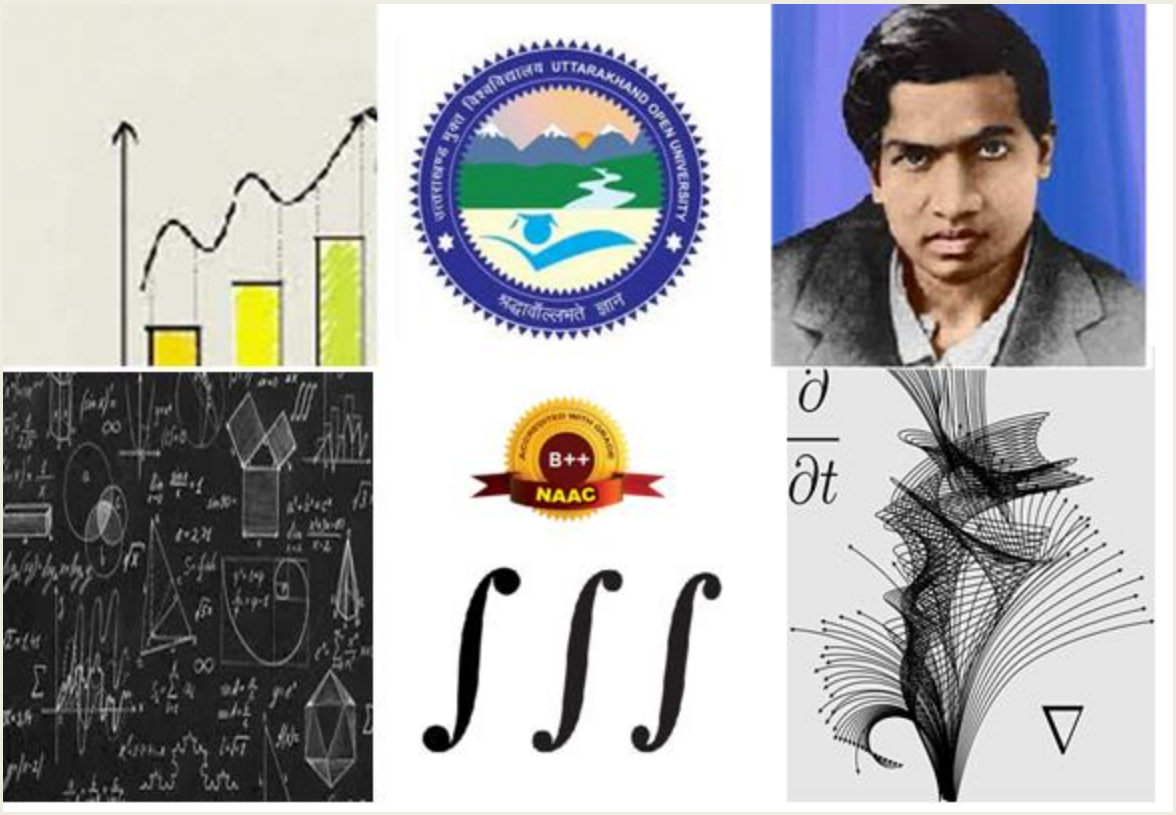
Master of Science
(FIRST SEMESTER)

MAT 501
ADVANCED ABSTRACT ALGEBRA



DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCES
UTTARAKHAND OPEN UNIVERSITY
HALDWANI, UTTARAKHAND
263139

COURSE NAME: ADVANCED ABSTRACT ALGEBRA

COURSE CODE: MAT 501

Department of Mathematics
School of Science
Uttarakhand Open University
Haldwani, Uttarakhand, India,
263139

BOARD OF STUDIES-FEBRUARY 2023

Editor

Dr. Jyoti Rani
Assistant Professor
Department of Mathematics,
School of Sciences, Uttarakhand Open University

Unit Writer	Block	Unit
Dr. Kamlesh Bisht Assistant Professor (AC) Department of Mathematics Uttarakhand Open University	**I, II, III, IV**	**01 – 09, 11-14**
Dr. Jyoti Rani Assistant Professor Department of Mathematics Uttarakhand Open University	**IV**	**10**

Course Title and Code : ADVANCED ABSTRACT ALGEBRA (MAT-501)

Copyright : Uttarakhand Open University

Edition : 2023

COURSE INFORMATION

The present self learning material **"Advanced Abstract Algebra"** has been designed for M.Sc. (First Semester) learners of Uttarkhand Open University, Haldwani. This self learning material is writing for increase learner access to high-quality learning materials.This course is divided into 14 units of study. The first unit is devoted to the normal subgroups and quotient groups, Unit 2 explained about Conjugate element, Normalizer and Center of group and Unit 3 explained about the homomorphism and isomorphism mapping between the groups. Unit 4 explained to Cayley's theorem and concept of class equation Unit 5 explain about the direct product of groups and Cauchy's theorem for finite abelian groups and Unit 6 are focused on Sylow's theorems and their application. The aim of Unit 7, 8 and 9 are to introduce the concept composition series, jordan holder theorem and solvable group. Unit 10 and Unit 11 explain about the important concept and their related theorems of rings, ideal, integral domain and fields. Unit 12 explained about the unique factorization domain, principal ideal domain and euclidean domain and Unit 13 explain the polynomial ring and irreducibility criteria. Unit 14 will explain the field extension, Galois groups and Galois extension. This material also used for competitive examinations. The basic principles and theory have been explained in a simple, concise and lucid manner. Adequate number of illustrative examples and exercises have also been included to enable the leaner's to grasp the subject easily.

Contents

Course: Advanced Abstract Algebra **Course code: MAT501**
Credit: 4

BLOCK I

NORMAL SUBGROUPS AND HOMOMORPHISM

Unit-1: NORMAL SUBGROUP AND QUOTIENT GROUPS

CONTENT:

1.1 *INTRODUCTION*

Évariste Galois was a French mathematician born in Bourg-la-Reine who possessed a remarkable genius for mathematics. Among his many contributions, Galois **founded abstract algebra and group theory**, which are fundamental to computer science, physics, coding theory and cryptography.

It is tribute to the genius of Galois that he recognized that those subgroups for which the left and right cosets coincide are distinguished ones. Very often in mathematics the crucial problem is to recognize and to discover what the relevant concepts are.

Évariste Galois
25 October 1811 – 31 May 1832

In the previous sessions, we have already learned that how any set *G* can be formed a group with respect to (*w.r.t.*) the given operation. We have also learned about various types of groups and their properties. Some applications of group like subgroup, cyclic group, order of the group, permutation group, homomorphism, isomorphism, center of the group, cosets and Lagranges theorem are already studies in previous classes. In this unit we will learn about the Normal subgroups and its use to construct the quotient group.

As we know that, in a group *G*, it is not always true that $gH = Hg$ for all $g \in G$ where, *H* is a subgroup of a group *G*.

Example 1: Let *G* be a permutation group of degree 3 on three symbol 1, 2, 3 and $H = \{I, (1\ 2)\}$ is a subgroup of *G*. Since $a = (2, 3) \in G$ then the left coset of *a* in *G* i.e.,

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

And the right coset of *a* in *G* is,

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

Here clearly, we can see that $aH \neq Ha$

In other words, right cosets are not always the same as left cosets. Group theory depends heavily on the subgroups for which this characteristic holds because they enable the creation of a new class of groups known as factor or quotient groups. Homomorphisms, a generalisation of isomorphisms, can be used to study factor groups.

1.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the basic definition of normal subgroup and quotient group.
- Implement the application of theorems into various problem
- Construction of various types of quotient groups

1.3 *NORMAL SUBGROUP*

Definition: A subgroup *H* of a group *G* is normal in *G* if $gH = Hg$ for all $g \in$ G. In other words, the right and left cosets of a group *G* must be exactly the same for a subgroup *H* to be considered normal subgroup.

If *H* is a normal subgroup of the group *G* then symbolically it is represented as $H \trianglelefteq G$.

Example 2: Let G be a permutation group of degree 3 on three symbol 1, 2, 3 and $H = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ is a subgroup of G. Since $a = (1, 2) \in G$ then the left coset of a in G i.e.,

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

And the right coset of a in G is,

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

Similarly, we can see that $aH = Ha\ \forall a \in G$

So, we can say that H is the normal subgroup of G.

Note 1: If we are saying that H is a normal subgroup of G i.e., $gH = Hg$ for all $g \in$ G then its mean that there exist $h \in H$ such that gh is any element of gH which will be equal to any element of $h'g$ where $h' \in H$ i.e., $gh = h'g$.

In example 2, $(1\ 2)(1\ 3\ 2) = (1\ 2\ 3)(1\ 2)$

Proper subgroup: A subgroup H of a group G is called proper subgroup of G if $H \neq G$ and it is represented as $H < G$ and it is read as "H is a proper subgroup of G".

Since, $G \subseteq G$ *i.e.*, G is subset of itself so G, is called improper subgroup of G.

A subgroup H which contains only identity element *i.e.*, $H = \{e\}$ is called the trivial subgroup of G.

1.3.1 *SIMPLE GROUP*

Definition: If a group has no proper normal subgroup is called a simple group.

Theorem 1: If G be a group and H is the subgroup of G. Then the following statement are equivalent.

1. The subgroup H is normal in G
2. For all $a \in G$, $aHa^{-1} \subseteq H$
3. For all $a \in G$, $aHa^{-1} = H$

Proof: $(1) \Rightarrow (2)$. We have given H is the normal subgroup of G then $aH = Ha\ \forall a \in G$. It means for a given $h \in H$, $a \in G$ there exist $h' \in H$ such that $ah = h'a$. Since $a \in G$ and G is the group then $a^{-1} \in G$.

$\Rightarrow (ah)a^{-1} = (ha)a^{-1}$

$\Rightarrow aha^{-1} = h \in H$

So, $aHa^{-1} \subseteq H\ \ \forall a \in G$

$(2) \Rightarrow (3)$ Let $a \in G$ and H is normal subgroup of G, then we have already prove that $aHa^{-1} \subseteq H$. Now we have only to show that $H \subseteq aHa^{-1} \ \forall a \in G$.

Since $a \in G \Rightarrow a^{-1} \in G$

Therefore we have $a^{-1}H\left(a^{-1}\right)^{-1} \subseteq H \ \forall a \in G$

$\Rightarrow a^{-1}Ha \subseteq H \ \forall a \in G$

$\Rightarrow a\left(a^{-1}Ha\right)a^{-1} \subseteq aHa^{-1} \ \forall a \in G$

$\Rightarrow a\left(a^{-1}Ha\right)a^{-1} \subseteq aHa^{-1} \ \forall a \in G$

$\Rightarrow H \subseteq aHa^{-1} \ \forall a \in G$

Now again for each $a \in G$, $aHa^{-1} \subseteq H$ and $H \subseteq aHa^{-1}$

So, for all $a \in G$, $H = aHa^{-1}$

$(3) \Rightarrow (1)$ Suppose that $H = aHa^{-1} \ \forall a \in G$ then we have to prove that H is normal in G.

Since, for all $a \in G$, $H = aHa^{-1}$

$\Rightarrow Ha = \left(aHa^{-1}\right)a \ \forall a \in G$

$\Rightarrow Ha = aH \ \ \forall a \in G$

$\Rightarrow$ each left coset of H in G is a right coset of H in G.

$\Rightarrow H$ is normal subgroup of G.

Theorem 2: A subgroup H of a group G is normal in G iff the product of two right or left coset of H in G is again a right or left coset of H in G.

Proof: Suppose H is a normal subgroup in G and Ha, Hb are two right coset of H in G where, $a, b \in G$. Then

$$(Ha)(Hb) = H(aH)b$$

$$= H(Ha)b \qquad [\because H \text{ is normal } \Rightarrow Ha = aH\ ]$$

$$= HHab \qquad [\because HH = H\ ]$$

$$= Hab \qquad [\, a \in G, b \in G \Rightarrow ab \in G\,]$$

Therefore, Hab is also a right coset of H in G.

Conversely, we will suppose that the product of two right cosets of H in G is again a right coset of H in G. Let x be any arbitrary element of G then x^{-1} will also an element of G. So, Hx and Hx^{-1} are two distinct right cosets of H in G. Thus, $HxHx^{-1}$ is also a right coset of H in G. Therefore we must have,

$HxHx^{-1} = H \ \forall x \in G$

$\Rightarrow h_1xhx^{-1} \in H \ \forall x \in G$ and $\forall h_1, h \in H$

$\Rightarrow h_1^{-1}\left(h_1 x h x^{-1}\right) \in h_1^{-1} H \ \forall x \in G$ and $\forall h_1, h \in H$

$\Rightarrow xhx^{-1} \in H \ \forall x \in G$ and $\forall h \in H$ [$\because h_1^{-1} H = H$ as $h_1^{-1} \in H$ since $h_1 \in H$]

$\Rightarrow H$ is a normal subgroup of *G*.

Theorem 3: Intersection of two normal subgroup of a group is also a normal subgroup of the group.

Solution: Let *G* be a group and *H, K* are of its two normal subgroup of *G*. Now, we have to prove that $H \cap K$ is also a normal subgroup of *G*. Let *a* be any element of $H \cap K$ *i.e.*,

$x \in H \cap K \Rightarrow x \in H$ *and* $x \in K$

Since, *H* and *K* are both normal in *G*. Therefore, $a \in G, h \in H \Rightarrow axa^{-1} \in H$

Similarly, $a \in G, x \in K \Rightarrow axa^{-1} \in K$

Now, again $axa^{-1} \in H$, $axa^{-1} \in K \Rightarrow axa^{-1} \in H \cap K$

Hence $H \cap K$ is a normal subgroup of *G*.

Corollary: Arbitrary collection of normal subgroup is also a normal subgroup of the group i.e., let *G* be a group and let $\{H_n : n \in \wedge\}$ be the family of normal subgroup of *G* where $\wedge$ is the index set then $\underset{n\in\wedge}{\cap} H_n$ is the arbitrary intersection of the family of normal subgroups which is also a normal subgroup of G.

Solved Examples

Example 3: Show that each subgroup of the Abelian group *G* is a normal subgroup of the group.

Solution: Let *G* be a Abelian group and *H* is a subgroup of the group. Suppose that $h \in H$ and $x \in G$.

Now consider, $xhx^{-1} = x(x^{-1}h)$

$= (xx^{-1})h$

$= eh = h \in H$

So, $\forall x \in G, h \in H, xhx^{-1} \in H \Rightarrow H$ is a normal subgroup of *G*.

Example 4: Prove that the alternating subgroup A_n is the normal subgroup of the symmetric group S_n

Solution: Suppose that $\alpha \in S_n$ and $\beta \in A_n$. As we know that A_n is collection of all even permutation of S_n so, β is a even permutation. Now, there are two cases arises,

Case I: If α is odd permutation then α^{-1} is also an odd permutation. As we know that product of odd and even permutation is odd permutation, it means $\alpha\beta$ is odd permutation. Similarly, product of two odd permutation is even permutation *i.e.*, $\alpha\beta\alpha^{-1}$ is even permutation.

So, for $\alpha \in S_n, \beta \in A_n, \alpha\beta\alpha^{-1} \in A_n$. Thus, A_n is normal subgroup.

Case II: If α is even permutation then α^{-1} is also an even permutation. As we know that product of two even permutation is even permutation, it means $\alpha\beta$ is even permutation. Similarly, product of two even permutation $\alpha\beta$ and α^{-1} is even permutation *i.e.*, $\alpha\beta\alpha^{-1}$ is even permutation.

So, for $\alpha \in S_n, \beta \in A_n, \alpha\beta\alpha^{-1} \in A_n$. Thus, A_n is normal subgroup.

From the both cases we have conclude that A_n is normal subgroup of S_n.

Example 5: If *H* is a subgroup of index 2 in *G* then *H* is a normal subgroup of *G*.

Solution: If H is a subgroup of index 2 in G, it means, number of distinct right (left) coset of H in G are 2. So, *G* can be written in the union of two of its distinct right (left) cosets *i.e.*, $G = H \cup Hx = H \cup xH$, here $x \notin H$ because if it is $xH = H = Hx$.

As we know that no element common to H and xH therefore, we must have $xH = Hx \forall x \in G$

Hence *H* is normal subgroup of *G*.

e.g. Index of alternating subgroup A_n in the symmetric group S_n is 2. So, A_n is the normal subgroup in the symmetric group S_n**.**

Example 6: If *H* is normal in *G* and *K* is a subgroup of *G* such that $H \subseteq K \subseteq G$. Then, show that *H* is also a normal subgroup of *K*.

Solution: We have given that *H* is normal in *G* so, *H* will also a subgroup of *G*. Since, $H \subseteq K$ where, *K* is a subgroup of *G*. So we have only to show that *H* is also a normal subgroup of *K*. Let *x* be any arbitrary element of *K* then *x* will also belong to *G* therefore we have $Hx = xH$. Since, *H* is a subgroup of *G* and $\forall x \in K$ we have $Hx = xH$. Thus, *H* is normal subgroup of *K*.

Example 7: If *N* is normal in *G* and *H* is subgroup of *G* then show that $H \cap N$ is normal subgroup of *H*.

Solution: As we know that intersection of two subgroup of *G* is also a subgroup of *G* then $H \cap N$ will be subgroup of *G*. Similarly, since $H \cap N \subseteq H$ so, $H \cap N$ will also subgroup of *H*. Now, only to prove that $H \cap N$ is normal in *H*.

Let *x* be any element of *H* and *a* be any element of $H \cap N$ then *a* will belong in both *H* and *N*. Since, *N* is normal in *G* then $axa^{-1} \in N$. Again,

$x, a \in H \Rightarrow axa^{-1} \in H$

Thus, we can say that $axa^{-1} \in H \cap N$

i.e., $H \cap N$ is normal subgroup of *H*.

Example 8: Prove that every complex is commutative with normal subgroup.

