that $(V/W,+)$ is an abelian group.

Let $v_1+W, v_2+W, v_3+W, v_4+W\in V/W$ with $v_1+W=v_2+W$ and $v_3+W=v_4+W.$

Then $v_1-v_2\in W$ and $v_3-v_4\in W.$

Since W is a subspace of V, we get that $(v_1-v_2)+(v_3-v_4)\in W.$ That implies

$(v_1+v_3)-(v_2+v_4)\in W.$ Therefore $(v_1+v_3)+W=(v_2+v_4)+W$ and hence

$(v_1+W)+(v_3+W)=(v_2+W)+(v_4+W).$ Thus '+' is well defined.

Let $v_1+W, v_2+W, v_3+W\in V/W.$

Now

$$(v_1+W)+\big((v_2+W)+(v_3+W)\big)=(v_1+W)+\big((v_2+v_3)+W\big)$$
$$=\big(v_1+(v_2+v_3)\big)+W$$
$$=\big((v_1+v_2)+v_3\big)+W$$
$$=\big((v_1+v_2)+W\big)+(v_3+W)$$
$$=\big((v_1+W)+(v_2+W)\big)+(v_3+W)$$

Therefore '+' is associative.

Let $v+W\in V/W$. Then clearly, we have that $0+W\in\frac{V}{W}$.

Now $(v+W)+(0+W)=(v+0)+W=v+W.$

Therefore $(v+W)+(0+W)=v+W$, for all $v+W\in\frac{V}{W}$.

Hence $0+W=W$ is the additive identity element in V/W.

Let $v+W\in\frac{V}{W}$. Since $v\in V$, we get that $-v\in V$ and hence $-v+W\in V+W$.

Now $(v+W)+\big((-v)+W\big)=\big(v+-(-v)\big)+W=0+W.$

Therefore $(v+W)+\big((-v)+W\big)=0+W$, for all $v+W\in\frac{V}{W}$.

Hence $-v+W$ is the additive inverse element of $v+W$ in $\frac{V}{W}$.

Thus $(\frac{V}{W},+)$ is a group.

Let $v_1+W,v_2+W\in\frac{V}{W}$.

Since $v_1,v_2\in V$, we get that $v_1+v_2=v_2+v_2$.

Now$(v_1+W)+(v_2+W)=(v_1+v_2)+W=(v_2+v_1)+W=(v_2+W)+(v_1+W)$

Therefore $(\frac{V}{W},+)$ is an abelian group.

Define $\cdot:F\times\frac{V}{W}\to\frac{V}{W}$ by $\alpha\cdot(v+W)=\alpha\cdot v+W.$

Let $v_1+W,v_2+W\in V/W$ with $v_1+W=v_2+W$.

Then $v_1-v_2\in W\Rightarrow\alpha(v_1-v_2)\in W$, for all $\alpha\in W\Rightarrow\alpha v_1-\alpha v_2\in W$

$\Rightarrow\alpha v_1+W=\alpha v_2+W\Rightarrow\alpha(v_1+W)=\alpha(v_2+W)$

Therefore $\cdot$ is well defined.

Let $\alpha,\beta\in W$ and $v_1+W,v_2+W\in\frac{V}{W}$

Now $\alpha\big((v_1+W)+(v_2+W)\big)=\alpha\big((v_1+v_2)+W\big)$
$$=\alpha(v_1+v_2)+W$$
$$=(\alpha v_1+\alpha v_2)+W$$
$$=(\alpha v_1+W)+(\alpha v_2+W)$$
$$=\alpha(v_1+W)+\alpha(v_2+W).$$

Now $(\alpha+\beta)(v_1+W)=(\alpha+\beta)v_1=(\alpha v_1+\beta v_1)+W$
$$=(\alpha v_1+W)+(\beta v_1+W)$$
$$=\alpha(v_1+W)+\beta(v_1+W)$$

Now $(\alpha\beta)(v_1+W)=(\alpha\beta)v_1+W$
$$=\alpha(\beta v_1)+W$$
$$=\alpha(\beta v_1+W)$$

$= \alpha(\beta(v_1 + W))$

Now $1(v_1 + W) = 1.v_1 + W \quad (since\ 1 \in F)$

$= v_1 + W$

Therefore V/W is a vector space over F.

18.2.12. Theorem: If T is a homomorphism of U onto V with kernel W, then V is isomorphism to U/W. Conversely, if U is a vector space and W, a subspace of U, then there is a homomorphism of U onto U/W.

Proof: Let $T: U \to V$ be a onto homomorphism with kernel W.

Define $\phi: \frac{U}{W} \to V$ by $\phi(u + W) = T(u)$

Let $u_1 + W, u_2 + W \in U/W$.

Now

$u_1 + W = u_2 + W \Leftrightarrow u_1 - u_2 \in W \Leftrightarrow T(u_1 - u_2) = 0 (since\ W = Kernel\ of\ T) \Leftrightarrow$
$T(u_1) - T(u_2) = 0 \quad (since\ T\ is\ a\ homomorphism) \Leftrightarrow T(u_1) = T(u_2) \Leftrightarrow \phi(u_1 + W) = \phi(u_2 + W)$

.

Therefore ϕ is well defined and one-one.

Let $T(u) \in V$. Then there exists an element $u + W \in U/W$ such that $\phi(u + W) = T(u)$.

Therefore ϕ is onto.

Let $u_1 + W, u_2 + W \in U/W$ and $\alpha \in F$.

Now $\phi\big((u_1 + W) + (u_2 + W)\big) = \phi\big((u_1 + u_2) + W\big)$

$= T(u_1 + u_2)$

$= T(u_1) + T(u_2)\ (since\ T\ is\ homomorphism)$

$= \phi(u_1 + W) + \phi(u_2 + W).$

Now $\phi\big(\alpha(u_1 + W)\big) = \phi(\alpha u_1 + W)$

$= T(\alpha u_1)$

$= \alpha T(u_1)\ (since\ T\ is\ homomorphism)$

$= \alpha\phi(u_1 + W)$

Therefore ϕ is a homomorphism and hence $\frac{U}{W} \cong V$.

Conversely, let U be a vector space and W be a subspace of U.

Define $\phi: U \to U/W$ by $\phi(u) = u + W$.

Clearly, we have that ϕ is well defined.

For every $u + W \in \frac{U}{W}$, we have that $\phi(u) = u + W$. Therefore ϕ is onto.

Let $u_1, u_2 \in U$ and $\alpha \in F$.

Now $\phi(u_1 + u_2) = u_1 + u_2 + W = (u_1 + W) + (u_2 + W) = \phi(u_1) + \phi(u_2)$.

Now $\phi(\alpha u_1) = \alpha u_1 + W = \alpha(u_1 + W) = \alpha\phi(u_1)$

Therefore ϕ is homomorphism

Hence ϕ is onto homomorphism.

18.2.13. Definition: Let V be the vector space over F and let $U_1, U_2, \dots, U_n$ be subspaces of V. V is said to be the internal direct sum of $U_1, U_2, \dots, U_n$, if every element $v \in V$ can be written in one and only one way as $v = u_1 + u_2 + \cdots + u_n$ where $u_i \in U_i$.

18.2.14. Definition: Let $V_1, V_2, \dots, V_n$ be any finite number of vectors spaces over the field F.

Consider $V = V_1 \times V_2 \times \dots \times V_n$, is the set of all ordered $n-$tuples $(v_1, v_2, \dots, v_n)$ where $v_i \in V_i$ i.e. $V = \{(v_1, v_2, \dots, v_n) | \ v_i \in V_i, \ 1 \le i \le n\}$. Two elements $(v_1, v_2, \dots, v_n)$ and $(v_1', v_2', \dots, v_n')$ of V to be equal if and only if $v_i = v_i'$ for $1 \le i \le n$. Let $(v_1, v_2, \dots, v_n), (w_1, w_2, \dots, w_n) \in V$ and $\alpha \in F$ Define $(v_1, v_2, \dots, v_n) + (w_1, w_2, \dots, w_n) = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$ and $\alpha(v_1, v_2, \dots, v_n) = (\alpha v_1, \alpha v_2, \dots, \alpha v_n)$.