Solution: Let *N* is a normal subgroup and *H* is any complex of the group *G*. Then we have to prove that *NH = HN*.

Let $nh \in NH \text{ where } n \in N, h \in H$. We can rewrite $nh = hh^{-1}nh = h(h^{-1}nh)$. Since, N is normal subgroup therefore, $h^{-1}nh \in N$. Hence $nh \in HN$ which means, $NH \subseteq HN$.

Again, let $hn \in HN \text{ where } n \in N, h \in H$. We can rewrite $hn = hnh^{-1}h = \left(hnh^{-1}\right)h$. Since, N is normal subgroup therefore, $hnh^{-1} \in N$. Hence $hn \in NH$ which means, $HN \subseteq NH$.

Hence $NH = HN$.

Example 9: If N is normal subgroup of G and H is subgroup of G, Prove the following

(i) HN is a subgroup of G

(ii) N is a normal subgroup of HN.

Solution: As, we know by theorem that if H, K are subgroup of G, then HK is subgroup of G *iff* $HK = KH$. Using the previous example, HN will also a subgroup because N and H both are subgroup of G such that $NH = HN$.

Now HN is subgroup of G and N is normal subgroup of G also $N \subseteq HN$. Therefore, N is subgroup of HN. We have only to prove that N is a normal in HN. Let h_1n_1 be arbitrary element of HN and n be any element of N. Then $h_1 \in H, n_1 \in N$ and we have $(h_1n_1)n(h_1n_1)^{-1} = h_1(n_1nn_1^{-1})h_1^{-1} \in N$. Since N is normal in G and $n_1nn_1^{-1} \in N, h_1 \in G$. Therefore N is a normal subgroup of HN.

Example 10: If N and M are two normal subgroups of G such that $N \cap M = \{e\}$. Then show that each element of N commutes with each element of M.

Solution: Since N and M are two normal subgroups of G such that $N \cap M = \{e\}$. Then to prove that for any element $n \in N, m \in M$

$\Rightarrow nm = mn \; \forall m, n$

Consider the element $nmn^{-1}m^{-1}$. As we know $mnm^{-1} \in N$ because N is normal and $n \in N$ therefore, $nmn^{-1}m^{-1} \in N$.

Again, as we know $nmn^{-1} \in M$ because M is normal and $m \in M$ therefore, $nmn^{-1}m^{-1} \in M$.

Now, $nmn^{-1}m^{-1} \in N$ and $nmn^{-1}m^{-1} \in M \Rightarrow nmn^{-1}m^{-1} \in N \cap M$

$\Rightarrow nmn^{-1}m^{-1} = \{e\}$ [Because, $N \cap M = \{e\}$]

$\Rightarrow nm = mn \; \forall m \in M, n \in N$

i.e., every element of N commutes with every element of M.

Example 11: If in a group G, H is the only subgroup of finite order m then H is normal in G.

Solution: We have given H is subgroup of G such that $O(H) = m$. To prove this example, first we consider the set $xHx^{-1} = \left\{xhx^{-1} : h \in H\right\}$ and we will prove that this set is the subgroup of G. As we

know by the theorem that any set H will subgroup of G if $ab^{-1} \in H \; \forall a, b \in H$. Let $h_1, h_2 \in H$ then $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$

Now consider, $xh_1x^{-1}\left(xh_2x^{-1}\right)^{-1} = xh_1x^{-1}\left(xh_2^{-1}x^{-1}\right) = xh_1\left(x^{-1}x\right)h_2^{-1}x^{-1}$

$= xh_1(e)h_2^{-1}x^{-1} = x(h_1h_2^{-1})x^{-1} \in xHx^{-1}$

$\Rightarrow h_1h_2^{-1} \in xHx^{-1} \; \forall h_1, h_2 \in xHx^{-1}$. Hence, xHx^{-1} is subgroup of G.

Now we will prove that $O(xHx^{-1}) = m$. Let $H = \{h_1, h_2, h_3, ..., h_m\}$ where all $h_i, i = 1 to m$ are distinct then $xHx^{-1} = \{xh_1x^{-1}, xh_2x^{-1}, xh_3x^{-1}, ..., xh_mx^{-1}\}$. Here, no element in xHx^{-1} are same because if it is,

$xh_ix^{-1} = xh_jx^{-1} \Rightarrow h_i = h_j$, which is not possible. So, $O(xHx^{-1}) = m$.

But we have H is the only such subgroup of order m. Therefore we must have, $xHx^{-1} = H \; \forall x \in G$. Thus, H is normal subgroup of G.

Example 12: By an example verify that if H is normal in G and K is normal in H then K may not be normal in G.

Solution: Let us consider the following subgroup of the group S_4 on the four symbols *a, b, c, d*.

$G = \{I, (a\,b\,c), (a\,d\,c\,b), (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c), (a\,c), (b\,d)\}$

$H = \{I, (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c)\}$

$K = \{I, (a\,b)(c\,d)\}$

As we can easily seen that H is a subgroup of G and K is a subgroup of H. Index of H in G is 2 *i.e.*, $[G:H] = 2$, it means H is normal in G. Similarly, index of K in H is 2 *i.e.*, $[H:K] = 2$, it means K is normal in H. $[\because [G:H] = O(G)/O(H) = 8/4 = 2]$

Here, K is not normal in G because for the element $(a,b,c,d) \in G$ and the element $(a,b)(c,d) \in K$.

We have $(a\,b\,c\,d)(a\,b)(c\,d)(a\,b\,c\,d)^{-1} = (a\,b\,c\,d)(a\,b)(c\,d)(d\,c\,b\,a) = (a\,d)(b\,c) \notin K$

Thus, K is not normal subgroup of G.

Example 13: If H is subgroup of G, let $N(H) = \{x \in G : xhx^{-1} = H\}$ then show that

(1) $N(H)$ is the largest subgroup of G in which H is normal.

(2) H is normal in G iff $N(H) = G$.

Solution 1: In example 11, we have already prove that $N(H)$ is the subgroup of G which is normal in G.

First we have to prove that H is a normal subgroup of $N(H)$. Let $h \in H$, therefore $hHh^{-1} = H$.

Thus $h \in N(H)$ *i.e.,* $H \subseteq N(H)$. So, *H* is subgroup of *N*(*H*). To show that *H* is normal in *N*(*H*). Let $x \in N(H)$, then $xHx^{-1} = H$

$\Rightarrow xH = Hx \forall x \in N(H)$

$\Rightarrow$ *H* is normal in *N*(*H*).

Now, we have to prove that *N*(*H*) is largest such subgroup in which *H* is normal. For it, let *K* is a subgroup of *G* in which *H* is normal then we have only to prove that $K \subseteq N(H)$.

Let $k \in K$, since *H* is normal in *K*, therefore we have $Hk = kH$

$\Rightarrow kHk^{-1} = H \ \forall k \in K$

$\Rightarrow k \in N(H)$

$\Rightarrow K \subseteq N(H)$

2: Let *H* is the normal subgroup of *G* and $x \in G$. Then $xH = Hx \forall x \in G$

$\Rightarrow xHx^{-1} = H \forall x \in G$

$\Rightarrow x \in N(H)$ therefore $G \subseteq N(H)$ but we know $N(H) \subseteq G$.

Thus, $G = N(H)$

Conversely, let $G = N(H)$ then $x \in G \Rightarrow x \in N(H)$

$\Rightarrow xHx^{-1} = H \forall x \in G$

$\Rightarrow xH = Hx \forall x \in G$

H is normal in *G*.

1.4 *QUOTIENT GROUP*

Definition: If *H* is a normal subgroup of a group *G*. Then the collection of all distinct cosets of *H* in *G* denoted by *G*/*H* is a group with respect to the operation multiplication of cosets defined as,

$$(aH)(bH) = abH \text{ 'or' } (Ha)(Hb) = Hab \ \forall a, b \in G$$

Or

If *H* is a normal subgroup of a group *G*, then the set

$G/H = \{Ha : a \in G\}$ is always form a group under the composition multiplication of cosets such that

$(Ha)(Hb) = Hab \ \forall a, b \in G$

Note: If *H* is a normal subgroup of the additive group *G*. Then the set G/H is defined as $G/H = \{H + a : a \in G\}$ with respect to the operation addition of cosets such that

$(H + a) + (H + b) = H + (a + b) \forall a, b \in G$

Theorem 13: Set of all distinct cosets of normal subgroup of a group is a group with respect to composition multiplication of cosets.

Proof: Let us consider collection of distinct right (left) cosets of normal subgroup H under G is

$G/H = \{Ha : a \in G\}$

and the composition multiplication of cosets is

$(Ha)(Hb) = Hab \ \forall a, b \in G$

Closure axioms: Let $Ha, Hb \in G/H$ where $a, b \in G$ then

$(Ha)(Hb) = H(aH)b = H(Ha)b = HHab = Hab \in G/H$

Since we know that if H is normal subgroup of G then

(i) $Ha = aH \ \forall a \in G$

(ii) $HH = H$

And also if G is a group then it will satisfy closure property *i.e.*, if $a, b \in G \Rightarrow ab \in G$

Associativity: Let $Ha, Hb, Hc \in G/H$ where $a, b, c \in G$

Now consider, $(Ha)[(Hb)(Hc)] = (Ha)[H(bH)c] = (Ha)[H(Hb)c] = (Ha)(Hbc)$

$= Ha(bc) = H(ab)c = H(ab)(Hc) = [(Ha)(Hb)](Hc)$

[Because G is group so it will satisfy associative property]

Existence of identity: We know that $H = He \in G/H$ where e is the identity element of G, then we have only to prove that H is the identity element of the group G/H.

Let $Ha \in G/H$ then $(He)(Ha) = H(ea) = Ha$

$\Rightarrow H$ is the identity element of the group G/H.

Existence of inverse: Let $Ha \in G/H$. Then $Ha^{-1} \in G/H$ [Because if $a \in G$ then $a^{-1} \in G \Rightarrow Ha^{-1} \in G/H$]

Now, $(Ha)(Ha^{-1}) = H(aa^{-1}) = He = H$

So, coset Ha is the inverse of Ha^{-1} in G/H

Hence, collection of distinct right (left) of normal subgroup H in G is form a group with respect to the operation product of cosets.

Example 14: The alternating group $A_3 = \{I, (123), (132)\}$ is the normal subgroup of the symmetric group $S_3 = \{I, (12), (13), (23), (123), (132)\}$ then $S_3 / A_3 = \{A_3, (23)A_3\}$ is the quotient group.

Example 15: Consider the normal subgroup of $3Z$ of Z. The coset of $3Z$ in Z are,

$0 + 3Z = \{..., -6, -3, 0, 3, 6, 9, ...\}$

$1 + 3Z = \{..., -5, -2, 1, 4, 7, 10, ...\}$

$2+3Z=\{...,-4,-1,2,,5,8,11...\}$

Here, $Z=(0+3Z)\cup(1+3Z)\cup(2+3Z)$

The composition table of the group $Z/3Z$ is given below.

+	$0+3Z$	$1+3Z$	$2+3Z$
$0+3Z$	$0+3Z$	$1+3Z$	$2+3Z$
$1+3Z$	$1+3Z$	$2+3Z$	$0+3Z$
$2+3Z$	$2+3Z$	$0+3Z$	$1+3Z$

In general, the cosets of nZ in Z are

$Z=(0+nZ)\cup(1+nZ)\cup(2+nZ)\cup(3+nZ)\cup...\cup((n-1)+nZ)$ then

$G/nZ=\{(0+nZ),(1+nZ),(2+nZ),(3+nZ),...,((n-1)+nZ)\}$

The sum of the cosets $k+Z$ and $l+Z$ is $k+l+Z$. Notice that we have written our cosets additively, because the group operation is integer addition.

Example 16: If *H* is a normal subgroup of the finite group *G* then $O[G/H]=\dfrac{O(G)}{O(H)}$.

Solution: As we know that $O[G/H]=$Number of distinct right coset of *H* in *G*.

$\Rightarrow O[G/H]=$Index of *H* in *G*.

$$\Rightarrow O[G/H]=\frac{Number\ of\ element\ in\ G}{Number\ of\ element\ in\ H}$$

$$\Rightarrow O[G/H]=\frac{O(G)}{O(H)}$$

Example 17: Prove that corresponding to every *Abelian* group its quotient group is *Abelian* but their converses need not to be true.

Solution: Let G be a Abelian group and H is its normal subgroup. If elements $a,b\in G$ are such that Ha, Hb are distinct right cosets of quotient group G/H.

Now, $(Ha)(Hb)=H(ab)=H(ba)=(Hb)(Ha)$ [Since G is Abelian $\Rightarrow ab=ba\ \forall a,b\in G$]

$\Rightarrow G/H$ is Abelian group.

But converse is need not be true. Since $S_3/A_3=\{A_3,(23)A_3\}$ is Abelian group because order of $O[S_3/A_3]=6/3=2$ which is prime and we know that every group of prime order is Abelian while S_3 is not a Abelian group.

Example 18: If *H* is normal in *G* and *a* be any element of order *n* in *G* then order of the element *Ha* in *G*/*H* is divisor of *n*.

Solution: As we know that the identity element of the quotient group G/H is H itself. We have given in a group G, $a \in G$ *s.t.* $O(a) = n$ *i.e.* $a^n = e$. Let us assume $O(Ha) = m$.

Now consider,

$(Ha)^n = (Ha)(Ha)(Ha)....upto\, n\, times = H(aaa...upto\, n\, times) = Ha^n = He = H$

But we have already assume that $O(Ha) = m$ *i.e.*, $(Ha)^m = H$.

$\Rightarrow O(Ha) / O(a)$ [If order of any element a in a group G is n then $a^m = e$ *iff* $n \mid m$]

Check your progress

Problem 1: What will be the order of the group $O\left(\frac{Q_8}{\{1,-1\}}\right)$?

Problem 2: Check the distinct right and left coset of S_3?

Problem 3: Check that A_5 is the normal subgroup of S_5?

1.5 *SUMMARY*

In this unit, we have studied the basic definition of Normal subgroup, Simple group and Quotient group. We have also learn about the above discussed group's related theorems and there implementation in various examples. The overall summarization of this units are as follows:

- Right cosets are not always the same as left cosets
- Alternating subgroup A_n is the normal subgroup of the symmetric group S_n
- If a group has no proper normal subgroup is called a simple group.
- Quotient group always forms a group not a subgroup because identity element of group and subgroup are always same while quotient group and group has always different identity

1.6 *GLOSSARY*

- H is a subgroup of the group G is represented symbolically as $H \leq G$.
- H is a normal subgroup of the group G is represented symbolically as $H \trianglelefteq G$.
- Group with no proper normal subgroup is called a simple group.

1.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.

- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5^{th} Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.

1.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3^{rd} Edition), Wiley, 2011.

1.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that alternating group (A_n) is the normal subgroup the symmetric group (S_n).

2. Prove that a factor group of a cyclic group is cyclic.

3. Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a normal subgroup of G.

4. Show that S_4 has a unique subgroup of order 12.

5. Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n.

Short Answer Type Question:

6. Give one example each of the following

(a) A subgroup H of a group G which is not normal in G.

(b) A non-abelian subgroup H of a non-abelian subgroup G which is normal in G.

7. If $|G| = 30, |H| = 5$ then what will be $|G/H|$.

8. Prove that each subgroup of cyclic group is normal.

9. Determine the coset decomposition of the subgroup $H = \{I, (12)\}$ corresponding to the symmetric group S_3.

Fill in the blanks:

10. Product of two right coset in a group G is …….. in G.

11. Every subgroup H of index 2 in H is ……. in G.

12. If H is normal subgroup of G then G/H is called ……..

1.10 *ANSWERS*

Answer of self cheque question:

1. 4 **2.** $I, (12), (1,2,3)$ **3.** Yes

Answer of terminal question:

7. $|G/H| = 6$ **10.** Right coset **11.** Normal **12.** Quotient group

Unit-2: CONJUGATE ELEMENT, NORMALIZER AND CENTER OF GROUP

CONTENT:

2.1 *INTRODUCTION*

The main purpose to learn about the conjugate element in a group is that to differentiate any group into different conjugate classes by its property of satisfying the condition of equivalence relation. After partition group into different conjugate classes we will learn about the important definition of normalizer of any element in a group and centre of the group which will help us to define the class equation.

In this unit we will also learn various theorems of conjugate element, normalizer and centre of the group and their related application to solve different types of examples.

Cayley table for D_4 showing elements of the center, {e, a^2}, commute with all other elements (this can be seen by noticing that all occurrences of a given center element are arranged symmetrically about the center diagonal or by noticing that the row and column starting with a given center element are transposes of each other).

∘	E	B	a	a^2	a^3	ab	a^2b	a^3b
E	**E**	B	a	a^2	a^3	ab	a^2b	a^3b
B	B	**E**	a^3b	a^2b	ab	a^3	a^2	a
A	a	Ab	a^2	a^3	**e**	a^2b	a^3b	b
a^2	a^2	a^2b	a^3	**e**	a	a^3b	b	ab
a^3	a^3	a^3b	**e**	a	a^2	b	ab	a^2b
Ab	ab	A	b	a^3b	a^2b	**e**	a^3	a^2
a^2b	a^2b	a^2	ab	b	a^3b	a	**e**	a^3
a^3b	a^3b	a^3	a^2b	ab	b	a^2	a	**e**

2.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the concept of conjugate element and equivalence relation in cojugacy.
- Understand the application of normalize of an element.
- Understand about the special type of normal subgroup name as center of the group.

2.3 *CONJUGATE ELEMENT*

Definition: Two elements a and b in a group G are said to be conjugate to each other or b is said to be conjugate to a if $\exists x \in G$ *s.t.*

$$b = x^{-1}ax$$

Then b is called transform of a by x. Symbolically, it is denoted by $b \sim a$ and this relation in G is called relation of conjugacy.

Theorem 1: Conjugacy relation is an equivalence relation on G.