Clearly, V is a vector space with its operations over F. Thus V is called external direct sums of $V_1, V_2, \dots, V_n$ and is denoted by $V = V_1 \oplus V_2 \oplus \dots \oplus V_n$.

18.2.15. Theorems: If V is the internal direct sum of $U_1, U_2, \dots, U_n$ then V is isomorphic to the external direct sum of $U_1, U_2, \dots, U_n$.

Proof: Let V be the internal direct sum of $U_1, U_2, \dots, U_n$. Then every element $v \in V$ can be uniquely written as $v = u_1 + u_2 + \cdots + u_n$, where $u_i \in U_i$ for $1 \le i \le n$.
Let V' be the external direct sum of $U_1, U_2, \dots, U_n$
That is $V' = U_1 \oplus U_2 \oplus \dots \oplus U_n = \{u_1, u_2, \dots, u_n | \ u_i \in U_i, for \ 1 \le i \le n\}$
We prove that V is isomorphic to V'. Define $T: V \to V'$ by
$T(v) = T(u_1 + u_2 + \cdots + u_n) = (u_1, u_2, \dots, u_n)$.

T is well defined and one – one: Let $v, v' \in V$. Then v, v' can be uniquely written as $v = u_1 + u_2 + \cdots + u_n$, where $u_i \in U_i$, for $1 \le i \le n$ and $v' = u_1' + u_2' + \cdots + u_n'$, where $u_i' \in U_i$, for $1 \le i \le n$.
Now $v = v' \Leftrightarrow u_1 + u_2 + \cdots + u_n = u_1' + u_2' + \cdots + u_n'$
$\Leftrightarrow (u_1 - u_1') + (u_2 - u_2') + \cdots + (u_n - u_n') = 0$
$\Leftrightarrow u_i - u_i' = 0$, for $1 \le i \le n$
$\Leftrightarrow u_i = u_i'$, for $1 \le i \le n$
$\Leftrightarrow (u_1, u_2, \dots, u_n) = (u_1' + u_2' + \cdots + u_n')$
$\Leftrightarrow T(u_1 + u_2 + \cdots + u_n) = T(u_1' + u_2' + \cdots + u_n')$
$\Leftrightarrow T(v) = T(v')$
$\therefore T$ is well defined and one - one.
T is onto: Let $(u_1, u_2, \dots, u_n) \in V'$. Then there exists an element $v = u_1 + u_2 + \cdots + u_n \in V$ such that $T(v) = T(u_1 + u_2 + \cdots + u_n) = (u_1, u_2, \dots, u_n)$.
Therefore T is onto.

T is homomorphism: Let $v, v' \in V$ and $\alpha \in F$. Then v, v' can be uniquely written as $v = u_1 + u_2 + \cdots + u_n$, where $u_i \in U_i$, for $1 \le i \le n$ and $v' = u_1' + u_2' + \cdots + u_n'$, where $u_i' \in U_i$, for $1 \le i \le n$.
Now $T(v + v') = T(u_1 + u_2 + \cdots + u_n + u_1' + u_2' + \cdots + u_n')$

$$= T(u_1 + u_1' + u_2 + u_2' + \cdots + u_n + u_n')$$
$$= (u_1 + u_1', u_2 + u_2', \ldots, u_n + u_n')$$
$$= (u_1 + u_2 + \cdots + u_n) + (u_1' + u_2' + \cdots + u_n')$$
$$= T(v) + T(v')$$

Now $T(\alpha v) = T\big(\alpha(u_1 + u_2 + \cdots + u_n)\big)$
$$= T(\alpha u_1 + \alpha u_2 + \cdots + \alpha u_n)$$
$$= (\alpha u_1, \alpha u_2, \ldots, \alpha u_n)$$
$$= \alpha(u_1, u_2, \ldots, u_n) = \alpha T(v)$$

$\therefore T$ is homomorphism and hence T is an isomorphism.

18.2.16. Self Assessment Question: If U and V are vector spaces over F, define an addition and multiplication by scalars in $Hom(U,V)$ so as to make $Hom(U,V)$ into a vector space over F.

18.3. MODEL EXAMINATION QUESTIONS:

18.3.1. If V is a vector space over F then prove that

1 $\alpha 0 = 0$ for $\alpha \in F$

2 $0v = O$ for $v \in V$

3 $(-\alpha)v = -(\alpha v)$ for $\alpha \in F, v \in V$

if $v \neq 0$, then $\alpha v = 0$ implies that $\alpha = 0$

18.3.2. If V is a vector space over F and if W is a subspace of V, then show that V/W is a vector space over F, where $v_1 + W, v_2 + W \in V/W$ and $\alpha \in F$,

1. $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$
2. $\alpha(v_1 + W) = \alpha v_1 + W$.

V/W is called the quotient space of V by W.

18.3.3. If T is a homomorphism of U onto V with kernel W, then prove that V is isomorphism to U/W. Conversely, if U is a vector space and W, a subspace of U, then show that there is a homomorphism of U onto U/W.

18.3.4. If V is the internal direct sum of $U_1, U_2, \ldots, U_n$ then prove that V is isomorphic to the external direct sum of $U_1, U_2, \ldots, U_n$.

18.4 SUMMARY:

We proved some important properties on vector spaces and also we derived every homomorphic image of a vector space is isomorphic to its quotient space. Later, we proved that internal direct sum of vector space V is isomorphic to external direct sum of V.

18.5 TECHNICAL TERMS:

Vector Space: A non-empty set V is said to be a vector space over a field F if V is an abelian group under an operation which we denote by +, and if for every $\alpha \in F, v \in V$ there is defined an element, written αV, in subject to

1. $\alpha(v+w)=\alpha v+\alpha w$
2. $(\alpha+\beta)v=\alpha v+\beta v$
3. $\alpha(\beta v)=(\alpha\beta)v$
4. $1.v=v$, for all $\alpha,\beta\in F; v,w\in V$ where the 1 represents the unit element of F under multiplication.

Subspace: Let V be a vector space over F and $W\subset V$. Then W is said to be a subspace of V if W itself is a vector space over F with respect to the operations of vector addition and scalar multiplications in V.

Equivalently, W is a subspace of V whenever $w_1,w_2\in W;\alpha,\beta\in F$ implies that $\alpha w_1+\beta w_2\in W$

Homomorphism: Let U and V be two Vector spaces over F. The mapping T of U into V is said to be a homomorphism if

1. $(u_1+u_2)T=u_1T+u_2T$
2. $(\alpha u_1)T=\alpha(u_1T)$; for all $u_1,u_2\in U$ and all $\alpha\in F$

If T, in addition, is one-to-one, we call it as an isomorphism.

Define kernel of T as $\{u\in U/uT=0\}$, where 0 is the identity element of the addition in V.

Internal Direct Sum: Let V be the vector space over F and let $U_1,U_2,\dots,U_n$ be subspaces of V. V is said to be the internal direct sum of $U_1,U_2,\dots,U_n$, if every element $v\in V$ can be written in one and only one way as $v=u_1+u_2+\cdots+u_n$ where each $u_i\in U_i$.

External Direct Sum: Let $V_1,V_2,\dots,V_n$ be any finite number of vectors spaces over the field F.