Proof: Reflexivity: Let a be any arbitrary element of a group G and e is the identity of the group. Then

$a = e^{-1}ae \Rightarrow a \sim a \; \forall \; a \in G$. Therefore the relation is reflexive.

Symmetry: We have to prove if $a \sim b$ then $b \sim a$. Let $a \sim b$ then $\exists x \in G$ *s.t.*

$\Rightarrow a = x^{-1}bx$

$\Rightarrow xax^{-1} = x\left(x^{-1}bx\right)x^{-1} \Rightarrow xax^{-1} = b$

As we know if $x \in G$ then $x^{-1} \in G$

Transitivity: Let $a \sim b$ and $b \sim c$ then $a = x^{-1}bx, b = y^{-1}cy$ for some $x, y \in G$.

Again, $a = x^{-1}\left(y^{-1}cy\right)x$

$\Rightarrow a = x^{-1}y^{-1}cyx = (yx)^{-1}c(yx)$ [Since G is a group then $yx \in G, \left(yx\right)^{-1} \in G$]

$\Rightarrow a \sim c$ and thus, relation is transitive.

Hence, conjugacy is an equivalence relation.

Classes of conjugate elements: The differences between the classes are follows:

(1) Elements from the same classes will be conjugate.

(2) Different elements from different classes will be not conjugate.

The collection of all elements which are conjugate to $a \in G$ will be denoted by $C(a)$ or $\tilde{a}$ and defined as:

$C(a) = \left\{x \in G \middle| x \sim a\right\}$ or $C(a) = \left\{b \in G \middle| b = x^{-1}ax\right\}$

For the finite group G, number of distinct element in $C(a)$ will be denoted by c_a.

2.4 *NORMALIZER OF AN ELEMENT OF A GROUP*

Definition: If G is a group and a be any arbitrary element of a group then normalizer of a is the collection of such elements in G which commutes with a. It is denoted by $N(a)$ and defined as:

$N(a) = \left\{x \in G \middle| ax = xa\right\}$

Note 1: If e is the identity element of G then $N(e) = G$

2: If G is abelian group and $a \in G$ then $N(a) = G$

Theorem 2: The normalizer of $a \in G$ is the subgroup of G.

Proof: Since, $N(a) = \left\{x \in G \middle| ax = xa\right\}$. Let x, y are any element of G then $ax = xa, ay = ya$. First, we will show that, $y^{-1} \in G$. Since, $y \in G \Rightarrow y^{-1} \in G$ because G is a group.

Now, $y^{-1}\left(ay\right)y^{-1} = y^{-1}(ya)y^{-1}$ [Pre and post multiply by y^{-1} in $ay = ya$]

$\Rightarrow y^{-1}a(yy^{-1}) = (y^{-1}y)ay^{-1}$ [G satisfied the associativity]

$\Rightarrow y^{-1}ae = eay^{-1}$ [e is the identity element of G]

$\Rightarrow y^{-1}a = ay^{-1}$

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

Now we have to prove that $xy^{-1} \in N(a)$

Consider, $a(xy^{-1}) = (ax)y^{-1}$

$\Rightarrow a(xy^{-1}) = (xa)y^{-1}$ [$ax = xa$]

$\Rightarrow a(xy^{-1}) = x(ay^{-1})$ [G satisfied the associativity]

$\Rightarrow a(xy^{-1}) = x(y^{-1}a)$ [$y^{-1}a = ay^{-1}$]

$\Rightarrow a(xy^{-1}) = (xy^{-1})a$ [G satisfied the associativity]

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

Hence, normalizer of any element $a \in G$ *i.e.*, $N(a)$ is the subgroup of G.

Theorem 3: Any two elements of a group give rise to same conjugate to $a \in G$ *iff* they belong to the same right coset of normalizer of a in G.

Proof: Let us consider, $x, y \in G$ then $x \in N(a)x$ and $y \in N(a)y$. Since x, y are in the same right coset of $N(a)$ in G.

$\Leftrightarrow N(a)x = N(a)y$ [If H is subgroup and $x \in H$ then $Hx = H$]

$\Leftrightarrow xy^{-1} \in N(a)$ [If H is a subgroup of G, then $Ha = Hb \Leftrightarrow ab^{-1} \in H$]

$\Leftrightarrow axy^{-1} = xy^{-1}a$ [By definition of normalizer of an element of G]

$\Leftrightarrow x^{-1}\left(axy^{-1}\right)y = x^{-1}\left(xy^{-1}a\right)y$

$\Leftrightarrow x^{-1}ax(y^{-1}y) = (x^{-1}x)y^{-1}ay$

$\Leftrightarrow x^{-1}axe = ey^{-1}ay$

$\Leftrightarrow x^{-1}ax = y^{-1}ay$

$\Leftrightarrow x, y$ give rise to same conjugate of a.

Theorem 4: If G is a finite group then the number of distinct element in $C(a)$ are $\frac{O(G)}{O(N(a))}$.

Then further prove that $O(G) = \sum \frac{O(G)}{O(N(a))}$, where summation runs over one element of each conjugate class.

Proof: By the previous theorem 6, we know that two elements of a group give rise to same conjugate to $a \in G$ if they belong to the same right coset of normalizer of a in G. In the other sense it means, different conjugate to $a \in G$ belongs to different right coset of $N(a)$ in G. Thus we get a "*one-to-one correspondence between the conjugates of* $a \in G$ *and right cosets of* $N(a)$ *in* G".

Thus, c_a = Number of distnict element in $C(a)$

= Number of distinct right coset of $N(a)$ in G.

= The index of $N(a)$ in $G = \frac{O(G)}{O(N(a))}$

Further, If $C(a_1), C(a_2), ..., C(a_k)$ are k distinct conjugate class in G, Then

$G = C(a_1) \cup C(a_2) \cup ... \cup C(a_k)$

$\Rightarrow$Number of element in G = Number of element in $C(a_1)$+ Number of element in $C(a_2)$+ …+ Number of element in $C(a_k)$

$\Rightarrow O(G) = \sum c_a$, where summation runs over one element of each conjugate class

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

Hence proof the result.

2.4.1 *SELF CONJUGATE ELEMENT*

Definition: An element $a \in G$ is said to be self conjugate if $a = x^{-1}ax \forall\, x \in G$ *i.e*, $C(a)$ contains only singleton element $\{a\}$. In other manner, we can say those self conjugate elements are those elements of G which commutes with every element of G. Sometimes self conjugate element is also called invariant element of G.

2.5 *CENTRE OF A GROUP*

Definition: Collection of all self conjugate element of a group is called centre of group G. It is denoted by $Z(G)$ and defined as,

$Z(G) = \{x \in G | xa = ax \forall a \in G\}$

e.g.: The centre of the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is $Z(Q_8) = \{1, -1,\}$.

Theorem 5: The centre of a group G, $Z(G)$ is the normal subgroup of group.

Proof: First we will prove that $Z(G)$ is subgroup of G. For it, let $x_1, x_2 \in Z(G)$ then be definition $x_1 a = ax_1 \forall a \in G$ and $x_2 a = ax_2 \forall a \in G$

Since we have, $x_2 a = ax_2 \forall a \in G \Rightarrow x_2^{-1}(x_2 a)x_2^{-1} = x_2^{-1}(ax_2)x_2^{-1} \forall a \in G$

$\Rightarrow (x_2^{-1}x_2)ax_2^{-1} = x_2^{-1}a(x_2x_2^{-1}) \forall a \in G$

$\Rightarrow eax_2^{-1} = x_2^{-1}ae \forall a \in G$

$\Rightarrow ax_2^{-1} = x_2^{-1}a \forall a \in G$

$\Rightarrow x_2^{-1} \in Z(G)$

Now consider, $(x_1 x_2^{-1})a = x_1(x_2^{-1}a)$

$= x_1(ax_2^{-1})$ $[\, x_2^{-1} \in Z(G) \Rightarrow x_2^{-1}a = ax_2^{-1}]$

$= (x_1 a)x_2^{-1}$ [By associativity]

$= (ax_1)x_2^{-1}$ $[\, x_1 \in Z(G) \Rightarrow x_1 a = ax_1]$

$= a(x_1 x_2^{-1})$ [By associativity]

$\Rightarrow x_1 x_2^{-1} \in Z(G)$

Hence $Z(G)$ is subgroup of G.

Now we have only to prove that $Z(G)$ is always normal in G. For it let $x \in Z(G), a \in G$ then,

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

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

$= x(aa^{-1})$

$= x(e) = x \in Z(G)$

Thus, $x \in Z(G), a \in G \Rightarrow axa^{-1} \in Z(G)$

Hence, $Z(G)$ is the normal subgroup of group of G.

Theorem 6: Any element, $a \in Z(G)$ *iff* $N(a) = G$.

Proof: Let $a \in Z(G)$ then $xa = ax \forall x \in G$

Also, $N(a) = \{x \in G \mid xa = ax \forall x \in G\}$

So, $a \in Z(G) \Leftrightarrow xa = ax \forall x \in G$

$\Leftrightarrow x \in N(a) \forall x \in G$ [By definition of $N(a)$]

$\Leftrightarrow N(a) = G$

Corollary: If G is finite $a \in Z(G)$ *iff* $O(N(a)) = O(G)$.

Theorem 7: If G be the finite group and $Z(G)$ be the centre of the group G. Then class equation of G can be written as,

$$O(G) = O[Z(G)] + \sum_{a \notin Z(G)} \frac{O(G)}{O[N(a)]}$$

Where, summation runs over one element a in each conjugate class containing more than one element.

Proof: As we know by the previous theorem that class equation of G is

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

By corollary, we know that if G is finite $a \in Z(G)$ *iff* $O(N(a)) = O(G)$.

$\Leftrightarrow a \in Z(G)\, iff\, \frac{O(G)}{O(N(a))} = 1$

$\Leftrightarrow$ Number of elements in conjugate class of a is one whenever $a \in Z(G)$.

Thus, order of $Z(G)$ will be equal to the number of conjugate classes each having single element which is itself. If we take a such element which belongs any of these conjugate classes, we have $\frac{O(G)}{O(N(a))} = 1$. Hence the class equation can be rewrite as,

$$O(G) = \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$

Since, $O(Z(G)) = \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))}$

Hence, $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ …(1)

Note: This equation (1) is called the **class equation** of any finite group G.

Example 1: Find the class equation for the group S_3.

Answer: We know the symmetric group (S_3) on three symbols 1, 2, 3 is

$S_3 = \{I, (12), (13), (23), (123), (132)\}$.

Then we have,

Z(S_3) = $\{e\}$ and $C(12)$ = {(12),(23),(13)} because $(12)(13)(12)^{-1} = (23)$ shows that (2 3) is a conjugate of (1 3).

Similarly we can find, $C(123)$ = {(123),(132)}. Hence the class equation of S_3 is,

$|S_3|$ = |Z(S_3)| + |$C(12)$| + |$C(123)$| *i.e.*, 3! = 1 + 3 + 2.

Theorem 8: If $O(G) = P^n$, where P is a prime number, then $Z(G) \neq \{e\}$.

Proof: As we know for a finite group G the class equation of G is

$O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ where, summation runs over those conjugate class which containing more than one element. We have given $O(G) = P^n$ so, the divisor of $O(G)$ are $1, p, p^2, ..., P^k, ...P^n$ i.e., of the form P^k $where 1 \leq k \leq n$.

Since $\forall\, a \in G$ we have $N(a)$ is subgroup of G. By Lagrange's theorem we know that $O(N(a)) \mid O(G)$.

Also we know that if $a \notin Z(G) \Leftrightarrow N(a) \neq G \Rightarrow O[N(a)] < O(G)$.

Thus if $a \notin Z(G)$ then $O[N(a)]$ will be of the form P^k $where 1 \le k < n$.

Let us consider, $O(Z(G)) = m$, where *m* is a positive integer $m < n$. Now by class equation

$$P^n = m + \sum_{a \notin Z(G)} \frac{P^n}{P^k} \Rightarrow m = P^n - \sum_{a \notin Z(G)} \frac{P^n}{P^k} \quad where 1 \le k < n \qquad \ldots (1)$$

Since $P \mid P^n$ so, *P* will divide each term of the right hand side of the equation (1)

$\Rightarrow P \mid m$

Therefore centre of *G* must contain element other then identity. Therefore $Z(G) \neq \{e\}$.

Theorem 9: Every group of order P^2 is *Abelian.*

Proof: We have given order of the group is P^2 *i.e.,* $O(G) = P^2$. So, the positive divisors of P^2 are $1, P, P^2$. By the previous theorem 11 we know that if $O(G) = P^n$, where *P* is a prime number, then $Z(G) \neq \{e\}$. It means, $O(Z(G)) > 1$. As we know that centre of the group is subgroup of *G* and by Lagrange's theorem "Order of every subgroup of a finite group is divisor of the order of the group". So either $O(Z(G)) = P$ or $O(Z(G)) = P^2$.

If $O(Z(G)) = P^2$ then we have nothing to prove.

Otherwise, if $O(Z(G)) = P \Rightarrow$ there exist an element $x \in G$ which is not in *Z*(*G*) *i.e.,* $x \notin Z(G)$.

Since *N*(*x*) is subgroup of *G* and $x \in N(x)$. Also $a \in Z(G) \Rightarrow ax = xa \forall x \in G$.

$\Rightarrow a \in N(x)$

$\Rightarrow Z(G) \subseteq N(x)$

Since $x \notin Z(G) \Rightarrow O((N(x)) > P$ but $O(N(x))$ must be divisor of P^2

$\Rightarrow O((N(x))$ must be equal to P^2

$\Rightarrow N(x) = G$

$\Rightarrow x \in Z(G)$, thus we get a contradiction.

Hence, $O(Z(G)) = P^2 \Rightarrow G$ is *Abelian* group because $Z(G)$ is always *Abelian* group.

Example 2: Is a group of order 121 is *Abelian*?

Answer: Since, $O(G) = 121 = 11^2$, where 11 is a prime number. Hence *G* will be Abelian group.

Example 3: Prove that corresponding to every cyclic group its quotient group is cyclic but their converses need not to be true.

Solution: Let *G* be a cyclic group such that $G = < a > i.e.,$ *a* is the generator of *G* and *H* is its subgroup. Then according to theorem every subgroup of *G* will be normal subgroup of *G*. If elements $a^n \in G$ then $Ha^n = (Ha)^n$ will be element of quotient group G/H.

Therefore G/H is a cyclic group and Ha will be generator of it.

But converse is need not be true. Since $S_3/A_3 = \{A_3, (23)A_3\}$ is Abelian group because order of $O[S_3/A_3] = 6/3 = 2$ which is prime and we know that every group of prime order is cyclic while S_3 is not a Abelian group.

Theorem 10: If $G/Z(G)$ is cyclic if and only if *G* is Abelian.

Proof: Let us consider $G/Z(G)$ is cyclic. It means, if the element *a* is the generator of *G* then $Z(G)a$ will be generator of $G/Z(G)$.

Let $x, y \in G$ then $Z(G)x, Z(G)y \in G/Z(G) \Rightarrow \exists$ positive integers m, n such that

$Z(G)x = (Z(G)a)^m = Z(G)a^m$ & $Z(G)y = (Z(G)a)^n = Z(G)a^n$

$\Rightarrow$ we have $x = x_1 a^m$ where $x_1 \in Z(G)$ and $y = y_1 a^n$ where $y_1 \in Z(G)$

Now, $xy = (x_1 a^m)(y_1 a^n) = x_1(a^m y_1)a^n) = x_1(y_1 a^m)a^n = (x_1 y_1)a^m a^n = (y_1 x_1)a^m a^n$

$= y_1 x_1 (a^m a^n) = y_1 x_1 a^n a^m = y_1 a^n x_1 a^m = xy$

$\Rightarrow G$ is abelian.

Conversely, assume that *G* is Abelian. If *G* is Abelian then $Z(G) = G$.

$\Rightarrow G/Z(G) = \{e\}$ *i.e.* trivial subgroup which is always cyclic.

Hence the theorem.

Example 4: If *G* be a non-Abelian group of order P^3 where *P* is prime then *Z*(*G*) has exactly *P* element.

Proof: We have given be a non-Abelian group of order P^3 where *P* is prime. Then According to Lagrange's theorem possibilities of order of *Z*(*G*) is $1, P, P^2, P^3$.

Case Ist: We know by previous theorem if $O(G) = P^n$, where *P* is a prime number, then $Z(G) \neq \{e\} \Rightarrow O[Z(G)] > 1$.

Case IInd: Let $O[Z(G)] = P^2 \Rightarrow O(G/Z(G)) = P^3/P^2 = P$

$\Rightarrow G/Z(G)$ is cyclic and by theorem we can say that *G* is Abelian which is a contradiction. So our assumption is wrong.

Case IIIrd: Let $O[Z(G)] = P^3 \Rightarrow O(G/Z(G)) = P^3/P^3 = 1$

$\Rightarrow G/Z(G) = \{e\}$ is cyclic and by theorem we can say that *G* is Abelian which is again a contradiction. So again our one of the assumption is wrong.

So, the only possibilities is left that $O[Z(G)] = P$ *i.e.*, *Z*(*G*) has exactly *P* element.

Check your progress

Problem 1: Find the finite number of distinct classes in $Q_4 = \{1,-1,i,-i\}$?

Problem 2: Find the number of element in the centre of $Q_4 = \{1,-1,i,-i\}$?

Problem 3: Find the class equation of $Q_4 = \{1,-1,i,-i\}$?

2.6 *SUMMARY*

In this unit, we have studied the definition and theorems related to conjugate of an element, normalizer of an element and centre of the group and also learn their implementation on various examples. We have also learn in this unit how these subgroup are essentials in the formation of class equation which will further discussed briefly in the upcoming units. The overall summarization of this units are as follows:

- Conjugacy relation is an equivalence relation on *G*.
- $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ is known as class equation of any group.
- Every group of order p^2 is abelian group.