Consider $V=V_1\times V_2\times\dots\times V_n$, is the set of all ordered $n-$ tuples $(v_1,v_2,\dots,v_n)$ wher $v_i\in V_i$ i.e. $V=\{(v_1,v_2,\dots,v_n)|\ v_i\in V_i,\ 1\le i\le n\}$. Two elements $(v_1,v_2,\dots,v_n)$ and $(v_1',v_2',\dots,v_n')$ of V to be equal if and only if $v_i=v_i'$ for $1\le i\le n$. Let $(v_1,v_2,\dots v_n),(w_1,w_2,\dots w_n)\in V$ and $\alpha\in F$ Define $(v_1,v_2,\dots v_n)+(w_1,w_2,\dots w_n)=(v_1+w_1,v_2+w_2,\dots v_n+w_n)$ and $\alpha(v_1,v_2,\dots v_n)=(\alpha v_1,\alpha v_2,\dots\alpha v_n)$.

Clearly, V is a vector space with its operations over F. Thus V is called external direct sums of $V_1,V_2,\dots,V_n$ and is denoted by $V=V_1\oplus V_2\oplus\dots\oplus V_n$.

18.6 ANSWERS TO SELF ASSESSMENT QUESTIONS:

18.2.8. Let W be the kernel of a homomorphism of f. Let $u,v\in W$ implies $f(u+v)=f(u)+f(v)=0+0=0$. So that $u+v\in W$. Let $\alpha\in F$. So that $f(\alpha u)=\alpha f(u)=\alpha.0=0$. Hence $\alpha u\in W$. This satisfies that the conditions of subspace. Hence W is a subspace.

18.2.16. Let $T,S\in Hom(U,V),\alpha\in F$. Define $T+S:U\to V$ as $(T+S)(u)=Tu+Su$ for all u in U. So that $T+S$ is a homomorphism of U into V. $T+S\in Hom(U,V)$. Define $\alpha T:U\to V$ as $(\alpha T)(u)=\alpha(Tu)$. That is αT is a homomorphism of U into V. Hence

$aT \in Hom(U,V)$. It is easy to show that $Hom(U,V)$ is a vector space over F under the addition and multiplication by scalars.

18.7 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-Dr. Noorbhasha Rafi

LESSON - 19

LINEAR INDEPENDENCE AND BASES

OBJECTIVES:

The objectives of this lesson are to

- define the linear span and discuss the properties of linear span
- define finite dimensional vector space, linearly independent, dependent vectors over a field and solve some problems on linearly independent and dependent vectors.
- define basis of a vector space and prove that every finite dimensional vector space V is isomorphic to F^n.
- prove that any two bases of a finite dimensional vector space V over F have the same number of elements.
- Prove that for every subspace W of a finite dimensional vector space V is finite dimensional, $dim\ W \leq \dim V$ and $dim\frac{V}{W} = dim\ V - dim\ W$.

STRUCTURE:

19.1. INTRODUCTION:

In this lesson, we consider $L(S)$ as linear span of S where S is a non-empty subset of vector space V over a field F. We can prove that $L(S)$ is a subspace of V and study the properties of linear span. We define linear independent, dependent vectors and finite dimensional vector space V and later prove some results on them.

19.2. LINEAR INDEPENDENCE AND BASES:

19.2.1. Definition: Let V is a vector space over F and if $v_1, v_2, ..., v_n \in V$ then any element of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where the $\alpha_i \in F$, is a linear combination over F of $v_1, v_2, ..., v_n$.

19.2.2. Definition: If S is a nonempty subset of the vector space V, then $L(S)$, the linear span of S, is the set of all linear combinations of finite sets of elements of S.
i.e., $L(S) = \{\alpha_1 v_1, \beta_1 v_1 + \beta_2 v_2, \gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n \,|\, v_1, v_2, \cdots, v_n \in S \text{ and } \alpha_1, \beta_i's, \gamma_i's \in F\}$

19.2.3. Lemma: $L(S)$ is a subspace of V.

Proof: Let V be a vector space over F. Let $v, w \in L(S)$. Then $v = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n$ and $w = \mu_1 t_1 + \mu_2 t_2 + \cdots + \mu_m t_m$, where the $\lambda's, \mu's$ are in F and the s_i, t_i are all in S. Let $\alpha, \beta \in F$.
Now

$$\alpha v + \beta w = \alpha(\lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n) + \beta(\mu_1 t_1 + \mu_2 t_2 + \cdots + \mu_m t_m)$$
$$= (\alpha\lambda_1)s_1 + (\alpha\lambda_2)s_2 + \cdots + (\alpha\lambda_n)s_n + (\beta\mu_1)t_1 + (\beta\mu_2)t_2 + \cdots + (\beta\mu_m)t_m.$$

Therefore $\alpha v + \beta w \in L(S)$. Hence $L(S)$ is a subspace of V.

19.2.4. Lemma: If S, T are subsets of V, then

1. $S \subset T$ implies $L(S) \subset L(T)$.
2. $L(S \cup T) = L(S) + L(T)$.
3. $L(L(S)) = L(S)$.

Proof:

1. Assume that $S \subset T$. Let $v \in L(S)$. Then $v = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n$, where the $\lambda's$ are in F and the $s_i's$ are all in S. Since $S \subset T$, we get that $v = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n$, where the $\lambda's$ are in F and the $s_i's$ are all in T. Therefore $v \in L(T)$. Hence $L(S) \subset L(T)$.
2. Let $v \in L(S \cup T)$. Then $v = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n + \mu_1 t_1 + \mu_2 t_2 + \cdots + \mu_m t_m$, where the $\lambda's, \mu's$ are in F and the $\lambda's, \mu's$ are all in $S \cup T$. Since $\lambda's, \mu's$ are all in $S \cup T$, we can choose $s_1, s_2, \cdots, s_n \in S$ and $t_1, t_2, \cdots, t_m \in T$. Then $\lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n \in L(S)$ and $\mu_1 t_1 + \mu_2 t_2 + \cdots + \mu_m t_m \in L(T)$. Therefore $v =$ an element of $L(S)$ + an element of $L(T)$.
   Therefore $v \in L(S) + L(T)$ and hence $L(S \cup T) \subseteq L(S) + L(T)$. Conversely, let $v \in L(S) + L(T)$. Then $v = \alpha + \beta$, where $\alpha \in L(S)$, $\beta \in L(T)$. Since $\alpha \in L(S)$, $\beta \in L(T)$, we have that $\alpha =$ linear combination of finite number of elements of S and $\beta =$ linear combination of finite number of elements of T. That implies $v = \alpha + \beta =$ linear combination of finite number of elements of $S \cup T$. Therefore $v \in L(S \cup T)$ and hence $L(S) + L(T) \subseteq L(S \cup T)$. Thus $L(S \cup T) = L(S) + L(T)$.
3. Since $1 \in F$, we have that $s = 1.s \in L(S)$, for all $s \in S$. Therefore $S \subseteq L(S)$. By condition 1, we have that $L(S) \subseteq L(L(S))$. Let $v \in L(L(S))$. Then $v \in L(S)$. Then $v = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n$, where the $\lambda's$ are in F and the $s_i's$ are all in $L(S)$. Since $s_i's$ are all in $L(S)$, we can write $s_i = \alpha_{i_1} s_{i_1} + \alpha_{i_2} s_{i_2} + \cdots + \alpha_{i_k} s_{i_k}$, where $\alpha's \in F$, $s_i's \in S$ and $1 \le i \le n$.
   Now,
   $v = \lambda_1(\alpha_{11}s_{11} + \alpha_{12}s_{12} + \cdots + \alpha_{1k}s_{1k}) + \lambda_2(\alpha_{21}s_{21} + \alpha_{22}s_{22} + \cdots + \alpha_{2k}s_{2k}) + \cdots + \lambda_n(\alpha_{n1}s_{n1} + \alpha_{n2}s_{n2} + \cdots + \alpha_{nk}s_{nk})$
   That implies $v \in L(S)$. Therefore $L(L(S)) \subseteq L(S)$ and hence $L(L(S)) = L(S)$.