2.7 *GLOSSARY*

- $b \sim a$ denotes two elements a, b of a group *G* are conjugate to each other.
- $C(a)$ denotes collection of elements of group which are conjugate to *a*.
- c_a denotes number of elements in group which are conjugate to *a*.
- $Z(G)$ denotes centre of the group.
- $N(a)$ denotes the normalizer of *a*.

2.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna

Prakashan Media.

- https://en.wikipedia.org/wiki/Center_(group_theory)#:~:text=By%20definition%2C%20the%20center%20is,of%20each%20element%20of%20G.

2.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

2.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that any two conjugate classes of a group are either disjoint or identical.

2. If the order of a group G is prime (p), then prove of G has exactly p elements.

3. If H is normal subgroup of G, having prime index p then prove that G/N is cyclic.

4. If G be a non-Abelian group of order $O(G)=1331$ then prove that number of elements in centre of group $Z(G)$ are 11.

5. If G be a group of order $O(G)=121$ then find the number of elements in its centre.

6. State and prove the class equation.

7. Prove that cojugacy is an equivalence relation.

Short Answer Type Question:

8. Find the number of elements of the in the centre of the group having order $O(G)=5,7,25,31,49$.

9. Prove that centre of the group is an abelian group

10. If G is a non-abelian of order 8 then prove that $Z(G)$ has exactly 2 element.

11. Find number of element which are conjugate to $(12)\in S_3$.

12. Prove that if G is finite, $a\in Z(G)$ *iff* $O(N(a))=O(G)$.

Fill in the blanks:

13. Two elements a and b in a group G are such that $b=x^{-1}ax$ then b will called …… to a.

14. Every group of order p^2 ($p = prime$) is …….

15. Centre of the group G is the …… subgroup of G.

16. If G is non-abelian group of order 125 then $Z(G)$ has …….. elements.

2.11 *ANSWERS*

Answer of self cheque question:

1. 4 **2.** 4 **3.** $Q_4 = 1+1+1+1$

Answer of terminal question:

5. 121 **8.** $5, 7, 25, 31, 49$ **11.** 3 **13.** Conjugate

14. Abelian **15.** Normal **16.** **5**

Unit-3: HOMOMORPHISM AND ISOMORPHISM

CONTENT:

3.1 *INTRODUCTION*

The term "homomorphism" appeared as early as 1892, when it was attributed to the mathematician Felix Klein (1849–1925).

Christian Felix Klein was a German mathematician and mathematics educator, known for his work with group theory, complex analysis, non-Euclidean geometry, and on the associations between geometry and group theory. His 1872 Erlangen program, classifying geometries by their basic symmetry groups, was an influential synthesis of much of the mathematics of the time.

Christian Felix Klein

25 April 1849 – 22 June 1925

In this section we introduce the reader to the idea of an isomorphism which could also be termed as an 'indirect' equality in algebraic systems. Indeed, if two systems have the same number of elements and *behave* exactly in the same manner, nothing much is lost in calling them equal, although at times the idea of equality may look little uncomfortable, especially in case of infinite sets.

3.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the concept of special types of mapping between two groups named as homomorphism and isomorphism. It may be possible these groups are under the different binary operations.
- Know that under the isomorphism mapping how the properties of two groups are same.
- Understand about the other type of mapping like endomorphism, automorphism.
- Understand the basic properties of homomorphism and isomorphism and their related other theorems and definitions.

3.3 *HOMOMORPHISM*

Definition: A mapping f from a group $(G,*)$ into the group $(G',.)$ is said to be a homomorphism if it preserve the composition under f *i.e.*,

$$f(a*b) = f(a).f(b) \ \forall a,b \in G$$

Or

A mapping $f : G \to G'$ is said to be homomorphism if,

$$f(a*b) = f(a).f(b) \ \forall a,b \in G$$

where, G and G' are the groups under the operation $'*'$ and $'.'$ respectively.

Note 1: The range of f in G is called the homomorphic image of G'.

2: In general, we take both the groups G and G' under the same operation multiplication and write f is a homomorphism between G to G' if, $f(ab) = f(a)f(b) \ \forall a,b \in G$**,** without the loose of generality.

Example 1: A mapping $f : Z \to E$, from set of integer to the set of even integer such that $f(x) = 2x \forall x \in Z$ is a homomorphism.

Answer: We have given the mapping $f : Z \to E$ such that

$f(x) = 2x \forall x \in Z$

at first, we will check mapping is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

Now, we will check mapping also preserve the composition for it for any $x, y \in Z$

$f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$

$\Rightarrow f$ preserve the composition.

Hence given mapping f is an homomorphism.

Example 2: Show that the Mapping $f : Z \to G$, from set of integer under the operation addition to the group $G = \{1, -1\}$ under the operation multiplication defined as

$$f(x) = \begin{cases} 1, & if\ x\ is\ even \\ -1, & if\ x\ is\ odd \end{cases}$$

is a homomorphism.

Answer: Case I: If $x, y \in Z$ both are even integers. It means $f(x) = 1, f(y) = 1$ then their sum will also an even integer *i.e.*,

$f(x+y) = 1 = 1.1 = f(x) f(y)\ \forall x, y \in Z$

Case II: If $x, y \in Z$ both are odd integers i.e., $f(x) = -1, f(y) = -1$ then their sum will be even integer *i.e.*,

$f(x+y) = 1 = (-1).(-1) = f(x) f(y)\ \forall x, y \in Z$

Case III: If $x, y \in Z$ are such that *x* is even integer and *y* is odd integer *i.e.*, $f(x) = 1, f(y) = -1$ then their sum will be odd integer then,

$f(x+y) = -1 = 1.(-1) = f(x) f(y)\ \forall x, y \in Z$

Case IV: If $x, y \in Z$ are such that *x* is odd integer and *y* is even integer *i.e.*, $f(x) = -1, f(y) = 1$ then their sum will be odd integer then,

$f(x+y) = -1 = (-1).(1) = f(x) f(y)\ \forall x, y \in Z$

Hence the given mapping f is an homomorphism.

Example 3: Show that the Mapping $f : R^+ \to R$, from set of positive real numbers to the set of real number defined as $f(x) = \log x \forall x \in R^+$ is an homomorphism.

Answer: As we know that set of positive real numbers (R^+) is form group under the operation multiplication and the group *R* is form group under the operation addition.

Here, clearly the mapping is well-defined since, for

$x = y$

$\Rightarrow \log x = \log y$ [Taking logarithm both side]

$\Rightarrow f(x) = f(y) \; \forall \, x, y \in R^+$

Now, $f(xy) = \log(xy) = \log x + \log y = f(x) + f(y) \; \forall \, x, y \in R^+$

Hence *f* is a homomorphism.

Homomorphism onto: A **onto** mapping from a group $(G,*)$ into the group $(G',.)$ is said to be a homomorphism onto if it preserve the composition under f *i.e.*,

$f(a*b) = f(a).f(b) \; \forall \, a, b \in G$**.**

Endomorphism: A homomorphism from a group G to itself is called an endomorphism.

Example 4: If *G* be a group and a mapping such that, $f : G \to G$ such that $f(x) = x^{-1}$ be a homomorphism then show that *G* is a *A*belian group.

Proof: Since *G* be a group then for any elements $x, y \in G$, *G* will satisfies the closure property *i.e.*, $xy \in G$ and for every element belongs to *G* there exist its inverse in *G*.

Now, $xy = \left(y^{-1}x^{-1}\right)^{-1} = f\left(y^{-1}x^{-1}\right) = f\left(y^{-1}\right)f\left(x^{-1}\right) = yx$

$\Rightarrow G$ is *A*belian group.

Theorem 1: If $f : G \to G'$ be a homomorphism then,

- ***(i)*** If *e* is the identity of *G*, then $f(e)$ is the identity of G'
- ***(ii)*** For any element $a \in G$, $f(a^{-1}) = \left[f(a)\right]^{-1}$
- ***(iii)*** If *H* is subgroup of G then $f(H)$ is subgroup of G'
- ***(iv)*** If *K* is subgroup of G', then $f^{-1}(K) = \left\{k \in G \middle| f(k) \in G'\right\}$ is a subgroup of *G*. Furthermore, if *K* is normal in G' then $f^{-1}(K)$ is normal in *G*.
- ***(v)*** If order of any element $a \in G$ is finite then the order of $f(a)$ is divisor of the order of $a \in G$.

Proof (*i*): Let e and e' are the identity elements of the group *G* and G'. Since f is the mapping from *G* to G' then $f(e)$ will be the elements of G'.

Now, $e' f(e) = f(e) = f(ee) = f(e) f(e)$, then by the right cancellation law

$e' = f(e)$

i.e., $f(e)$ is the identity of G'.

(*ii*): Let *a* be any element of *G* then a^{-1} will be also in *G* because *G* itself a group. Since we have,

$e' = f(e) = f(aa^{-1}) = f(a) f(a^{-1})$ … (1)

As we know that if $a \in G \Rightarrow f(a) \in G'$ and G' is also a group then $[f(a)]^{-1} \in G'$

Now multiplying by $[f(a)]^{-1}$ both side in equation (1)

Then, $[f(a)]^{-1}e' = [f(a)]^{-1}[f(a)f(a^{-1})] = ([f(a)]^{-1}f(a))f(a^{-1}) = f(a)$

So, $[f(a)]^{-1} = f(a)$

(*iii*): We have given H is subgroup of G then to prove that $f(H)$ is subgroup of G'. If $x, y \in H \Rightarrow xy^{-1} \in H$ [By the subgroup test of any nonempty subset of G]

Since f is the homomorphism then there exist $a, b \in f(H)$ *s.t.* $a = f(x), b = f(y)$

Now consider, $ab^{-1} = f(x)[f(y)]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$

Hence we have prove that if $a, b \in f(H)$ then $ab^{-1} \in f(H)$

$\Rightarrow f(H)$ is subgroup of G'.

(*iv*): Let K is subgroup of G' and define H to be $f^{-1}(K)$; that is H is the set of all $g \in G$ such that $f(g) \in K \subseteq G'$. If $a, b \in H$, then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} \in K$. Since K is subgroup of G'. Therefore, $ab^{-1} \in H$ and H is the subgroup of G.

If K is normal in G' then we have to show $g^{-1}hg \in H$ for $h \in H, g \in G$

But, $f(g^{-1}hg) = f(g^{-1})f(h)[f(g)]^{-1} = [f(g)]^{-1}(f(h)[f(g)]) = ([f(g)]^{-1}f(g))f(h) = f(h) \in K$

Since K is normal in G therefore $g^{-1}hg \in H$

$\Rightarrow H$ is normal subgroup of G.

(*v*): Let $a \in G$ and $O(a) = m$ *i.e.*, $a^m = e$

Taking *f*-image both side we get, $f(a^m) = f(e)$

$\Rightarrow f(a)f(a)f(a)....f(a)$ (m times) $= f(e)$

$\Rightarrow [f(a)]^m = e'$

If order of $f(a)$ in G' is n then $o(f(a)) \mid O(a)$

3.3.1 *KERNEL OF A HOMOMORPHISM*

Definition: If $f : G \to G'$ is a homomorphism then kernel of homomorphism is the collection of all elements of domain set which are mapped into the identity elements of range set.

OR

If $f : G \to G'$ is a homomorphism then,

$\ker f = \{x \in G \mid f(x) = e'\}$

Where e' is the identity element of G'

Theorem 2: If $f : G \to G'$ is a homomorphism then $\ker f$ is the normal subgroup of G.

Proof: Since we have given $f : G \to G'$ is an homomorphism and we know that

$\ker f = \{x \in G \mid f(x) = e'\}$ then first we will prove that $\ker f$ is a subgroup of G. for it let

$x, y \in \ker f \Rightarrow f(x) = e', f(y) = e'$

Now, $f(xy^{-1}) = f(x) f(y^{-1}) = f(x)[f(y)]^{-1} = e'[e']^{-1} = e'$

$\Rightarrow xy^{-1} \in \ker f$

Hence $\forall x, y \in \ker f$ we have $xy^{-1} \in \ker f$ it means $\ker f$ is the subgroup of G.

Now we have to prove that $\ker f$ is the normal subgroup of G. For it let g be any element of G and k be any element of $\ker f$. Then $f(k) = e'$, we have

$f(gkg^{-1}) = f(g) f(k) f(g^{-1}) = f(g)e' f(g^{-1}) = f(g)[f(g)]^{-1} = e'$

$\Rightarrow xgkg^{-1} \in \ker f$

Hence, $\ker f$ is normal subgroup of G.

Theorem 3: A homomorphism $f : G \to G'$ is one-one if and only if $\ker f = \{e\}$.

Proof: We have given $f : G \to G'$ is an homomorphism and let mapping is ono-one. If $x \in \ker f$ be any element

Then $f(x) = e'$ and also $f(e) = e'$

Since f is one-one so, $f(x) = f(e) \Rightarrow x = e \forall x \in \ker f$

Hence, $\ker f = \{e\}$.

Conversely, let $\ker f$ contains only the identity element.

For it let, $f(x) = f(y)$

then $f(x)[f(y)]^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \ker f = \{e\}$

$\Rightarrow xy^{-1} = \{e\}$

$\Rightarrow x = y$

$\Rightarrow f$ is one-one.

3.4 *ISOMORPHISM*

Definition: A mapping f from a group $(G,*)$ into the group $(G',.)$ is said to be isomorphism if it satisfies the following condition,

(i) f is ono-one *i.e*, f is injective

(ii) f is on-to *i.e*, f is surjective

(iii) $f(a*b) = f(a).f(b)\ \forall a,b \in G$ *i.e*., f preserve the composition

Example 5: Show that the Mapping $f : R^+ \to R$, from set of positive real numbers to the set of real number defined as $f(x) = \log x \forall x \in R^+$ is an isomorphism.

Answer: In the previous example we have already proved that given mapping is a homomorphism. Now, we are going only to show that mapping (*f*) is a bijective mapping (*i.e*., *f* is one-one and on-to)

One-One: Let $x, y \in R^+$ *s.t*., $f(x) = f(y)$

$\Rightarrow \log x = \log y$

$\Rightarrow e^{\log x} = e^{\log y}$

$\Rightarrow x = y$

$\Rightarrow f$ is one-one mapping.

On-to: If $y \in R$ be any real number then clearly $e^y \in R^+$. It means for each $y \in R$ we have $e^y \in R^+$ such that $f(e^y) = \log(e^y) = y \in R$

$\Rightarrow f$ is on-to mapping.

Hence, f is an isomorphism.

Example 6: Show that there is no isomorphism from $f : Q \to Q - \{0\}$ where, Q is set of rational number.

Answer: To prove this example let we assume that $f : Q \to Q - \{0\}$ is an isomorphism. Since f is an isomorphism so f will also a on-to function i.e., for $2 \in Q - \{0\}\ \exists\, x \in Q$ s.t.,

$f(x) = 2$

$\Rightarrow f\left[\frac{x}{2} + \frac{x}{2}\right] = 2$

$\Rightarrow f\left(\frac{x}{2}\right) f\left(\frac{x}{2}\right) = 2$ [Since, *f* preserve the compostion]

$\Rightarrow f\left(\frac{x}{2}\right) f\left(\frac{x}{2}\right) = 2$

$\Rightarrow y^2 = 2$ where, $y = f\left(\frac{x}{2}\right)$, which is a contradiction because there is no rational number which is the solution of quadratic equation $x^2 - 2 = 0$. Hence our assumption is wrong. So, there is no map $f : Q \to Q - \{0\}$ which is an isomorphism.

Theorem 4: Let N be a normal subgroup of a group G. A mapping f, $f : G \to G/N$ defined as $f(x) = Nx \forall\, x \in G$ then f is a homomorphism of G onto G/N and $\ker f = N$.

Proof: We have given the mapping $f : G \to G/N$ such that $f(x) = Nx \forall\, x \in G$. As we know if $x \in G$ then $Nx \in G/N$.

First we will check that f is a onto homomorphism from G to G/N. For it, let $a, b \in G/N$ then,

$f(ab) = Nab = (Na)(Nb) = f(a) f(b)$ [$\because N$ is normal subgroup of G]

$\Rightarrow f$ is a homomorphism from G to G/N.

Since for each element $Nx \in G/N$ there exist an element $x \in G$ such that $f(x) = Nx \forall\, x \in G$.

Hence, f is on-to mapping.

Let $\ker f$ is the kernel of this homomorphism then, $\ker f = \{x \in G \mid f(x) = N\}$

Now, we have only to prove that $\ker f = N$. Let x be any element of $\ker f$. Then $f(x) = N$, where N is the identity of G/N. But according to mapping $f(x) = Nx = N$ *i.e.*, $Nx = N \Rightarrow x \in N$

[Because if H is normal subgroup of G and $Hx = H$ then $x \in H$]

So, $x \in \ker f \Rightarrow x \in N$. Therefore $\ker f \subseteq N$

Conversely, let y be any element of N. Then $Ny = N$

We have $f(n) = Nn = N$. Therefore $n \in \ker f$

Thus, $n \in N \Rightarrow n \in \ker f$. Therefore $N \subseteq \ker f$

Hence, $\ker f = N$.

3.5 *FUNDAMENTAL THEOREMS*

Theorem 5: Fundamental theorem on group homomorphism: If $f : G \to G'$ is onto homomorphism then $\frac{G}{K} \cong G'$ where $K = \ker f$

OR

In other word, "Every homomorphic image of a group G is isomorphic to some quotient group of G".

Proof: We have given a on-to homomorphism f from $G\,to\,G'$. Let we define a map $\phi : \frac{G}{K} \to G'$ s.t.