19.2.5. Definition: The vector space V is said to be finite-dimensional (over F) if there is a finite subset S in V such that $V = L(S)$.

Note that $F^{(n)}$ is finite-dimensional over F, for if S consists of the n vectors $(1,0,\cdots,0), (0,1,\cdots,0), \cdots, (0,0,\cdots,1)$, then $V = L(S)$.

19.2.6. Definition: If V is a vector space over the field F and if $v_1, v_2, \cdots, v_n$ are in V, we say that they are linearly dependent over F if there exist elements $\lambda_1, \lambda_2, \cdots, \lambda_n$ in F, not all of them 0, such that $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$.
If the vectors $v_1, v_2, \cdots, v_n$ are not linearly dependent over F, they are said to be linearly independent over F.

19.2.7. Problem: Verify that given vectors $(1,0,0), (0,1,0), (0,0,1)$ are linearly independent or not
Solution: Let $\alpha_1, \alpha_2, \alpha_3 \in F$. Consider $\alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,0,1) = (0,0,0)$.
Then $\alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0$. Hence given vectors $(1,0,0), (0,1,0), (0,0,1)$ are linearly independent.

19.2.8. Problem: Verify that given vectors $(1,1,0), (3,1,3), (5,3,3)$ are linearly independent or not.
Solution: Let $\alpha_1, \alpha_2, \alpha_3 \in F$. Consider $\alpha_1(1,1,0) + \alpha_2(3,1,3) + \alpha_3(5,3,3) = (0,0,0)$.
Then $(\alpha_1 + 3\alpha_2 + 5\alpha_3, \alpha_1 + \alpha_2 + 3\alpha_3, 3\alpha_2 + 3\alpha_3) = (0,0,0)$. That implies
$\alpha_1 + 3\alpha_2 + 5\alpha_3 = 0$, $\alpha_1 + \alpha_2 + 3\alpha_3 = 0$, $3\alpha_2 + 3\alpha_3 = 0$. From the equation $3\alpha_2 + 3\alpha_3 = 0$, we get that $\alpha_2 = -\alpha_3$. If $\alpha_3 = 1$ then we get that $\alpha_2 = -1$ and $\alpha_1 = -2$.
Hence given vectors $(1,0,0), (0,1,0), (0,0,1)$ are linearly dependent.

19.2.9. Lemma: If $v_1, v_2, \cdots, v_n \in V$ are linearly independent, then every element in their linear span has a unique representation in the form $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$ with the $\lambda_i \in F$.

Proof: Let $v_1, v_2, \cdots, v_n \in V$ be linearly independent elements. Take $S = \{v_1, v_2, \cdots, v_n\}$. Suppose $x \in L(S)$ has two representations say $x = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$ and
$x = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_n v_n$.
Then $0 = x - x = (\lambda_1 - \mu_1)v_1 + (\lambda_2 - \mu_2)v_2 + \cdots + (\lambda_n - \mu_n)v_n$. Since $v_1, v_2, \cdots, v_n \in V$ are linearly independent, we have that $\lambda_1 - \mu_1 = 0$, $\lambda_2 - \mu_2 = 0, \cdots, \lambda_n - \mu_n = 0$. That implies
$\lambda_1 = \mu_1$, $\lambda_2 = \mu_2, \cdots, \lambda_n = \mu_n$. Hence every element of $L(S)$ has unique representation.
19.2.10. Theorem: If $v_1, v_2, \cdots, v_n \in V$ then either they are linearly independent or some v_k is a linear combination of the preceding ones, $v_1, v_2, \cdots, v_{k-1}$.

Proof: Let $v_1, v_2, \cdots, v_n \in V$.
Suppose $v_1, v_2, \cdots, v_n$ are linearly independent. Then there is, of course, nothing to prove. Suppose that $v_1, v_2, \cdots, v_n$ are linearly dependent. Then there exist scalars $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ not all of the $\alpha's$ are zero such that $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$. Let k be the largest integer such that $\alpha_k \neq 0$, for $k \leq n$ and $\alpha_i = 0$, for all $i > k$. Then $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$. That implies
$\alpha_k v_k = -(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1})$.

Since α_k is non zero element of F, we get that $\alpha_k^{-1} \in F$. That implies $v_k = (-\alpha_k^{-1}\alpha_1 v_1) + (-\alpha_k^{-1}\alpha_2 v_2) + \cdots + (-\alpha_k^{-1}\alpha_{k-1} v_{k-1})$. Therefore v_k is a linear combination of its predecessors.

19.2.11. Corollary: If $v_1, v_2, \cdots, v_n$ in V have W as linear span and if $v_1, v_2, \cdots, v_k$ are linearly independent, then we can find a subset $v_1, v_2, \cdots, v_n$ of the form $v_1, v_2, \cdots, v_n, v_{i_1}, v_{i_2}, \cdots, v_{i_r}$ consisting of linearly independent elements whose linear span is also W.

Proof: Suppose $v_1, v_2, \cdots, v_n$ are linearly independent. Then there is nothing to prove. Suppose that $v_1, v_2, \cdots, v_n$ are linearly dependent. By the above theorem, choose the first element v_j such that v_j is the linear combination of its predecessors. Since $v_1, v_2, \cdots, v_k$ are linearly independent, we have that $j > k$.
Thus $v_1, v_2, \cdots, v_{j-1}, v_{j+1}, \cdots, v_n$ has $n-1$ elements. Therefore, its linear span is contained in W. However, we claim that it is actually equal to W. Let $x \in W$. Then x can be written as a linear combination of $v_1, v_2, \cdots, v_n$.
That is $x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k + \cdots + \alpha_j v_j + \cdots + \alpha_n v_n$. Since v_j is the linear combination of its predecessors, there exist $\beta_1, \beta_2, \cdots, \beta_{j-1} \in F$ such that $v_j = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{j-1} v_{j-1}$. That implies $x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k + \cdots + \alpha_j(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{j-1} v_{j-1}) + \cdots + \alpha_n v_n$.
That implies $x = (\alpha_1 + \alpha_j\beta_1)v_1 + (\alpha_2 + \alpha_j\beta_2)v_2 + \cdots + (\alpha_{j-1} + \alpha_j\beta_{j-1})v_{j-1} + \alpha_{j+1}v_{j+1} + \cdots + \alpha_n v_n$.

19.2.12. Corollary: If V is a finite-dimensional vector space, then it contains a finite set $v_1, v_2, \cdots, v_n$ of linearly independent elements whose linear span is V.

Proof: Let V be a finite-dimensional vector space. Then there exists a finite subset $S = \{v_1, v_2, \cdots, v_m\}$ such that $L(S) = V$. By the above corollary, there exists a finite subset of these denoted by $v_1, v_2, \cdots, v_n$ consisting of linearly independent elements, whose span is V.

19.2.13. Definition: A subset S of a vector space V is called a basis of V if S consists of linearly independent elements (that is, any finite number of elements in S is linearly independent) and $V = L(S)$.

19.2.14. Corollary: If V is a finite-dimensional vector space and if $u_1, u_2, \cdots, u_m$ span V then some subset of $u_1, u_2, \cdots, u_m$ forms a basis of V.

19.2.15. Result: If V is a finite dimensional vector space over F then V is isomorphic to $F^{(n)}$.

Proof: Let V be a finite-dimensional vector space. Then V has finite basis $\{v_1, v_2, \cdots, v_n\}$.
Let $v \in V$. Then v has a unique representation in the form $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ with $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$. Define $\phi : V \to F^{(n)}$ by $\phi(v) = \phi(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Clearly, ϕ is well defined. Let $v, v' \in V$ such that $\phi(v) = \phi(v')$. Since $v, v' \in V$, v, v' have a unique representations in the form $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ and $v' = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$, where $\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_n \in F$. Since $\phi(v) = \phi(v')$, then we have that $\phi(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = \phi(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n)$. That implies $(\alpha_1, \alpha_2, \cdots, \alpha_n) = (\beta_1, \beta_2, \cdots, \beta_n)$. That implies $\alpha_i = \beta_i$, for $1 \le i \le n$. That implies $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$. That implies $v = v'$. Hence ϕ is one-one. Let $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in F^{(n)}$. Then there exists $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \in V$ such that $\phi(v) = (\alpha_1, \alpha_2, \cdots, \alpha_n)$. Therefore ϕ is onto. Let $v, v' \in V$. Then v, v' have a unique representations in the form $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ and $v' = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$, where $\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_n \in F$.

Now

$$\begin{aligned}\phi(v + v') &= \phi(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n) \\ &= \phi((\alpha_1 + \beta_1) v_1 + (\alpha_2 + \beta_2) v_2 + \cdots + (\alpha_n + \beta_n) v_n) \\ &= (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \cdots, \alpha_n + \beta_n) \\ &= (\alpha_1, \alpha_2, \cdots, \alpha_n) + (\beta_1, \beta_2, \cdots, \beta_n) \\ &= \phi(v) + \phi(v').\end{aligned}$$

Let $\alpha \in F$.

Now

$$\begin{aligned}\phi(\alpha v) &= \phi(\alpha(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n)) \\ &= \phi(\alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + \cdots + \alpha\alpha_n v_n) \\ &= (\alpha\alpha_1, \alpha\alpha_2, \cdots, \alpha\alpha_n) \\ &= \alpha(\alpha_1, \alpha_2, \cdots, \alpha_n) \\ &= \alpha\phi(v).\end{aligned}$$

Therefore ϕ is homomorphism and hence ϕ is isomorphism.

19.2.16. Self Assessment Question: If V is a finite dimensional and T is a homomorphism of V onto V prove that T must be one-to-one, and so, an isomorphism

19.2.17. Lemma: If $v_1, v_2, \cdots, v_n$ is a basis of V over F and if $w_1, w_2, \cdots, w_m$ in V are linearly independent over F, then $m \le n$.

Proof: Let $v_1, v_2, \cdots, v_n$ be a basis of V over F and let $w_1, w_2, \cdots, w_m$ be linearly independent elements of V. Since $w_m \in V$, we have that w_m is a linear combination of $v_1, v_2, \cdots, v_n$ and hence $w_m, v_1, v_2, \cdots, v_n$ are linearly dependent elements. Since $v_1, v_2, \cdots, v_n$ span V, we have that $w_m, v_1, v_2, \cdots, v_n$ also span V.

By corollary 1, $w_m, v_1, v_2, \cdots, v_n$ has a proper subset $w_m, v_{i_1}, v_{i_2}, \cdots, v_{i_k}$, where $i_k \le n-1$ is a basis of V. Repeat this process by adding $w_2, w_3, \cdots, w_{m-1,}$ finally, we get that $w_2, w_3, \cdots, w_m, v_{j_1}, v_{j_2}, \cdots, v_{j_m}$, where $j_m \le n-(m-1)$ and is a basis of V. Now consider w_1. Since $w_1, w_2, \cdots, w_m$ are linearly independent, w_1 cannot be written as a linear combination of

$w_2, w_3, \cdots, w_m$. Hence at least one v_i must belong to the above basis. Therefore $m-1 \le n-1$. Thus $m \le n$.

19.2.18. Corollary: If V is finite-dimensional over F then any two bases of V have the same number of elements.

Proof: Let $v_1, v_2, \cdots, v_n$ be a basis of V over F and $w_1, w_2, \cdots, w_m$ be another basis of V. By above lemma, we get that $m \le n$ and $n \le m$. Therefore $m = n$.

19.2.19. Corollary: $F^{(n)}$ is isomorphic $F^{(m)}$ if and only if $m = n$.

Proof: $F^{(n)}$ has a basis $\{(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,0,\cdots,1)\}$ having n elements. Since $F^{(n)}$ is isomorphic $F^{(m)}$, the images of $\{(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,0,\cdots,1)\}$ is a basis of $F^{(m)}$ if and only if $m = n$.

19.2.20. Corollary: If V is finite-dimensional over F then V is isomorphic to $F^{(n)}$ for a unique integer n; in fact, n is the number of elements in any basis of V over F.

19.2.21. Definition: The integer n in the above corollary is called the dimension of V over F. It is denoted by $\dim_F V$.

19.2.22. Corollary: Any two finite-dimensional vector spaces over F of the same dimension are isomorphic.

Proof: Let V, V' be any two finite-dimensional vector spaces over F having the same dimension n. Then $V \cong F^{(n)}$ and $V' \cong F^{(n)}$. Therefore $V \cong V'$.

19.2.23. Lemma: If V is finite-dimensional over F and if $u_1, u_2, \cdots, u_m \in V$ are linearly independent, then we can find vectors $u_{m+1}, \cdots, u_{m+r} \in V$ such that $u_1, u_2, \cdots, u_m, u_{m+1}, \cdots, u_{m+r}$ is a basis of V.

Proof: Let V be finite-dimensional over F and $u_1, u_2, \cdots, u_m \in V$ be linearly independent. Suppose $v_1, v_2, \cdots, v_n$ be a basis of V. Since these span V, $u_1, u_2, \cdots, u_m, v_1, v_2, \cdots, v_n$ also span V. That implies there is a subset of these of the form $u_1, u_2, \cdots, u_m, v_{i_1}, v_{i_2}, \cdots, v_{i_r}$ which consists of linearly independent elements which span V. Take $v_{i_1} = u_{m+1}, v_{i_2} = u_{m+2}, \cdots, v_{i_r} = u_{m+r}$. Therefore $u_1, u_2, \cdots, u_m, u_{m+1}, \cdots, u_{m+r}$ is a basis of V.

19.2.24. Lemma: If V is finite-dimensional and if W is a subspace of V, then W is finite-dimensional, $dim W \le dim V$ and $dim(V/W) = dim V - dim W$

Proof: Let V be a finite-dimensional and W be a subspace of V. Let us take $\dim V = n$. Then any $n+1$ elements in V are linearly dependent. In particular, any $n+1$ elements in W are linearly dependent. So we can find a largest set of linearly independent elements in W, $w_1, w_2, \cdots, w_m$ where $m \le n$. Let $w \in W$. Then $w, w_1, w_2, \cdots, w_m$ are linearly dependent. That implies there exist $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_m \in F$ not all of them are zero's such that $\alpha w + \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m = 0$.

Suppose $\alpha = 0$. Then by the linear independence of the w_i, we get that $\alpha_i = 0$, which is a contradiction. Therefore $\alpha \neq 0$. Since $\alpha \in F$, we have that $\alpha^{-1} \in F$. Now $w = -\alpha^{-1}(\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m) = (-\alpha^{-1}\alpha_1)w_1 + (-\alpha^{-1}\alpha_2)w_2 + \cdots + (-\alpha^{-1}\alpha_m)w_m$. That implies $W = L(\{w_1, w_2, \cdots, w_m\})$. Therefore $\{w_1, w_2, \cdots, w_m\}$ is a basis of W. Hence W is a finite dimensional vector space and $dimW = m \leq n = dimV$. Thus $dimW \leq dimV$ Since $w_1, w_2, \cdots, w_m$ are linearly independent elements of V, we have that $w_1, w_2, \cdots, w_m, v_1, v_2, \cdots, v_r$ is a basis of V with $m + r = n$. Let $v + w \in V/W$. Since $v \in V$, we have that $v = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_m v_m$. That implies

$$\begin{aligned} v + W &= (\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_r) + W \\ &= (\alpha_1 w_1 + W) + (\alpha_2 w_2 + W) + \cdots + (\alpha_m w_m + W) + (\beta_1 v_1 + W) + (\beta_2 v_2 + W) + \cdots + (\beta_r v_r + W) \\ &= \alpha_1(w_1 + W) + \alpha_2(w_2 + W) + \cdots + \alpha_m(w_m + W) + \beta_1(v_1 + W) + \beta_2(v_2 + W) + \cdots + \beta_r(v_r + W). \end{aligned}$$

Since $w_1, w_2, \cdots, w_m \in W$, we have that $w_i + W = 0 + W$ for $1 \leq i \leq m$ and hence $v + W = \beta_1(v_1 + W) + \beta_2(v_2 + W) + \cdots + \beta_r(v_r + W)$. Therefore $\{v_1 + W, v_2 + W, \cdots, v_r + W\}$ span of V/W.