$\phi(Ka) = f(a), a \in G$

First, we have to show that ϕ is an isomorphism. For it initially we shall show the mapping ϕ is well-defined by, $Ka = kb$

$\Rightarrow ab^{-1} \in K = \ker f$

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

$\Rightarrow f(a) f(b^{-1}) = e'$

$\Rightarrow f(a)\left[f(b)\right]^{-1} = e'$

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

$\Rightarrow \phi(Ka) = \phi(Kb)$

On retracing theses steps backwards, we will get that ϕ is one-one.

Again as $\phi(KaKb) = \phi(Kab) = f(ab) = f(a) f(b) = \phi(Ka)\phi(Kb)$

$\Rightarrow \phi$ is an homomorpshism.

Now we will check ϕ is onto, let $g' \in G'$ be any element. Since $f : G \to G'$ is onto then there exist $g \in G$ such that,

$f(g) = g'$

Now, $\phi\left[Kg\right] = f(g) = g'$.

$\Rightarrow \phi$ is on-to

$\therefore \phi$ is an isomorphism.

Hence, $\frac{G}{K} \cong G'$.

Theorem 6: (Second fundamental theorem of Isomorphism). If H and K are two subgroups of the group G where H is normal subgroup of G then,

$\frac{HK}{H} \cong \frac{K}{H \cap K}$.

Proof: By the previous theorems in normal subgroups we can easily seen that $H \cap K$ will be normal subgroup of K because $H \cap K \subseteq H \; and \; H \cap K \subseteq K$. Similarly, as $H \subseteq HK \subseteq G, H$ will be normal in HK.

Now, we define a map $f : K \to \frac{HK}{H}$ s.t.,

$f(k) = Hk$

Then as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

Which shows the mapping is well-defined.

Again, $f(k_1k_2) = Hk_1k_2 \Rightarrow Hk_1Hk_2 = f(k_1)f(k_2)$

$\Rightarrow f$ is an homomorphism.

Obviously, the mapping is on-to also then by using the first fundamental theorem we find that

$$\frac{HK}{H} \cong \frac{K}{\ker f}$$

Since, $k \in \ker f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow k \in H$ [As H is normal subgroup of G]

$\Leftrightarrow k \in H \cap K$ [$k \in K$ *as* $\ker f \subseteq K$]

So, $\ker f = H \cap K$

Hence the theorem is proved.

Lemma: Let in a group G, if H, K are normal in G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and converse of the theorem is also true.

Proof: $\frac{K}{H}$ is a non empty subset of $\frac{G}{H}$, by definition.

Now, for any $Hk_1, Hk_2 \in \frac{K}{H}$

$$(Hk_1)(Hk_2)^{-1} = (Hk_1)(Hk_2^{-1}) = Hk_1k_2^{-1} \in \frac{K}{H}$$

$\Rightarrow \frac{K}{H}$ is a subgroup.

Again for any $Hk \in \frac{K}{H}$ and $Hg \in \frac{G}{H}$, we notice that

$$(Hg)^{-1}(Hk)(Hg) = Hg^{-1}HkHg = Hg^{-1}kg \in \frac{K}{H}$$

as $g \in G, k \in K, K$ is normal in G gives $g^{-1}kg \in K$.

Conversely, let any element $x \in G$ and $k \in K$. In order to prove that K is normal in G we must show that $xkx^{-1} \in K$.

We know that $Hx \in \frac{G}{H} where\, x \in G$ and $Hk \in \frac{K}{H} where\, k \in K$. Since we have given $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$, therefore

$(Hx)(Hk)(Hx)^{-1} \in \frac{K}{H}$

$\Rightarrow Hxkx^{-1} \in \frac{K}{H}$ [As H is normal in G]

$\Rightarrow xkx^{-1} \in K$

$\therefore K$ is normal subgroup of G. Also the quotient group $\frac{K}{H}$ implies that H is normal in G. Therefore, K is normal subgroup of G and $H \subseteq K$.

Theorem 7: (Third isomorphism theorem). If two subgroups H, K are normal in G such that $H \subseteq K$, then

$\frac{G}{K} \cong \frac{G \setminus H}{K \setminus H}$

Proof: By the above lemma we know that if H, K are normal in G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk about $\frac{G \setminus H}{K \setminus H}$.

First, we will define a map $f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$f(Ha) = Ka, a \in G$

Since, H is well defined as

$Ha = Hb$

$\Rightarrow ab^{-1} \in H \subseteq K$

$\Rightarrow Ka = Kb$

$\Rightarrow f(Ha) = f(Hb)$

Now, we will check f is a homomorphism as

$f(HaHb) = f(Hab) = Kab = (Ka)(Kb) = f(Ha) f(Hb)$.

Here, ontoness of f is obvious.

Using first fundamental theorem of group homomorphism we can write that,

$\frac{G}{K} \cong \frac{G/H}{\ker f}$, so, we will claim that $\ker f = \frac{K}{H}$.

A member of $\ker f$ will be some member of $\frac{G}{H}$.

Now, $Ha \in \ker f \Leftrightarrow f(Ha) = K$

$\Leftrightarrow Ka = K$

$\Leftrightarrow a \in K$

$\Leftrightarrow Ha \in \frac{K}{H}$

Hence we find $\frac{G}{K} \cong \frac{G/H}{K/H}$

Hence our result is proved. This theorem is also named as "Freshman's Theorem".

Remarks: In the above theorem, since we have put $\frac{K}{H} = \ker f$ because we have notice that $\frac{K}{H}$ is normal in $\frac{G}{H}$ and hence we are talking about $\frac{G/H}{K/H}$. Thus we do not need to prove separately that $\frac{K}{H}$ is normal in $\frac{G}{H}$.

Theorem 8: Let the mapping $f: G \to G'$ be an onto homomorphism with $\ker f = K$. Let the subgroup H' of the group G', define

$H = \{x \in G \mid f(x) \in H'\}$

Then

(i) H is subgroup of G and $K \subseteq H$.

(ii) H' is normal in G' *iff* H is normal in G.

(iii) H' is normal in G' then $\frac{G'}{H'} \cong \frac{G}{H}$

(iv) There exist a one to one association from the from the family S' of all subgroup of G' onto the family S of all subgroup of G, that contain K.

Proof (i): Since, $f(e) = e' \in H' \Rightarrow e \in H$, it means $H \neq \phi$.

Let $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)[f(y)]^{-1} \in H'$

$\Rightarrow f(xy^{-1}) \in H'$

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

Thus H is subgroup of G.

Since $x \in \ker f = K \Rightarrow f(x) = e' \in H'$

Hence for each $x \in K$ we have $x \in H \Rightarrow K \subseteq H$.

(ii): Suppose H is normal subgroup of G. Let the elements $g' \in G', h' \in H'$. Since the given mapping is onto so $\exists g \in G, h \in H$ s.t. $f(g) = g'$, $f(h) = h'$. Since $h \in H, h' \in H'$

Now,

$g^{-1}h'g' = (f(g))^{-1} f(h) f(g)$

$= f(g^{-1}) f(h) f(g) = f(g^{-1}hg) \in H'$ [Because H is normal subgroup in G means $g^{-1}hg \in H$]

Thus H' is normal in G'.

Conversely, assume that H' is normal in G'.

For any elements $h \in H$, $g \in G$,

$f\left(g^{-1}hg\right) = (f(g))^{-1} f(h) f(g) \in H'$

as $f(h) \in H'$, $f(g) \in G'$

as $f(h) \in H'$, $f(g) \in G'$ [H' is normal in G']

$\Rightarrow g^{-1}hg \in H$

i.e., H is normal in G

(iii) Let us defining a mapping $\phi : G \to \frac{G'}{H'}$ s.t.,

$\phi(g) = H' f(g)$

Since ϕ is well define as $g_1 = g_2 \Rightarrow f(g_1) = f(g_2)$

$\Rightarrow H' f(g_1) = H' f(g_2)$

$\Rightarrow \phi(g_1) = \phi(g_2)$, which shows mapping is well defined.

Now, we will verify that the mapping ϕ preserve the composition as

$\phi(g_1 g_2) = H' f(g_1 g_2) = H' f(g_1) f(g_2) = H' f(g_1) H' f(g_2) = \phi(g_1)\phi(g_2)$

Again, for any $H'g' \in \frac{G'}{H'}$, since $g' \in G'$ and f is onto $\exists g \in G$ s.t., $f(g) = g'$

Or that $\phi(g) = H' f(g) = H'g'$ showing that ϕ is onto.

By using fundamental theorem then

$\frac{G'}{H'} \cong \frac{G}{\ker \phi}$

Now, $x \in \ker\phi \Leftrightarrow \phi(x) = H'$

$\Leftrightarrow H' f(x) = H'$

$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$

Hence $\ker\phi = H$

(iv) Define mapping $\psi : S' \to S$, s.t.,

$\psi(H') = H$

Where H is $\{x \in G \mid f(x) \in H'\}$ for any H' in S' by (i) we know that it is subgroup of G, containing K and thus a member of S. ψ is well defined mapping.

Let now $\psi(H') = \psi(T')$ where $H', T' \in S'$

Then $H = T$ where

$H = \{x \in G \mid f(x) \in H'\}$

$T = \{x \in G \mid f(x) \in T'\}$

Now for any $h' \in H' \subseteq G'$, since $f : G \to G'$ is onto, we can find $h \in G$, s.t.,

$f(h) = h' \in H'$

But this shows $h \in H = T$

$\Rightarrow f(h) \in T'$

$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$

Similarly $T' \subseteq H'$

i.e., $T' = H'$ or ψ is one-one.

We will show now that ψ is onto.

Let $H \in S$ be any member, H is a subgroup of G and $K \subseteq H$.

Consider $f(H) = \{f(h) \mid h \in H\}$

Then $f(H) \neq \phi$ as $e \in H \Rightarrow f(e) = e' \in f(H)$

Again, for any $f(h_1), f(h_2) \in f(H), h_1, h_2 \in H$

And $f(h_1)(f(h_2))^{-1} = f(h_1 h_2^{-1}) \in f(H)$

i.e., $f(H)$ is subgroup of G'.

We show $f(H) = H'$ is the required pre-image of H under ψ,

i.e., we show $\psi(H') = H$,

For it we have to show $H = \{x \in G \mid f(x) \in H'\}$

Let $x \in H$ then $f(x) \in f(H) = H'$

$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$

Or that $H \subseteq \{x \in G \mid f(x) \in H'\}$

Again, if $x \in \{x \in G \mid f(x) \in H'\}$

Then $f(x) \in H' = f(H)$

$\exists h \in H, s.t.\ f(x) = f(h)$

$\Rightarrow f(xh^{-1}) = e'$

$\Rightarrow xh^{-1} \in \ker f = K$

$\Rightarrow x \in Kh \subseteq H \quad [K \subseteq H]$

Thus $\{x \in G \mid f(x) \in H'\} \subseteq H$

Hence $H = \{x \in G \mid f(x) \in H'\}$

Or that $\psi(H') = H$ and so ψ is onto

Hence the theorem proved.

Example 7: Show that any infinite cyclic group is isomorphic to $G =< Z, + >$ the group of integers.

Solution: Let $G =< a >$ be any infinite cyclic group.

Define, $f : G \to Z$, *s.t.*,

$f(a^i) = i,\ i \in Z$

Since $G =< a >$ is of infinite order, $a^i \in G$ for all $i \in Z$ and $a^i = a^j$ for no $i \neq j$

Thus $a^i = a^j \Rightarrow i = j \Rightarrow f(a^i) = f(a^j)$ or that f is well defined.

Again $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j \Rightarrow f$ is 1-1.

$f(a^i.a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$

Shows that f is a homomorphism.

f is obviously onto and hence the isomorphism is established.

Corollary: Every subgroup of an infinite cyclic group is an infinite cyclic group which is isomorphic to the group itself.

Example 8: Any finite cyclic group of order *n* is isomorphic to Z_n the group of integers addition modulo *n*.

Solution: Let $G =< a >$ be a cyclic group s.t.,

$O(G) = O(a) = n$

then $G = \{e, a, a^2, ..., a^{n-1}\}, Z_n = \{0, 1, 2, ..., n-1\}$

Define $f : G \to Z_n$ s.t., $f(a^i) = i$

f is clearly well defined 1-1 onto mapping.

Again $f(a^i.a^j) = f(a^{i+_n j}) = i +_n j = f(a^i) +_n f(a^j)$

Thus f is a homomorphism and hence an isomorphism.

Remark: Any two cyclic groups of same order (finite or infinite) are isomorphic.

Check your progress

Problem 1: Since $Q_4 \cong Z_2 \times Z_2$, then find whether the identity element 1 of Q_4 map in $Z_2 \times Z_2$?

Problem 2: Is $Z_4 \cong Q_8$ and why?

3.6 *SUMMARY*

In this unit, we have studied about the mapping like homomorphism, isomorphism and also learn their implementation on various examples. After completions of this unit we have learned that two groups if isomorphic to each other than their all properties in terms of cardinality, order of elements, cyclic will be same. On the other manner we can say that if two groups are isomorphic in which one group is completely given then on the basis of given group we can unfold the unknown group completely even these groups are under the different binary operations. We have also learned about the fundamental theorems of isomorphism which are helpful to solve out various problems.

One of the important concept we have learned in this unit that every infinite cyclic group is isomorphic to the set of integers (*Z*).

3.7 *GLOSSARY*

- $G \cong G'$ represents two groups G, G' are isomorphic to each other.
- ker f represents the kernel of homomorphism mapping *f*.

3.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.

- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- https://en.wikipedia.org/wiki/Center_(group_theory)#:~:text=By%20definition%2C%20the%20center%20is,of%20each%20element%20of%20G.

3.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

3.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. If $f: G \to G'$ is an homomorphism then prove that the set $A = \{x \in G \mid f(x) = e'\}$ where e' is the identity element of G' is the normal subgroup of G.

2. Prove that every finite cyclic group of order n is isomorphic to the set of integer under the operation addition modulo *n*.

3. Prove that every infinite cyclic group is isomorphic to Z.

4. Prove that if H and K are two subgroups of the group G where H is normal subgroup of G then, $\frac{HK}{H} \cong \frac{K}{H \cap K}$.

5. Prove that every homomorphic image of a group *G* is isomorphic to some quotient group of *G*.

6. Prove that there is no isomorphism from Q to $Q^* = Q - \{0\}$.

7. If $f: G \to G'$ is an homomorphism then order of any element $f(a) \in G'$ is divisor of the order of $a \in G$.

8. If two subgroups H, K are normal in G such that $H \subseteq K$, then

$$\frac{G}{K} \cong \frac{G \setminus H}{K \setminus H}$$

9. Prove that relation of isomorphism is an equivalence relation.

Short Answer Type Question:

10. If $f : G \to G'$ is an homomorphism and H is subgroup of G then $f(H)$ is subgroup of G'.

11. If f is a homomorphism from $f : G \to G'$ then prove that f is one-one if and only if $\ker f = \{e\}$.

12. Prove that any finite cyclic group of order n is isomorphic to the quotient group Z / N, where $N = < n >$

13. An endomorphism f in a group G such that $f(x) = x^{-1}$ then G is abelian.

Fill in the blanks:

14. If $f : G \to G'$ be a homomorphism then for any element $a \in G$, $f(a^{-1}) = ...$

15. If two groups G, G' are isomorphic then $O(G) = ...$

16. If two groups G, G' of finite order are isomorphic then number of elements of order n in G are = …….

17. If $f : G \to G'$ be a homomorphism and e is the identity element of G then identity element of G' will be ……

18. …… is the infinite cyclic group

19. A cyclic group of order 123456789 is isomorphic to …….

3.11 *ANSWERS*

Answer of self cheque question:

1. (0, 0) **2.** No, because $z_2 \times z_2$ is abelian group while Q_8 is not

Answer of terminal question:

14. $[f(a)]^{-1}$ **15.** $O(G')$ **16.** Number of elements of order n in G'

17. $f(e)$ **18.** Z **19.** $Z_{123456789}$

BLOCK II

CLASS EQUATION AND SYLOW'S THEOREM

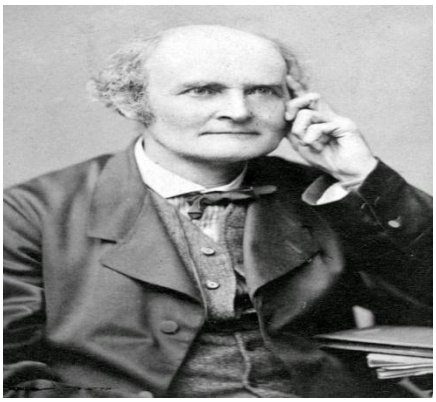
Unit-4: CAYLEY'S THEOREM AND CLASS EQUATION

CONTENT:

4.1 *INTRODUCTION*

British mathematician Arthur Cayley FRS, who lived from 16 August 1821 to 26 January 1895, was very active and focused primarily on algebra. He contributed to establishing the current British school of pure mathematics.

Cayley used to find it amusing to solve challenging arithmetic problems as a kid. He enrolled in Trinity College in Cambridge, where he excelled in mathematics, Greek, French, German, and Italian. He practised law for 14 years.



Arthur Cayley FRS

16 August 1821 – 26 January 1895

https://en.wikipedia.org/wiki/Arthur_Cayley

Theorizing that every square matrix is a root of its own characteristic polynomial, he established what is now known as the Cayley-Hamilton theorem for matrices of orders 2 and 3. He was the first to introduce the contemporary definition of a group as a set with a binary operation that complies with certain rules. Mathematicians used to refer to permutation groups when they used the term "groups." In honour of Cayley, Cayley's theorem, Cayley tables, and Cayley graphs all bear his name.

4.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the concept that how we can define an isomorphism from any group to the permutation group which is named as Cayley's theorem.
- Solve more examples on class equation.
- Understand the basic properties of Cayley's theorem and class equation and also their related other theorems.

4.3 *CAYLEY'S THEOREM*

Theorem 1: Every group G is isomorphic to a permutation group.