Now we prove that $v_1 + W, v_2 + W, \cdots, v_r + W$ are linearly independent. Let $\gamma_1, \gamma_2, \cdots, \gamma_r \in F$ such that $\gamma_1(v_1 + W) + \gamma_2(v_2 + W) + \cdots + \gamma_r(v_r + W) = 0 + W$. Then $(\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_r v_r) + W = 0 + W$ and hence $\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_r v_r \in W$. That implies $\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_r v_r = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m$ and hence $(-\gamma_1)v_1 + (-\gamma_2)v_2 + \cdots + (-\gamma_r)v_r + \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m = 0$. Since $\{v_1, v_2, \cdots, v_r, w_1, w_2, \cdots, w_m\}$ is a basis of V, we have that $\alpha_i = 0$ and $\gamma_i = 0$, for all i, j. That implies $\{v_1 + W, v_2 + W, \cdots, v_r + W\}$ is linearly independent. Therefore $\{v_1 + W, v_2 + W, \cdots, v_r + W\}$ is a basis of V/W. Hence

$dim\ (V/W) = r = n - m = dimV - dimW$

Thus $\dim(V/W) = \dim V - \dim W$.

19.2.25. Corollary: If A and B are finite-dimensional subspaces of a vector space V, then $A + B$ is finite-dimensional and $\dim(A + B) = \dim(A) + \dim(B) - \dim(A \cap B)$.

Proof: We have that $\frac{A+B}{B} \approx \frac{A}{A \cap B}$. Since A and B are finite dimensional, we get that $\dim(A + B) - \dim B = \dim\left(\frac{A+B}{B}\right) = \dim\left(\frac{A}{A \cap B}\right) = \dim A - \dim(A \cap B)$. Therefore $\dim(A + B) = \dim A + \dim B - \dim(A \cap B)$.

19.3. MODEL EXAMINATION QUESTIONS:

19.3.1. Prove that $L(S)$ is a subspace of V.

19.3.2. Verify that given vectors (1,1,0), (3,1,3), (5,3,3) are linearly independent or not.

19.3.3. If $v_1, v_2, \cdots, v_n \in V$ then show that either they are linearly independent or some v_k is a linear combination of the preceding ones, $v_1, v_2, \cdots, v_{k-1}$.

19.3.4. If V is a finite dimensional and T is a homomorphism of V onto V prove that T must be one-to-one, and so, an isomorphism.

19.3.5. If V is finite-dimensional and if W is a subspace of V, then prove that W is finite-dimensional, $dimW \leq dimV$ and $dimV/W = dimV - dimW$.

19.4 SUMMARY:

We proved that $L(S)$ is a subspace of V and study the properties of linear span. We defined linear independent, dependent vectors and finite dimensional vector space V and later, derived some results on them.

19.5 TECHNICAL TERMS:

Linear Combination: Let V is a vector space over F and if $v_1, v_2, ..., v_n \in V$ then any element of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where the $\alpha_i \in F$, is a linear combination over F of $v_1, v_2, ..., v_n$.

Linear Span: If S is a non empty subset of the vector space V, then $L(S)$, the linear span of S, is the set of all linear combinations of finite sets of elements of S.
i.e., $L(S) = \{\alpha_1 v_1, \beta_1 v_1 + \beta_2 v_2, \gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n \mid v_1, v_2, \cdots, v_n \in S \text{ and } \alpha_1, \beta_i's, \gamma_i's \in F\}$

Finite-Dimensional Vector Space: The vector space V is said to be finite-dimensional (over F) if there is a finite subset S in V such that $V = L(S)$.

Linearly Dependent and Linearly Independent: If V is a vector space over the field F and if $v_1, v_2, \cdots, v_n$ are in V, we say that they are linearly dependent over F if there exist elements $\lambda_1, \lambda_2, \cdots, \lambda_n$ in F, not all of them 0, such that $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$.
If the vectors $v_1, v_2, \cdots, v_n$ are not linearly dependent over F, they are said to be linearly independent over F.

Basis: A subset S of a vector space V is called a basis of V if S consists of linearly independent elements (that is, any finite number of elements in S is linearly independent) and $V = L(S)$.

19.6 ANSWERS TO SELF ASSESSMENT QUESTIONS:

19.2.16. Let $v_1, v_2, \ldots v_n$ be one basis of V. $T(v_1), T(v_2), \ldots, T(v_n)$ span of V. For if $v \in V$ then $v = T(w)$ for some $w \in V$. Since T is an onto mapping. $w = \sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$. Now $v = T(w) = T(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{i=1}^{n} \alpha_i T(v_i)$. So that $T(v_1), T(v_2), \ldots T(v_n)$ span of V. By known results we conclude that $T(v_1), T(v_2), \ldots T(v_n)$ are linearly independent. Let $v \in V$ and $v = \sum_{i=1}^{n} \beta_i v_i$. If $T(v) = 0$, then $T(v) = T(\sum_{i=1}^{n} \beta_i v_i) = \sum_{i=1}^{n} \beta_i T(v_i) = 0$.
Since $T(v_1), T(v_2), \ldots T(v_n)$ are linearly independent. We have $\beta_1 = \beta_2 = \ldots = \beta_n = 0$.
Hence $v = \sum_{i=1}^{n} \beta_i v_i = 0$. T is one to one. T is an isomorphism of V onto V.

19.7 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-**Dr. Noorbhasha Rafi**

LESSON - 20

DUAL SPACES

OBJECTIVES:

The objectives of this lesson are to

- prove that Hom(V, W) the set of all vector space homomorphism of a vector space V over F into a vector space W over F is a vector space over F under pointwise addition and scalar multiplication.
- prove that dim Hom(V, W) = nm, where n = dimV and m = dimW.
- define the dual space $\hat{V}$ of a vector space V.
- prove that dim$\hat{V}$ = n, if dimV = n, V is a finite dimension vector space.
- define annihilator, A(W), of a subspace W of a vector space.
- Prove that $\hat{W}$ is isomorphic to $\hat{V}$/ A(W) and dim A(W) = dimV – dimW, where V is a finite dimension vector space and W is a subspace of V.
- A(A(W)) = W for any subspace W of a finite dimension vector space V.

STRUCTURE:

20.1. INTRODUCTION:

In this lesson the set Hom(V, W) of all vector space homomorphism of a vector space V over F into a vector space W over F is realized as a vector space over F. The dual space $\hat{V}$ of a vector space V is defined and studied. For a finite dimension vector space V it is shown that dim$\hat{V}$ = dimV. The annihilator A(W) of a subspace W of a vector space is defined and its dimension expressed interms of dimV and dimW, where V is a finite dimensional vector space.

20.2. DUAL SPACES:

20.2.1. Theorem: Let V, U be vector spaces over a filed F. Then the set of all homomorphism of V into $U (i.e., Hom(V, U))$ is also a vector space over F.

Proof: Let $f, g \in Hom(V, U)$. Define $(v)(f+g) = (v)f + (v)g,$ for all $v \in V$.
Let $v_1, v_2 \in V$ and $\alpha_1, \alpha_2 \in F$.
(i). Now
$$\begin{aligned}(\alpha_1 v_1 + \alpha_2 v_2)(f+g) &= (\alpha_1 v_1 + \alpha_2 v_2)f + (\alpha_1 v_1 + \alpha_2 v_2)g \\ &= \alpha_1[(v_1)f] + \alpha_2[(v_2)f] + \alpha_1[(v_1)g] + \alpha_2[(v_2)g] \\ &= \alpha_1[(v_1)f] + \alpha_1[(v_1)g] + \alpha_2[(v_2)f] + \alpha_2[(v_2)g] \\ &= \alpha_1[(v_1)(f+g)] + \alpha_2[(v_2)(f+g)]\end{aligned}$$
So $f+g$ is also a homomorphism of V into U and that $f+g \in Hom(V, U)$

(ii). Now $(v)[(f+g)+h] = (v)(f+g)+(v)h$
$= \big((v)f+(v)g\big)+(v)h$
$= (v)f+((v)g+(v)h)$
$= (v)f+((v)(g+h))$
$= (v)(f+(g+h))$
Therefore $(f+g)+h = f+(g+h)$.

(iii). We have $(v)0 = 0$, for all $v \in V$ and hence $0 \in Hom(V,U)$.
Also we have that $f+0 = 0 = 0+f$, for all $f \in Hom(U,V)$.

(iv). For ant $f \in Hom(V,U)$, define $-f: V \to U$ by $(v)(-f) = -(v)f$, for all $v \in V$.

Now $(\alpha_1 v_1+\alpha_2 v_2)(-f) = -(\alpha_1 v_1+\alpha_2 v_2)f$
$= -[\alpha_1(v_1)f+\alpha_2(v_2)f]$
$= -[\alpha_1((v_1)f)+\alpha_2((v_2)f)]$
So $-f \in Hom(U,V)$. Also we have that $f+(-f) = 0 = (-f)+f$.

(v). Now $(v)(f+g) = (v)f+(v)g = (v)g+(v)f = (v)(g+f)$, for all $v \in V$.
Hence $f+g = g+f$.
Therefore $Hom(V,U)$ is an abelian group under addition.
For any $\alpha \in F$, $f \in Hom(V,U)$, define $(v)(\alpha f) = \alpha[(v)f]$, for all $v \in V$.

(vi). Let $\beta_1, \beta_2 \in F$.
Now $(\beta_1 v_1+\beta_2 v_2)(\alpha f) = \alpha[(\beta_1 v_1+\beta_2 v_2)f]$
$= \alpha[\beta_1(v_1)f+\beta_2(v_2)f]$
$= (\alpha\beta_1)[(v_1)f]+(\alpha\beta_2[(v_2)f]$
$= \beta_1 v_1(\alpha f)+\beta_2 v_2(\alpha f)$
Therefore αf is a homomorphism of V into U and hence $\alpha f \in Hom(V,U)$

(vii). Clearly we have that $(\alpha\beta)f = \alpha(\beta f)$

(viii). Cleary we have that $(\alpha+\beta)f = \alpha f+\beta f$

(ix). Now $(v)[\alpha(f+g)] = \alpha[(v)(f+g)]$
$= \alpha[(v)f+(v)g]$
$= \alpha[(v)f]+\alpha[(v)g]$
$= (v)(\alpha f)+(v)(\alpha g)$
$= (v)[\alpha f+\alpha g]$
Therefore $\alpha(f+g) = \alpha f+\alpha g$
Clearly $if = f$. Hence $Hom(V,U)$ is a vector space over F.

20.2.2. Theorem: Let V, U be finite dimensional vector spaces over a field F of dimensions m and n respectively. Then the dimension of the vector space $Hom(V,U)$ is mn.

Proof: Suppose V has a basis $v_1, v_2, \ldots, v_n$ consisting of n vectors and U has a basis $u_1, u_2, \ldots, u_m$ consisting of m vectors.

Let $v \in V$. Then $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ and this representation of v is unique.

Let $1 \leq i \leq n, 1 \leq j \leq m$. Define $T_{ij}: V \to U$ by $(v)T_{ij} = \alpha_i u_j$

Clearly T_{ij} is a homomorphism of V into U.

Hence $A = \{T_{ij} | \ 1 \leq i \leq n, 1 \leq j \leq m\} \subseteq Hom(V, U)$.

Let $S \in Hom(V, U)$

Let $(v_i)S = \beta_{i1} u_1 + \beta_{i2} u_2 + \cdots + \beta_{im} u_m$, for $\beta_{ik} \in F$.

We have

$T = (\beta_{11} T_{11} + \beta_{12} T_{12} + \cdots + \beta_{1m} T_{1m}) + (\beta_{21} T_{21} + \beta_{22} T_{22} + \cdots + \beta_{2m} T_{2m}) + \cdots + (\beta_{n1} T_{n1} + \beta_{n2} T_{n2} + \cdots + \beta_{nm} T_{nm}) \in Hom(V, U)$.

$Now\ (v_i)S = (v_i)\beta_{i1} T_{i1} + \beta_{i2} T_{i2} + \cdots + \beta_{im} T_{im} = \beta_{i1} u_1 + \beta_{i2} u_2 + \cdots + \beta_{im} u_m$,

for $1 \leq i \leq n$ as $(v_k)T_{ij} = \begin{cases} 0, & if\ k \neq i \\ u_j, & if\ k = i \end{cases}$

Since $(v_j)S = (v_i)T\ \forall\ 1 \leq i \leq n,\ S = T$ and that S is a linear combination of $T_{ij}, 1 \leq i \leq m, 1 \leq j \leq m$.

So A spans $Hom(V, U)$

Suppose that

$0 = (\gamma_{11} T_{11} + \gamma_{12} T_{12} + \cdots + \gamma_{1m} T_{1m}) + (\gamma_{21} T_{21} + \gamma_{22} T_{22} + \cdots + \gamma_{2m} T_{2m}) + \cdots + (\gamma_{m1} T_{n1} + \gamma_{m2} T_{n2} + \cdots + \gamma_{nm} T_{nm})$

That implies $0 = v_i(0) = v_i(\gamma_{i1} T_{i1} + \gamma_{i2} T_{i2} + \cdots + \gamma_{im} T_{im}) = \gamma_{i1} w_1 + \gamma_{i2} w_2 + \cdots + \gamma_{im} w_m$

Since $w_1, w_2, \ldots w_m$ are linearly independent, we get $0 = \gamma_{i1} = \gamma_{i2} = \cdots = \gamma_{im}$

Therefore $\gamma_{ij} = 0$ for all $1 \leq i \leq n, 1 \leq j \leq m$.

Hence A is a linearly independent set in $Hom(V, U)$ that it is a basis. So dim $Hom(V, U) = nm$

20.2.3. Corollary. Let V be a finite dimensional vector space over a field F of dimension n. Then $\dim(V, F) = n$.

20.2.4. Definition: Let V be a vector space over a field F. Then the vector space $Hom(V, F)$ is called the dual space of V.

20.2.5. Lemma: Let V be a vector space of dimension n. If $0 \neq v \in V$ then there is $f \in Hom(V, F)$ such that $f(v) \neq 0$.

Proof: Suppose V is a vector space of dimension n over F and $0 \neq v \in V$.

Then $\{v\}$ is a linearly independent set of V as $0 \neq v$

So we get a basis of V of the form $v = v_1, v_2, \ldots v_n$

Now $f: V \to F$ defined by $f(v' = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = \alpha_1$ is a homomorphism of V into F and $f(v = v_1) = 1 \neq 0$.

20.2.6. Notation: $Hom(V,F)$ the dual of V is denoted by $\hat{V}$ *and* $(\hat{V}) = \hat{\hat{V}}$ is called the second dual of V.