Proof: $A(G)$ is the collection of all permutations of the set G, where G is the any group. Let us define a map $f_a : G \to G$ such that

$f_a(x) = ax$, where $a \in G$

First we will check the mapping is well defined as,

$x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

One-One: $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ [By cancellation rule in G]

$\Rightarrow$ mapping is one-one

Onto: For any $y \in G$, since $f_a(a^{-1}y) = a(a^{-1}y) = y$. Here we can easily see that $a^{-1}y$ is pre-image of y or that f_a is onto and hence permutation on G.

Thus, $f_a \in A(G)$

Assume that K be set of all such permutations. Now we will show that K is a subgroup of $A(G)$. Since K is non-empty set because $f_e \in K$.

Let $f_a, f_b \in K$

Then since $f_b o f_{b^{-1}}(x) = f_b\left(f_{b^{-1}}(x)\right) = f_b(b^{-1}x) = b(b^{-1}x)$

$= ex = f_e(x) \forall x$

We find $f_{b^{-1}} = (f_b)^{-1}$ [Note $f_e = I$, identity of $A(G)$]

Also as $(f_a o f_b)(x) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x) \forall x$

We find $f_{ab} = f_a o f_b$

So, $f_a o (f_b)^{-1} = f_a o f_{b^{-1}} = f_{ab^{-1}} \in K$

$\Rightarrow K$ is subgroup of $A(G)$.

Define mapping $\phi : G \to K$, s.t.,

$\phi(a) = f_a$

then ϕ is well defined as well as one-one map as,

$a = b$

$\Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x) \ \forall x$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \phi_a = \phi_b$

Obviously, ϕ is onto and

$\phi(ab) = f_{ab} = f_a o f_b = \phi(a)\phi(b)$

Hence, ϕ is a homomorphism and also an isomorphism which proves the result that every group G is isomorphic to a permutation group.

Remarks: We can define other statement of Cayley's theorems like " If G is finite group of order n then G will be isomorphic to the subgroup of symmetric group S_n.

Example 1: Using Cayley's theorem find the permutation group which is isomorphic to the group $G = \{2,4,6,8\}$ under the operation multiplication modulo $(\times_{10})$.

Answer: Let A be any permutation group such as defined in the Cayley's theorem.

$A = \{f_a \mid a \in G\}$, where f_a is defined as $f_a = ax \ s.t. \ \ a, x \in G$

So, $f_2(2) = 4, \ f_2(4) = 8, \ f_2(8) = 6, \ f_2(6) = 2$

$f_4(2) = 8, \ f_4(4) = 6, \ f_4(8) = 2, \ f_4(6) = 4$

$f_8(2) = 6, \ f_8(4) = 2, \ f_8(8) = 4, \ f_8(6) = 8$

$f_6(2)=2,\ f_6(4)=4,\ f_6(8)=8,\ f_6(6)=6$

Thus, $f_6 = I$ and $K=\{f_2, f_4, f_8, f_6 = I\}$

If we identify f_2 with the permutation (1234), other permutations are $(13)(24),(1432)$. Hence $A=\{(123),(13)(24),(1432),I\}$ is required permutation group isomorphic to G.

Example 2: Using Cayley's theorem find the permutation group which is isomorphic to the D_4.

Answer: As we know that the dihedral group (D_4) of order 8 is

$D_4=\{a,a^2,a^3,a^4,ab,a^2b,a^3b,a^4b \mid a^4=e=b^2, ab=ba^{-1}\}$

Let the set defined in the Cayley's theorem is given by $K=\{f_x \mid x\in G\}$ where function defined by, $f_x(y)=xy$ and $D_4 \cong K$ by the theorem. Now we determine K, the required permutation group as

$f_a(a)=a^2,\ f_a(a^2)=a^3,\ f_a(a^3)=a^4=e,\ f_a(ab)=a^2b$

$f_{a^2}(a^2b)=b,\ f_a(a^3b)=b,\ f_a(b)=ab,\ f_a(e)=a$

Thus f_a can be identified with the permutation $(1234)(5678)$

Again, $f_{a^2}(a)=a^3,\ f_{a^2}(a^2)=e,\ f_{a^2}(a^3)=a,\ f_{a^2}(ab)=a^3b$

$f_{a^2}(a^2b)=b,\ f_{a^2}(a^2b)=ab,\ f_{a^2}(b)=a^2b,\ f_{a^2}(e)=a^2$

Thus, f_{a^2} can be identified with $(13)(24)(57)(68)$.

In the continuation, we can say, $f_{a^3}=(1432)(5876)$

Again, $f_{ab}(a)=aba=b,\ f_{ab}(a^2)=aba^2=a^3b$ etc., we get

$f_{ab}=(18)(27)(36)(45)$

Similarly, $f_{a^2b}=(15)(28)(37)(46)$

$f_{a^3b}=(16)(25)(38)(47)$

$f_b=(17)(26)(35)(48)$

Therefore, $K=\left\{\begin{matrix}(1234)(5678),(13)(24)(57)(68),(1432)(5876),I,(18)(27)(36)(45),\\(15)(28)(37)(46),(16)(25)(38)(47),(17)(26)(35)(48)\end{matrix}\right\}$

Hence, $K\cong D_4$

4.4 *CLASS EQUATION*

In the unit 2 we have already learned about some important theorems of class equations and their proof which are as follows:

Theorem 2: If *G* be the finite group and *Z*(*G*) be the centre of the group *G*. Then class equation of *G* can be written as

$$O(G) = O[Z(G)] + \sum_{a \notin Z(G)} \frac{O(G)}{O[N(a)]}$$

In this section we will learn applications part of class equation in different type of examples. **Example 3:** If n is the index of $Z(G)$ in a group G then the conjugate class has at most n elements.

Answer: We have $n = \frac{O(G)}{O(Z(G))}$ and $O(cl(a)) = \frac{O(G)}{O(N(a))}$

Since, $Z(G) \subseteq N(a)$ always

$O(Z(G)) \subseteq O(N(a)) \Rightarrow O(N(a)) = k.O(Z(G))$

i.e., $O(C(a)) = \frac{O(G)}{O(N(a))} = \frac{n.O(Z(G))}{k.O(Z(G))} = \frac{n}{k}$

Hence, maximum value of $O(C(a))$ is when $k = 1$.

Example 4: If P^3 be order of a non-abelian group then determine $O(Z(G))$ and also number of conjugate classes of *G*.

Solution: We have given group (G) is non-abelian, $\exists a \in G$, s.t., $Z(G) \subsetneq N(a) \subsetneq G$

Since we know that $O(Z(G)) \mid O(G) = P^3$

So, the possibilities that $O(Z(G))$ will be $1, P, P^2, P^3$

Similarly $O(N(a)) = 1, P, P^2, P^3$

But by the previous theorems we know that $O(Z(G)) \neq 1$. Since group is non-abelian then $O(Z(G)) \neq P^3$. So, the only possibilities will be $O(Z(G)) = P \, or \, P^2$.

Similarly, $O(N(a)) = P \, or \, P^2$ and as $Z(G) \subsetneq N(a)$

So, we find $O(Z(G)) = P$, $O(N(a)) = P^2$

Let we assume *k* be the total number of conjugate classes. Since

$$G = \bigcup_{a \in G} C(a)$$

$$O(G) = \sum_{a \in G} O(C(a)) = \sum_{a \in Z(G)} O(C(a)) + \sum_{a \notin Z(G)} O(C(a))$$

$$p^3 = O(Z(G)) + \sum_{a \notin Z(G)} O(C(a))$$

When $a \in Z(G)$ then number of conjugate classes is $O(Z(G)) = p$

[Since $a \in Z(G) \Leftrightarrow C(a) = \{a\} \, or \, O(C(a)) = 1$]

So, $k-p$ are remaining classes and each have order given by

$$O(C(a)) = \frac{O(G)}{O(N(a))} = \frac{p^3}{p^2} = p$$

Hence, $p^3 = p + (k-p)p \Rightarrow k = p^2 + p - 1$

Example 5: Write the class equation of quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Solution: We have the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

First we determine the conjugate class of i. Since we know that in any group $< a > \subseteq N(a)$

[$x \in < a > \Rightarrow x = a^m$ and as $a.a^m = a^m.a$, we find $a^m \subseteq N(a)$]

Thus, $< i > \subseteq N(i)$ or $\{i, i^2, i^3, i^4 = 1\} \subseteq N(i)$

Therefore, $< i > \subseteq N(i) \leq Q_8$ gives $4 \mid O(N(i)) \mid 8$

Since $j \notin N(i)$ because $ji \neq ij$

And $j \in Q_8 \Rightarrow N(i) \subsetneq Q_8$

Hence $O(N(i)) = 4$ or $N(i) = < i >$

As we know that $O(C(a)) = \frac{O(G)}{O(N(a))}$

$$\Rightarrow O(C(i)) = \frac{O(Q_8)}{O(N(i))} = \frac{8}{4} = 2$$

$\Rightarrow C(i) = \{i, -i\}$ [as $i \in C(i)$ and $-i = kik^{-1}, -i \in C(i)$]

Similarly other conjugate classes are $C(j) = \{j, -j\}, C(k) = \{k, -k\}, \{1\}, \{-1\}$

Since we know that $O(C(a)) = 1 \Leftrightarrow a \in Z(G)$ then as $O(C(1)) = 1, O(C(-1)) = -1$

$\Rightarrow Z(Q_8) = \{1, -1\}$

Now, we verify the class equation as

$$O(G) = O(Z(G)) + \sum_{a \notin Z(G)} O(C(a))$$

$8 = 1 + 1 + (2 + 2 + 2)$, which is the class equation of the group Q_8.

Example 6: For a finite group G let number of conjugate class is 3. Then prove that either group is cyclic or isomorphic to S_3.

Solution: Since we have given that group G has number of conjugate classes are 3. If these conjugate classes are of order 1, then $O(G) = 3$, which is of order prime that means group will be cyclic. If G has a class of order >1 then G is non-abelian because if G will abelian then there does not exist any class of order >1.

Let three classes of G are C_1, C_2, C_3.

Assume that $O(C_3) > 1$.

If $O(C_1) = O(C_2) = 1 \Rightarrow O(C_3) = n - 2$ [If we have assume that $O(G) = n$]

$\because O(C_3) = n-2 \mid O(G)$ and also we have $n-2 \mid n-2$

$\Rightarrow (n-2) \mid n-(n-2) = 2$

$\Rightarrow n-2 = 1 or\ 2$

$\Rightarrow n = 3 or\ 4$

$\Rightarrow G$ is abelian. [Because we know every group of order $p\ or\ p^2$ is abelian]

Now there is only one possibility left that in G one class is of length 1. Let $O(C_1) = 1, O(C_2) > 1, O(C_3) > 1$. It means $O(Z(G)) = 1$.

By class equation, $n = O(G) = O(C_1) + O(C_2) + O(C_3) = 1 + O(C_2) + O(C_3)$

But $O(C_3) \mid O(G) = n, O(C_3) \mid O(C_3)$

$\Rightarrow O(C_3) \mid n - O(C_3) = 1 + O(C_2)$

$\Rightarrow O(C_3) \leq 1 + O(C_2)$

Similarly, $O(C_2) \leq 1 + O(C_3)$

If $O(C_3) < 1 + O(C_2)$ and $O(C_2) < 1 + O(C_3)$

Then $O(C_3) \leq O(C_2)$, $O(C_2) \leq O(C_3)$

$\therefore O(C_3) = O(C_2)$

$\therefore O(C_3) \mid 1 + O(C_3) \Rightarrow O(C_3) \mid 1 \Rightarrow O(C_3) = 1$

This is a contradiction

Thus either $O(C_3) = 1 + O(C_2)$

Or $O(C_2) = 1 + O(C_3)$

If $O(C_3) = 1 + O(C_2)$

Then $O(G) = 1 + O(C_2) + 1 + O(C_2)$

$\Rightarrow O(G) - 2O(C_2) = 2$

But $O(C_2) \mid O(G), O(C_2) \mid O(C_2) \Rightarrow O(C_2) \mid 2O(C_2)$

$\therefore\ O(C_2) \mid O(G) - 2O(C_2) = 2$

$\therefore\ O(C_2) = 2$ and $O(C_3) = 3$

Or that $O(G) = 6$

Similarly, if $O(C_2) = 1 + O(C_3)$, then $O(G) = 6$

$\therefore$ G is non-abelian group of 6 which is isomorphic to S_3 i.e., $G \cong S_3$.

Example 7: Let G be a group such that $e \neq a \in G$, $O(a) =$ finite. If G has only two conjugate classes then prove that G is a group of order 2.

Answer: Let $e \neq b \in G$. Since G has only 2 conjugate classes, namely $\{e\}$ and $C(a)$.

$b \in C(a) \therefore b = g^{-1}ag$ for some $g \in G$.

$\therefore$ $O(b) = O(a)$ for all $b \neq e$ in G.

Suppose $O(a) = mn, m > 1, n > 1$

Then $O(a^m) = m$

Since order of all non identify elements in G is same, $O(a^m) = mn$

$\therefore n = mn \Rightarrow m = 1$; a contradiction

$\therefore O(a) = p = prime$

$\therefore O(b) = p =$ for all $e \neq b \in G$

Suppose $p \neq 2$

then $a^2 \neq e \Rightarrow a^2 \in C(a)$

$\therefore a^2 = g^{-1}ag$ for some $g \in G$

$\therefore (a^2)^2 = (g^{-1}ag)^2 = g^{-1}a^2g$

$\therefore (a^2)^2 = (g^{-1}ag)^2 = g^{-1}(g^{-1}ag)g = g^{-2}ag^2$

In this way, we get $a^{2^p} = g^{-p}ag^p$

Since $O(g) = O(a) = p$

$a^{2^p} = eae = a$

$\Rightarrow a^{2^p - 1} = e \Rightarrow O(a) = p \mid 2^p - 1$

By Fermat's theorem, $p \mid 2^p - 2$

$\therefore$ $p \mid (2^p - 1) - (2^p - 2) = 1$, a contradiction

$\therefore$ $p = 2$

$\Rightarrow O(a) = 2$. So, $O(b) = 2$ for all $e \neq b \in G$

$\Rightarrow G$ is abelian.

So, each conjugate class in G is of length one. Since G has only two classes, which means G is of order 2.

Note: There are infinite group having non-trivial element has finite order and group has only 2 conjugate classes. Therefore, it is necessary to assume that $\exists e \neq a \in G$ s.t. $O(a) = \text{finite}$.

4.5 *PARTITION OF AN INTEGER*

Let n be a positive integer. A sequence of positive integers $n_1, n_2, ..., n_k$ where $n_1 \leq n_2 \leq ... \leq n_k$ such that $n = n_1 + n_2 + ... + n_k$ is called a partition of n and $n_1, n_2, ..., n_k$ are called parts of partition.

For example, let $n = 3$, then number of partition are 3 i.e.,

$$3 = \begin{cases} 1+1+1 \\ 1+2 \\ 3 \end{cases}$$

let $n = 4$, then number of partition are 5 i.e.,

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 2+2 \\ 1+3 \\ 4 \end{cases}$$

The number of partition of any integer n is denoted by $P(n)$. For example, $P(1) = 1$, $P(2) = 1, P(3) = 4, P(4) = 5$ e.tc.

Theorem 3: The number of conjugate classes in S_n is $P(n)$.

Proof: Let $A =$ Collection of all conjugate classes in S_n.

$B =$ Collection of all partition of *n*.

Let $C(\sigma), \sigma \in S_n$.

Assume that σ as product of disjoint cycles as $(a_1 ... a_{n_1})(b_1 ... b_{n_k})$ where $n_1 + ... + n_k = n$.

the selection of cycles in a pattern such that $n_1 \leq ... \leq n_k$. This gives a partition

$\{n_1, n_2, ..., n_k\}$ of n.

Now we define $f : A \to B$ s.t.,

$f(C(\sigma)) = \{n_1, n_2, ..., n_k\}$

f is well defined as $C(\sigma) = C(\eta)$

$\Rightarrow \sigma, \eta \in C(\sigma)$

$\Rightarrow \sigma, \eta$ are conjugate in S_n

$\Rightarrow \sigma, \eta$ are similar in S_n

$\Rightarrow \sigma = (a_1,...,a_{n_1})..(b_1,...,b_{n_k})$

$\eta = (a_1',...,a'_{n_1})..(b'_1,...,b'_{n_k})$

$\Rightarrow f(C(\sigma)) = \{n_1, n_2,..., n_k\} = f(C(\eta))$

Suppose $C(\sigma) \neq C(\eta)$

So, σ, η are not conjugate $\Rightarrow \sigma, \eta$ are not similar

$\Rightarrow \sigma, \eta$ have different cycle structure

$\Rightarrow$Corresponding partitions are different

i.e., $\{n_1, n_2,..., n_k\} \neq \{n'_1, n'_2,..., n'_r\}$ where, of course,

$n = n_1 + n_2 + ... + n_k = n'_1 + n'_2 + ... + n'_r$

$\Rightarrow f(C(\sigma)) \neq f(C(\eta))$

$\Rightarrow f$ is one-one

f is onto for, let $\{n_1, n_2,..., n_k\} \in B$ be a partition of n. Then $n = n_1 + n_2 + ... + n_k$

Define $\sigma = (a_1,...,a_{n_1})..(b_1,...,b_{n_k}) \in S_n$

Then $C(\sigma) \in A$

And $f(C(\sigma)) = \{n_1, n_2,..., n_k\}$

$\therefore f$ is both 1-1 and onto

So, $O(A) = O(B) = P(n)$

$\Rightarrow$number of conjugate classes in S_n is $P(n)$

Example 8: Verify the class equation in S_4 and also find its all conjugate classes.

Answer: By the theorem 4 we know that number of conjugate classes in S_4 are $P(4)$ which is 5. Also we know that two conjugate classes of any group are either disjoint or identical. In other word we can say that two permutations are conjugate if and only they are similar. In S_4 the base elements of conjugate classes are $I, (12), (123), (1234), (12)(34)$

As we know that in the permutation group S_n number of distinct *r*-cycle are $\frac{1}{r}\frac{n!}{(n-r)!}$. So, in S_4 number of distinct cycle of length 2 are $\frac{1}{2}\frac{4!}{(4-2)!} = 6$

Similarly, in S_4 number of distinct cycle of length 3 are $\frac{1}{3}\frac{4!}{(4-3)!} = 8$

Similarly, in S_4 number of distinct cycle of length 4 are $\frac{1}{4}\frac{4!}{(4-4)!}=6$

in S_4 number of permutation of type $(a\,b)(c\,d)$ are $(12)(34),(13)(24),(14)(23)$

so, $O(C((12)(34))=3$

Since centre of S_4 contains only identity element so, $O(Z(S_4))=1$ i.e., $O(C(I))=1$

Now the class equation of S_4 is,

$$O(S_4)=O(Z(S_4))+\sum_{a\notin Z(S_4)}\frac{O(S_4)}{O(N(a))}=O(Z(S_4))+\sum_{a\notin Z(S_4)}O(C(a))$$

i.e., $24=1+6+8+6+3$

Example 9: Find the class equation of a group of order 6.

Answer: Let G be a group of order 6. So, there are two cases arises that either group is abelian or not.

Case I: Let group is abelian then we know that G will be isomorphic to Z_6 i.e., $G\cong Z_6$ *or* $G\cong Z_2\times Z_3$

Since G is abelian then $O(Z(G))=6$

So, the class equation will be, $6=1+1+1+1+1+1$

Case II: If group is non-abelian then we know that G will be isomorphic to S_3 or D_3 i.e., $G\cong S_3\cong D_3$

As we know that the permutation on group on the 3 symbol $\{1,2,3\}$ is $S_3=\{I,(12),(13),(23),(123),(132)\}$.

Initially we examine the conjugacy classes of S_3 for it first we will find center element of S_3.

Since, $(12)(13)=(132)\neq(123)=(13)(12)$ and $(12)(23)=(123)\neq(132)=(23)(12)$ and so $(12),(23),(13)\notin Z(S_3)$

Further, $(123)(12)=(13)\neq(23)=(12)(123)$ and $(132)(12)=(23)\neq(13)=(12)(132)$.

So, $(123),(132)\notin Z(S_3)$. So the only trivial conjugacy class is [(1)]={1} i.e., $Z(S_3)=I$ or $O(Z(S_3))=1$.

Now observe that for the element (12) we have that:

$(12)(12)(12)^{-1}=(12)(12)(21)=(12)$

$(13)(12)(13)^{-1}=(13)(12)(31)=(23)$

$(23)(12)(23)^{-1}=(23)(12)(32)=(13)$

$(123)(12)(123)^{-1}=(123)(12)(321)=(23)$

$(132)(12)(132)^{-1} = (132)(12)(231) = (13)$

So, the conjugacy class of (12) is $C((12)) = \{(12),(13),(23)\}$ and the conjugacy classes of remaining elements are $C((123)) = C((132)) = \{(123),(132)\}$

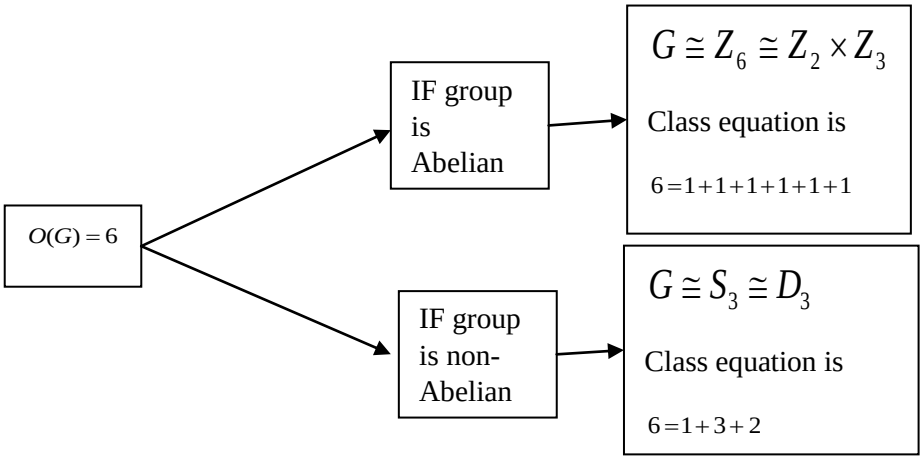
So, the conjugacy classes of S_3 is,

$S_3 = C(I) \cup C((12)) \cup C((123))$

And the class equation is,

$6 = 1+3+2$

Hence,



Note: Two permutations in S_n are conjugates iff they have the same cycle type. Let $\sigma \in S_n$ and also let $m_1, m_2, ..., m_r$ are the distinct integers which appear in $a_1, a_2, ..., a_r$ times respectively in the cycle type of σ (including 1 cycles). Let a_i be the number of cycles of length $m_i, i = 1 to r$, so that

$$\sum_{i=1}^{r} a_i m_i = n$$

then, number of conjugate of $\sigma = \dfrac{n!}{(m_1^{a_1} a_1!)(m_2^{a_2} a_2!)...(m_r^{a_r} a_r!)}$

OR

Number of element commutes with $\sigma = \dfrac{n!}{(m_1^{a_1} a_1!)(m_2^{a_2} a_2!)...(m_r^{a_r} a_r!)}$

Example 10: Find the number of cycle which commute with $\alpha = (543)(26)(78910) \in S_{10}$

Solution: We first rewrite the given permutation as $\alpha = (1)(543)(26)(78910) \in S_{10}$. Since all cycles of permutations are disjoint so they are commutes i.e., $\alpha = (1)(26)(543)(78910) \in S_{10}$. So, cycle type of α is,

Cycle of length $1 = (1)$

Cycle of length $2 = (26)$

Cycle of length $3 = (543)$

Cycle of length $4 = (78910)$

i.e., cycle type of $\alpha = (1,2,3,4)$, where $1+2+3+4=10$

So, number of conjugate of $\alpha = \frac{10!}{(1^1 1!)(2^1 1!)(3^1 1!)(4^1 1!)} = \frac{10!}{2.3.4}$

Example 11: Find the number of cycle which commute with $\alpha = (596)(874)(12) \in S_{11}$

Solution: We first re-write the given permutation as $\alpha = (12)(596)(874) \in S_{11}$. Since all cycles of permutations are disjoint so they are commutes i.e., $\alpha = (3)(4)(10)(11)(1\ 2)(596)(874) \in S_{11}$. So, cycle type of α is,

Cycle of length $1 = (3)(4)(10)(11)$

Cycle of length $2 = (1\ 2)$

Cycle of length $3 = (596)$

Cycle of length $4 = (874)$

i.e., cycle type of $\alpha = (1,1,1,1,2,3,3)$, where $1+1+1+1+2+2+3=11$

So, number of conjugate of $\alpha = \frac{11!}{(1^4 4!)(2^1 1!)(3^2 2!)} = \frac{11!}{4!.2.9.2}$

Example 12: Evaluate all permutations in A_5 which commutes with

(***i***) $\alpha = (12345)$ (***ii***) $\beta = (123)$ (***iii***) $\gamma = (12)(34)$

Solutions (***i***)**:** As we know that $O(A_5) = \frac{O(S_5)}{2} = \frac{120}{2} = 60$. Since $\alpha = (12345) \in A_5$ and $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 = I$ are distinct permutation in A_5.

$\therefore O(N(\alpha)) = 5 \text{ in } A_5$

$\therefore O(C(\alpha)) = \frac{O(A_5)}{O(N(\alpha))} = \frac{60}{5} = 12$ in A_5

As we know (12345) and (13245) break up into two conjugate classes each conjugate classes are of length 12 in A_5.

(***ii***)**:** Let $\theta \in S_5$ s.t. θ fixes 1, 2, 3. Then either $\theta = (45)$ or $\theta = I$. Since $\beta\theta, \beta^2\theta, \theta$ are all permutation in S_5 commuting with β. Thus β, β^2, I are only permutation in A_5 commuting with β.

$\therefore O(N(\beta)) = 3 \text{ in } A_5$

$\therefore O(C(\beta)) = \dfrac{O(A_5)}{O(N(\beta))} = \dfrac{60}{3} = 20$ in A_5

$\therefore C(\beta)$ has all cycles of length 3 in S_5

(***iii***)**:** As we know that there are 8 permutations in S_5 commuting with γ which are:

$\{I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$. From this set only even permutation $\{I, (12)(34), (13)(24), (14)(23)\} \in A_5$. All these permutations of A_5 commuting with $\gamma = (12)(34)$

$\therefore O(N(\gamma)) = 4$ in A_5

$\therefore O(C(\gamma)) = \dfrac{O(A_5)}{O(N(\gamma))} = \dfrac{60}{8} = 15$ in A_5 which is same like $\therefore O(C(\gamma))$ in S_5.

Hence conjugate class of γ in A_5 and S_5 remains same.

Example 13: Find all the conjugate classes of A_5 and also show that A_5 is simple.

Answer: By using the previous examples we can verify that A_5 has 5 conjugate classes and these are:

$C(I) = \{I\}$

$C((123)) = \{$All 20 permutation commute with cycle (123) of length 3 in S_5.$\}$

$C((12)(34)) = \{$All 15 permutation commute with cycle $(12)(34)$ in S_5.$\}$

$C((12345)) = \{12$ cycles of length $5\}$

$C((13245)) = \{12$ cycles of length $5\}$

These are the total 60 elements in A_5.

Let H be any subgroup of A_5 which is normal s.t $H \neq \{I\}$, $H \neq \{A_5\}$. As H is the union of some conjugate classes in A_5. Since $I \in H, O(H)$ cannot divide $O(A_5) = 60$.

Hence, A_5 is simple.

Check your progress

Problem 1: What will be the class equation of any group of order 3?

Problem 2: What will be the class equation of Klein group (**Klein group:** Any group of order 4 such that each of its non-identity elements are self inverse, generally this group is denoted by K_4-group)?

Problem 3: Which of the following isomorphism relation is correct and why?

(***i***) $D_2 \cong Z_4$ (***ii***) $D_2 \cong Z_2 \times Z_2$

4.6 *SUMMARY*

In this unit, we have studied about the Cayley's theorem, various examples related to the class equations and partition of an integer. After completions of this unit learners will be able to characterized to any group into distinguish conjugacy classes and also by the class equation of any group learners will be able to find the number of element in the centre, number of different conjugate classes, number of element in the different conjugate class and order of the group. In a simple way we can say that with the help of conjugate classes we can get most of the information about the group without any prior knowledge.

4.7 *GLOSSARY*

- $P(n)$ denotes the partition of any positive integer.
- In the permutation group S_n number of distinct r-cycle is $\frac{1}{r}\frac{n!}{(n-r)!}$.
- Number of element commutes with cycle $\sigma = \frac{n!}{(m_1^{a_1}a_1!)(m_2^{a_2}a_2!)...(m_r^{a_r}a_r!)}$.

4.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- See Cayley (1858) "A Memoir on the Theory of Matrices", *Philosophical Transactions of the Royal Society of London*, **148** : 24 : "I have verified the theorem, in the next simplest case, of a matrix of the order 3, … but I have not thought it necessary to undertake the labour of a formal proof of the theorem in the general case of a matrix of any degree."
- Cayley (1854) "On the theory of groups, as depending on the symbolic equation $\theta^n = 1$," *Philosophical Magazine*, 4th series, **7** (42) : 40–47. However, see also the criticism of this definition in: MacTutor: The abstract group concept.

4.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

4.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. State and prove the Cayley's theorem.

2. Prove that dihedral group D_3 is isomorphic to the symmetric group S_3.

3. Find number of conjugate classes in S_5.

4. Find the class equation of a non-abelian group of order 8.

5. Find the number of cycle which commute with $\alpha = (596)(874) \in S_{11}$.

6. Prove that A_5 is simple.

7. Let G be a group such that $e \neq a \in G$, $O(a) =$ finite. If G has only two conjugate classes then prove that G is a group of order 2.

8. Prove that the number of conjugate classes in S_n is $P(n)$.

9. Find the conjugate class of i and -1 in Q_8 and also find the class equation of Q_8.

Short Answer Type Question:

10. Write the class equation of non-abelian group of order 2^3.

11. Write all the partition of 5 i.e., $P(5)$.

12. Find the number of elements in the centre of the group having class equation $8 = 1+1+(2+2+2)$.

13. Write the class equation of $U(7) = \{1,2,3,4,5,6\}$ under the operation multiplication modulo 7.

Fill in the blanks:

14. Every group G is isomorphic to a …….

15. A_5 is ……. group.

16. Number of conjugate classes in S_n are …….

17. The class of non-abelian group of order 6 is ……

18. If the class equation of any group is $4=1+1+1+1$ then group is ……

4.11 *ANSWERS*

Answer of self cheque question:

1. 1+1+1 **2.** 1+1+1+1

3. $D_2 \cong Z_2 \times Z_2$ is correct because D_2 is abelian group not cyclic.

Answer of terminal question:

3. 6 **5.** $\frac{11!}{(1^5 5!)(3^2.2!)}$ **9.** $C(i)=\{i,-i\}, C(-1)=\{-1\}$ and class equation is $8=1+1+(2+2+2)$ **14.** Permutation group **15.**Simple **16.** $P(n)$

17. 6 = 1+2+3 **18.** Abelian

Unit-5: DIRECT PRODUCT OF GROUPS AND CAUCHY'S THEOREM FOR FINITE ABELIAN GROUPS

CONTENT:

5.1 *INTRODUCTION*

Baron Augustin-Louis Cauchy, a French mathematician, engineer, and physicist who lived from 21 August 1789 to 23 May 1857, produced groundbreaking discoveries in the fields of continuum mechanics and mathematical analysis. He rejected the prior authors' heuristic principle of the universality of algebra and was one of the first to state and formally verify calculus truths. He practically single-handedly founded abstract algebra's study of permutation groups and complex analysis.

Augustin-Louis Cauchy

21 August 1789 to 23 May 1857

https://en.wikipedia.org/wiki/Augustin-Louis_Cauchy

According to Cauchy's theorem, which is found in mathematics and more especially group theory, if G is a finite group and p is a prime integer that divides G's order (the number of its members), then G includes one element of order p.

The direct product is an operation in mathematics, notably in group theory, that takes two groups, G and H, and creates a new group, commonly designated $G \times H$. One of the crucial ideas of direct product in mathematics, this operation is the group-theoretic equivalent of the Cartesian product of sets.

5.2 *OBJECTIVES*

After reading this unit learners will be able to

- Implementation of Cauchy's theorem in different types of group.
- Describe the direct product of two or more than two groups.
- Analyze the theorems related to Cauchy's theorem and direct product of groups.

5.3 *EXTERNAL DIRECT PRODUCT*

In this section, we create an appropriate binary operation $(*)$ that we term the external direct product of groups on the cartesian product $G_1 * G_2$ of two groups, G_1 and G_2. This method is frequently used to create new groups out of existing ones as well as to break down existing groups into their component parts. Thus, an essential idea in the structure theory of finite groups is the external direct product of groups.

Let the $n-$groups, $G_1, G_2, G_3, ..., G_n$ are such that $G = G_1 \times G_2 \times G_3 \times ... \times G_n$ under the operation $*$, defined by

$(a_1, a_2, a_3, ..., a_n) * (b_1, b_2, b_3, ..., b_n) = (a_1 b_1, a_2 b_2, a_3 b_3, ..., a_n b_n)$

Where each $(a_1, a_2, a_3, ..., a_n), (b_1, b_2, b_3, ..., b_n) \in G = G_1 \times G_2 \times G_3 \times ... \times G_n$ and $a_i b_i, i = 1 to n$

For e.g., if the binary operation $*$ between the groups $K_4 \times Z$ defined by

$(a, m) * (b, n) = (ab, m + n) \forall (a, m), (b, n) \in K_4 \times Z$

Since the group $K_4 \times Z$ have the identity element $(e, 0)$ and for every element $(a, n) \in K_4 \times Z$ there exist $(a, n)^{-1} = (a, -n) \in K_4 \times Z$ [Because every element in K_4 is self inverse and K_4 is additive inverse of n in Z]

Similarly, $(G,*)$ is a group with identity elements $e=(e_1,e_2,e_3,...,e_n)$ and $(a_1,a_2,a_3,...,a_n)^{-1}=(a_1^{-1},a_2^{-1},a_3^{-1},...,a_n^{-1})$ for every $(a_1,a_2,a_3,...,a_n)\in G$ where e_i is the element of G_i for every $i=1,2,...,n$

Definition: Let $G_1,G_2,G_3,...,G_n$ are n groups and $G=G_1\times G_2\times G_3\times...\times G_n$ then $(G,*)$ is called the external direct product of the groups $G_i, i=1\ to\ n$.

Example 1: Consider the group S_3 and infinite group $(Z,+)$. Then the operation $*$ on $S_3\times Z$ is given by: $(\alpha,m)*(\beta,n)=(\alpha\beta,m+n)$

Since identity element is $(e,0)$ and $(\alpha,m)^{-1}=(\alpha^{-1},-m)\ \forall\ \alpha\in S_3, m\in Z$. For example,

$((12),4)^{-1}=((12),-4)$

And $((123),2)^{-1}=((132),-2)$

Now,

$((12),4)*((13),7)=((12)(13),4+7)=((132),11)$

And $((13),7)*((12),4)=((13)(12),7+4)=((123),11)$

Which shows that $S_3\times Z$ is non-commutative. Also $S_3\times Z$ is an infinite group.

Note: It is interesting to observe that non-commutativity of $S_3\times Z$ comes from the non-commutative group S_3 whereas the infiniteness comes from Z.