20.2.7. Theorem: Let V be a vector space over F of dimension n. Then the canonical mapping ψ of V into $\hat{\hat{V}}$ is an isomorphism of V onto $\hat{\hat{V}}$.

Proof: Suppose V is a finite dimensional vector space of dimension n over a field F. we have that $\hat{V}$ and $\hat{\hat{V}}$ are dual and second dual of V.

Let $v \in V$. Define $T_V: \hat{V} \to F$ by $T_V(f) = f(V)$ for all $\hat{V}$. Now

$T_V(\alpha f_1 + \beta f_2) = (\alpha f_1 + \beta f_2)v = \alpha f_1(v) + \beta f_2(v) = \alpha T_V(f_1) + \beta T_V(f_2)$

So T_V is a linear function on $\hat{V}$ and that $T_V \in \hat{\hat{V}}$.

Define $\psi: V \to \hat{\hat{V}}$ by $\psi(v) = T_v$ is the canonical mapping of V into $\hat{\hat{V}}$.

$T_{\alpha v_1 + \beta v_2}(f) = \alpha f(v_1) + \beta f(v_2) = \alpha T_{v_1}(f) + \beta T_{v_2}(f) = (\alpha T_{v_1} + \beta T_{v_2})f,$ for all $f \in \hat{V}$.

So $T_{\alpha v_1 + \beta v_2} = \alpha T_{v_1} + \beta T_{v_2}$ and that

$\psi(\alpha v_1 + \beta v_2) = T_{\alpha v_1 + \beta v_2} = \alpha T_{v_1} + \beta T_{v_2} = \alpha\psi(v_1) + \beta\psi(v_2)$

$\therefore \psi$ is a homomorphism of V into $\hat{\hat{V}}$.

Suppose that $\psi(v_1) = \psi(v_2)$

Now $T_{v_1} = T_{v_2}$ and that $T_{v_1}(f) = T_{v_2}(f)$ for all $f \in \hat{V}$. That is $f(v_1) = f(v_2)$ for all $f \in \hat{V}$. That is $f(v_1 - v_2) = 0$ for all $f \in \hat{V}$. So $v_1 - v_2 = 0$ and that $v_1 = v_2$. So ψ is one one and that $\dim(V) = \dim \psi(V)$. But $n = \dim V = \dim \hat{V} = \dim \hat{\hat{V}}$. So $\dim \hat{\hat{V}} = n = \dim \psi(V)$ and hence $\hat{\hat{V}} = \psi(V)$ and that ψ is onto $\hat{\hat{V}}$.

Hence ψ is an isomorphism of V onto $\hat{\hat{V}}$.

20.2.8. Definition: Let V be a vector space over a field F and $\hat{V}$ be the dual of V and W be a subspace of V. Then the annihilator of W denoted by $A(W)$, is defined as

$A(W) = \{ f \in \hat{V} / f(w) = 0, \forall\, w \in W\}$.

20.2.9. Theorem: Let V be a finite dimensional vector space over F and W be a subspace of V. Then $\frac{\hat{V}}{A(W)}$ is isomorphic to $\hat{W}$ and $\dim A(W) = dim\hat{V} - dim\hat{W} = \dim V - \dim W$.

Proof: Let V be a finite dimensional vector space of dimension n over F and W be a subspace of V. Let $\hat{V}$ and $\hat{W}$ be the dual spaces of V and W respectively. Let $f \in \hat{V}$. Let $\bar{f}$ be the restriction of f to W. So $\bar{f}: W \to F$ defined by $\bar{f}(w) = f(w)$ for all $w \in W$. Clearly $\bar{f} \in \hat{W}$.

Define $T: \hat{V} \to \hat{W}$ by $T(f) = \bar{f}$ for all $f \in \hat{V}$.

$$\begin{aligned} T(\alpha f_1 + \beta f_2) &= \overline{\alpha f_1 + \beta f_2} \\ &= \alpha \bar{f_1} + \beta \bar{f_2} \\ &= \alpha T(f_1) + \beta T(f_2) \end{aligned}$$

So T is a homomorphism of $\hat{V}$ into $\hat{W}$.

$Ker\ T = \{ f \in \hat{V} : T(f) = 0 \}$

$$= \{f \in \hat{V} : \bar{f} = 0\}$$
$$= \{f \in \hat{V} : f \in A(W)\} = A(W)$$

Let $g \in \hat{W}$. We have $\dim W \leq \dim V = n$.

Let $\dim W = m$. We have a basis $w_1, w_2, \ldots w_m$ of W consisting of m vectors. This can be extended to a basis of V of the form $w_1, w_2, \ldots w_m, v_{i1}, v_{i2}, \ldots v_{ik}$ where $m + k = n$.

Let U be the linear span of $v_{i1}, v_{i2}, \ldots v_{ik}$. Now $V = W \oplus U$.

Define $f: V \to F$ by $f(V) = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m + \beta_1 v_{i1} + \beta_2 v_{i2} + \cdots + \beta_k v_{ik}$
$= g(\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m)$

Clearly f is a linear functional on V and f=g on W that is $\bar{f} = g$. So $f \in \hat{V}$ and $T(f) = \bar{f} = g$ and ψ is onto $\hat{W}$. Hence $\frac{\hat{V}}{A(W)} \cong \hat{W}$.

So $\dim \hat{V} - \dim(A(W)) = \dim \hat{W}$ and that $\dim A(W) = \dim \bar{V} - \dim \hat{W}$

$$\dim A(W) = \dim V - \dim W$$

Hence the theorem.

20.2.10.Corollary: Let V be a finite dimensional vector space and W be a subspace of V. Then $A(A(W)) = W$

Proof: V is a finite dimensional vector space over F and W is a subspace of V over F.

Let dim$V = n$ and dim $W = m$. Now n = dim$V \geq$ dim $W = m$.

Since T: V $\to \hat{\hat{V}}$ define by T(v) = g_v is a canonical isomorphism, we identify $g_v \in \hat{\hat{V}}$ with $v \in$ V.

Note that $\hat{\hat{V}} = \{g_v : v \in V\}$ and $g_v : \hat{\hat{V}} \to$ F is defined by g_v(f) = f(v).

Let $w \in W$ and let $h \in A(W)$. Now $g_w(h) = h(w)$

So $g_w \in A(A(W))$ and that $w \in A(A(W))$ and that $W \subseteq A(A(W))$.

We have $\dim A(A(W)) = \dim \hat{\hat{V}} - \dim A(W)$

$= \dim \hat{\hat{V}} - (\dim \hat{V} - \dim W)$

$= n - (n - m) = m = \dim W$.

Since $W \subseteq A(A(W))$ and $\dim W = m = \dim A(A(W))$.

Therefore, $W = A(A(W))$.

20.3 SUMMARY:

We defined dual space $\hat{V}$ of a vector space V. For a finite dimension vector space V it is shown that dim$\hat{V}$ = dimV. The annihilator A(W) of a subspace W of a vector space V is expressed interms of dimV and dimW and some results on them are given.

20.4 TECHNICAL TERMS:

- Hom(V, W), V, W are vector spaces over a field F.
- A(W), annihilator of a subspace W of a vector space V.

20.5 SELF ASSESSMENT QUESTION:

1. prove that A(S) = A(L(S)), S is a subset of a vector space V and L(S) is the linear span of S.

20.6 SUGGESTED READINGS:

1) I.N. Herstein, 'Topics in Algebra', Second Edition, John Wiley & Sons, 1999.
2) P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul. "Basic Abstract Algebra", Second Edition, Cambridge Press, 1995.
3) Thomas W. Hungerford, 'Algebra', Springer - Verlag, New York, 1974.
4) Serge Lang, 'Algebra', Revised Third Edition, Springer-Verlag, New York, 2002.

-Dr. Noorbhasha Rafi