Theorem 1: Let G_1 and G_2 are two groups. Then $G_1\times G_2\cong G_2\times G_1$.

Proof: First, we define the mapping $f: G_1\times G_2\to G_2\times G_1$ by,

$f(a,b)=(b,a)\ \forall\ (a,b)\in G_1\times G_2$.

Then

$$\begin{aligned} f((a_1,b_1)*(a_2,b_2)) &= f(a_1a_2,b_1b_2)\\ &= f(b_1b_2,a_1a_2)\\ &= (b_1,a_1)*(b_2,a_2)\\ &= f(a_1,b_1)*(a_2,b_2)\end{aligned}$$

$\Rightarrow f$ is a homomorphism and also f is one-one and on-to

$\Rightarrow f$ is an isomorphism.

Hence, $G_1\times G_2\cong G_2\times G_1$

Theorem 2: Let $G_1,G_2,...,G_n$ are *n*-groups. Then the group $G=G_1\times G_2\times...\times G_n$ is abelian if and only if each of the group $G_i, i=1\ to\ n$ is abelian.

Proof: First we assume that G is abelian then we will prove that each $G_i, i=1\ to\ n$ will also abelian.

Let us assume for $1 \le i \le n$ and $a, b \in G_i$. Then $(e_1, e_2, ..., e_{i-1}, a, e_{i+1}, ..., e_n)$, $(e_1, e_2, ..., e_{i-1}, b, e_{i+1}, ..., e_n)$, G and commutativity of G implies that

$(e_1, e_2, ..., e_{i-1}, a, e_{i+1}, ..., e_n) * (e_1, e_2, ..., e_{i-1}, b, e_{i+1}, ..., e_n) = (e_1, e_2, ..., e_{i-1}, b, e_{i+1}, ..., e_n) *$
$(e_1, e_2, ..., e_{i-1}, a, e_{i+1}, ..., e_n)$

$\Rightarrow (e_1, e_2, ..., e_{i-1}, ab, e_{i+1}, ..., e_n) = (e_1, e_2, ..., e_{i-1}, ba, e_{i+1}, ..., e_n)$

$\Rightarrow ab = ba$

Thus $\forall\, i=1\ to\ n, G_i$ is abelian.

Conversely, assume that each $G_i, i=1\ to\ n$ is abelian. Let $(a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n) \in G$. Then $a_i b_i \in G_i$ and since each G_i is abelian, so $a_i b_i = b_i a_i, 1 \le i \le n$.

Now, $(a_1, a_2, ..., a_n) * (b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$

$$= (b_1 a_1, b_2 a_2, ..., b_n a_n)$$

$$= (b_1, b_2, ..., b_n)(a_1, a_2, ..., a_n)$$

$\Rightarrow G_i$ is abelian

Theorem 3: If $G_1, G_2, ..., G_n$ are *n*-groups then $Z(G_1 \times G_2 \times ... \times G_n) \cong Z(G_1) \times Z(G_2) \times ... \times Z(G_n)$.

Proof: To prove the mentioned theorem, it will be sufficient to prove that result is true for $n=2$. Let two groups are G_1, G_2 and also consider $x \in G_1, y \in G_2$. Then

$(x, y) \in Z(G_1 \times G_2)$

$\Leftrightarrow (x, y) \in (g_1, g_2) = (g_1, g_2) * (x, y) \forall (g_1, g_2) \in G_1 \times G_2$

$\Leftrightarrow (xg_1, yg_2) = (g_1 x, g_2 y) \forall (g_1, g_2) \in G_1 \times G_2$

$\Leftrightarrow xg_1 = g_1 x\ and\ yg_2 = g_2 y \forall g_1 \in G_1, g_2 \in G_2$

$\Leftrightarrow x \in Z(G_1)\ and\ y \in Z(G_2)$

$\Leftrightarrow (x, y) \in Z(G_1) \times Z(G_2)$

Thus $Z(G_1 \times G_2) \cong Z(G_1) \times Z(G_2)$

Example 2: Prove by example that product of two cyclic may or may not be cyclic.

Proof: As we know that Z_4, Z_6 are two cyclic group while $Z_4 \times Z_6$ is not a cyclic group because order of $Z_4 \times Z_6$ is 24 but $Z_4 \times Z_6$ have no element of order 24.

In another example Z_2, Z_3 are two cyclic group and $Z_2 \times Z_3$ is also a cyclic group because order of $Z_2 \times Z_3$ is 6 and $(1, 2) \in Z_2 \times Z_3$ have order 6. Then by theorem $Z_2 \times Z_3$ is cyclic.

Theorem 4: Let two finite cyclic group G_1, G_2 of order m, n respectively. Then $G_1 \times G_2$ is cyclic if and only if $\gcd(m,n) = 1$

OR

Element (a,b) is a generator of $G_1 \times G_2$ *iff* elements a, b are individually generators of the group G_1, G_2 respectively.

Proof: First we assume that $G_1 \times G_2$ is cyclic group and also assume that (a,b) is generator of $G_1 \times G_2$ *i.e.*, $G_1 \times G_2 =< (a,b) >$. Then $O((a,b)) = mn$. Let $d = \gcd(m,n)$.

Now $(a,b)^{\frac{mn}{d}} = (a^{m\frac{n}{d}}, b^{n\frac{m}{d}}) = (e_1, e_2)$

$\Rightarrow mn \mid \frac{mn}{d}$

$\Rightarrow d = 1$

Conversely, assume that $\gcd(m,n) = 1$. Let us consider that a is the generator of G_1 ($G_1 =< a >$) and b is the generator of G_2 ($G_2 =< b >$). If we denote $O(a,b) = k$ then $(a,b)^{mn} = (a^{mn}, b^{mn}) = (e_1, e_2)$

$\Rightarrow k \mid mn$

Now, $(a^k, b^k) = (a,b)^k = (e_1, e_2)$

$\Rightarrow a^k = e_1$ and $b^k = e_2$; and so, $\Rightarrow m \mid k, n \mid k$

Then $\gcd(m,n) = 1 \Rightarrow mn \mid k$

Therefore, $k = mn = O(G_1 \times G_2) = |G_1 \times G_2|$.

Hence $G_1 \times G_2 =< (a,b) >$ is cyclic group.

Corollary: $Z_m \times Z_n \cong Z_{mn}$ iff $\gcd(m,n) = 1$

Proof: By the previous theorem we know that in a group for any element $a \in G_1$ of order m and $b \in G_2$ of order n, if $\gcd(m,n) = 1$, then

$O((a,b)) = mn$

Hence, $Z_m \times Z_n \cong Z_{mn} \Leftrightarrow \gcd(m,n) = 1$

e.g., Since $\gcd(2,3) = 1 \Leftrightarrow Z_2 \times Z_3 \cong Z_{2.3}$ or $Z_2 \times Z_3 \cong Z_6$

Theorem 5: For the finite groups G_1 and G_2 the order of $(a,b) \in G_1 \times G_2$ is $O((a,b)) = lcm(O(a), O(b))$.

Proof: As we know by definition that if $(a,b) \in G_1 \times G_2 \Leftrightarrow a \in G_1, b \in G_2$. Thus $\forall\ a \in G_1, b \in G_2, O(a)$ in G_1, $O(a)$ in G_2 and $O((a,b))$ in $G_1 \times G_2$ all are finite.

Now, let n is the least positive integer such that $(a,b)^n = (e_1, e_2)$,

$\Leftrightarrow n$ is the least positive integer such that $a^n = e_1$ and $b^n = e_2$

$\Leftrightarrow O(a) \mid n, O(b) \mid n$ [By theorem that for any integer $n, a^n = e \Leftrightarrow O(a) \mid n$]

Thus, $O((a,b)) = lcm(O(a), O(b))$

Note: It is not necessary that external direct product of two cyclic group is always a cyclic group. For e.g. let $Z \times Z$ is a cyclic group such that $Z \times Z = <(a,b)>$. Since $(1,1) \in Z \times Z$, so $\exists\ r \in Z$ s.t., $r(a,b) = (1,1) \Rightarrow a = b = 1 or -1$.

$\Rightarrow <(a,b)> = \{(n,n) \mid n \in Z\} \neq Z \times Z$. Which is a contradiction.

$\Rightarrow$ our assumption is wrong that $Z \times Z$ is a cyclic i.e., $Z \times Z$ is not a cyclic group.

Theorem 6: Let two groups are G_1 and G_2. Then

$G_1 \times G_2 / G_1 \times \{e'\} \cong G_2$ and $G_1 \times G_2 / \{e\} \times G_2 \times \cong G_1$

Proof: First we define mapping, $f : G_1 \times G_2 \to G_2$ s.t.,

$f(x,y) = y\ \forall (x,y) \in H \times K$.

So, f is a homomorphism and

$$\begin{aligned} \ker f &= \{(x,y) \in G_1 \times G_2 \mid f(x,y) = e'\} \\ &= \{(x,y) \in G_1 \times G_2 \mid f(x,y) = e'\} \\ &= \{(x,e') \mid x \in G_1\} \\ &= G_1 \times \{e'\} \end{aligned}$$

Since f is also onto function. Hence by using the first isomorphism theorem $G_1 \times G_2 / G_1 \times \{e'\} \cong G_2$.

Similarly, we have $G_1 \times G_2 / \{e\} \times G_2 \times \cong G_1$.

Theorem 7: Let G and G' are two groups. If H and H' are two normal subgroups of G and G' respectively, then $H \times H'$ is normal in $G \times G'$ and

$G \times G' / H \times H' \cong G / H \times G' / H'$

Proof: First we will define the mapping, $f : G \times G' \to G / H \times G' / H'$ by,

$f(x,y) = (xH, yH')\ \forall (x,y) \in G \times G'$.

Then, $\forall (x,y), (z,w) \in G \times G'$,

$f((x,y) * (z,w)) = f(xy, zw)$

$$= (xyH, zwH')$$

$$= (xHzH, yH'wH'')$$

$$= (xH, yH') * (zH, wH'')$$

$$= f(x, y) * f(z, w)$$

$\Rightarrow f$ is a homomorphism and also f is onto. Then by first isomorphism theorem,

$G \times G' / \ker f \cong G/H \times G/H'$

Now we have only to show that $\ker f = H \times H'$

So, $\ker f = \{(x, y) \in G \times G' \mid f(x, y) = (H, H')\}$

$$= \{(x, y) \in G \times G' \mid (xH, yH') = (H, H')\}$$

$$= \{(x, y) \in G \times G' \mid xH = H \text{ and } yH' = H'\}$$

$$= \{(x, y) \in G \times G' \mid x \in H \text{ and } y \in H'\}$$

$$= H \times H'$$

Hence the theorem proof.

5.4 *INTERNAL DIRECT PRODUCT*

The external direct products of groups, which give us a way to think of a family of different groups as subgroups of a bigger group, were introduced and described in the preceding section. Consider two groups G_1 and G_2 with identical elements e_1 and e_2, respectively, to be more precise. Then two normal subgroups of $G_1 \times G_2$ are $N_1 = G_1 \times \{e_2\} \cong G_1$ and $N_2 = \{e_1\} \times G_2 \cong G_2$. In this section we will consider the reverse problem i.e., in a given group whether there is family of subgroups $H_1, H_2, ..., H_k$ of G such that,

$G \cong H_1 \times H_2 \times ... \times H_k$

As we may anticipate, not all groups can achieve it. Even if a group G can exist, certain requirements must be met by any subgroups whose exterior direct product is isomorphic to G. The result below gives us an idea of the requirements that the subgroups must meet. Going forward, we will no longer use $*$ to denote the group operation of the direct product, but rather just multiplicative notation.

Theorem 8: Let the family of groups are $G_1, G_2, ..., G_n$. If $G = G_1 \times G_2 \times ... \times G_n$ and $H_i = \{(e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) \mid a_i \in G_i\}$ for each $i = 1, 2, ..., n$. Then

1. H_i is a normal in G and $H_i \cong G \quad \forall i = 1 \text{ to } n$

2. Every element of G can be expresses uniquely as $h_1h_2...h_n$ where $h_i \in H_i$ for each $i = 1, 2, ..., n$.

Proof 1: Since we know that $H_i \neq \phi$ because $(e_1, e_2, ..., e_n) \in H_i$

Let us consider $a = (e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n), b = (e_1, e_2, ..., e_{i-1}, b_i, e_{i+1}, ..., e_n) \in H_i$. Then

$$ab^{-1} = (e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)(e_1, e_2, ..., e_{i-1}, b_i, e_{i+1}, ..., e_n)^{-1}$$

$$= (e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)(e_1, e_2, ..., e_{i-1}, b_i^{-1}, e_{i+1}, ..., e_n)$$

$$= (e_1, e_2, ..., e_{i-1}, a_i b_i^{-1}, e_{i+1}, ..., e_n) \in H_i$$

So, by the necessary and sufficient condition for being subgroup of any group H_i is subgroup of G.

Now for each $g = (g_1, g_2, ..., g_n) \in G$,

$gag^{-1} = (e_1, ,..., e_{i-1}, g_i a g_i^{-1}, e_{i+1}, ..., e_n) \in H_i$

Hence H_i is normal in G.

2: Let any element $a = (a_1, a_2, ..., a_n) \in G$ where $a_i \in G_i$ so $h_i = (e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) \in H_i$ for each $i = 1, 2, ..., n$ are s.t., $a = h_1h_2, ..., h_n$

Now we will prove the uniqueness property. For it suppose $a = k_1k_2, ..., k_n$ where $k_i \in H_i$

$\Rightarrow k_i = (e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)$ for some $b_i \in G_i$. Then

$(a_1, a_2, ..., a_n) = a = k_1k_2...k_n = (b_1, b_2, ..., b_n)$

$\Rightarrow a_i = b_i$ and hence $h_i = k_i \; \forall \, i = 1, 2, ..., n$

Since each element in G is of the form $h_1h_2, ..., h_n$ where $h_i \in H_i \;\; \forall \; i = 1 to n$, it follows that $G = H_1H_2...H_n$. Also $G_i \cong H_i \;\; \forall \; i = 1, 2, ..., n$

$\Rightarrow G \cong H_1 \times H_2 \times ... \times H_n$

Definition: Let $N_i, i = 1 \; to \; k$ are the normal subgroup of a group G. If each element of G is uniquely expressed as $a = a_1a_2...a_k$ where $a_i \in N_i \; \forall \, i = 1, 2, ..., n$ then G is called internal direct product of $N_i, i = 1 \; to \; k$.

The word "internal" emphasises the fact that all of the components of the group N_i must be subgroups of the same group G and that the product $a = a_1a_2...a_k$ formed by the members of the group $N_1, N_2, ..., N_k$ is truly a product of the group G.

Example 3: For the Klein's 4-group $K_4 = \{e, a, b, c\}$, $H_1 = \{e, a\}$ and $H_2 = \{e, b\}$ are normal subgroup of K_4 – group. Now, $H_1H_2 = \{e, a\}\{e, b\} = \{e, a, b, c\} = K_4$

$\Rightarrow$ Each element of K_4 – group is expressed as product of an element of normal subgroup H_1 and an element of H_2.

Now, we have only to prove the uniqueness property, for it assume $x_1, x_2 \in H_1$ and $y_1, y_2 \in H_2$ such that $x_1 y_1 = x_2 y_2$. Then $x_2^{-1} x_1 = y_2 y_1^{-1} \in N_1 \cap N_2 = \{e\}$

$\Rightarrow x_2^{-1} x_1 = e = y_2 y_1^{-1}$

$\Rightarrow x_1 = x_2$ and $y_1 = y_2$.

Hence, K_4 – group is internal direct product of normal's H_1 and H_2.

Example 4: As we know for every nonzero complex number z has unique representation $z = re^{i\theta}$ where $r = |z|$ and $\theta = ampz$. Then group of positive real numbers ($r \in R^+$) and $e^{i\theta} \in S^1 = \{u \in C^* \,||\, u| = 1\}$. Hence C^* is internal direct product of R^+ and S^1.

Example 5: Set of integer (Z) cannot be represented as internal direct product of two subgroup of Z. It is to note that for distinct non zero integer m and n, $mn \in mZ \cap nZ \Rightarrow mZ \cap nZ \neq \{0\}$.

A group must meet the following requirements in order to be an internal direct product of a certain family of normal subgroups. This lemma is required in order to demonstrate this result.

Lemma 1: Let $H_1, H_2, ..., H_k$ are normal subgroup of G. If $H_i \cap (H_1 H_2 ..., H_{i-1} H_{i+1} ... H_k) = \{e\} \forall\, i = 1,2,...,k$ then $x_i x_j = x_j x_i \;\forall\; x_i \in H_i, x_j \in H_j, i \neq j$.

Proof: Let us consider $x_i \in H_i$ and $x_j \in H_j$. Then $x_i x_j x_i^{-1} x_j^{-1} \in (x_i H_j x_i^{-1}) H_j \subseteq H_j$, since H_j is normal in G. Similarly, $x_i x_j x_i^{-1} x_j^{-1} \in H_i$.

Hence $x_i x_j x_i^{-1} x_j^{-1} \in H_i \cap H_j \subseteq H_i \cap (H_1 H_2 ..., H_{i-1} H_{i+1} ... H_k) = \{e\}$

And so $x_i x_j = x_j x_i$.

Theorem 9: Let $H_1, H_2, ..., H_k$ are normal subgroup of G. Then G is the internal direct product of $H_1, H_2, ..., H_k$ iff

(i) $G = H_1 H_2 ... H_k$ and

(ii) $H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$ for each $i = 1,2,...,k$

Proof: Let we assume that G internal direct product of normals $H_1, H_2, ..., H_k$ of G. Then $\forall\, a \in G, \exists$ unique $x_i \in H_i$ s.t., $a = x_1 x_2 ... x_k$ and so $a \in H_1 H_2 ... H_k$. Hence $G \subseteq H_1 H_2 ... H_k$. Also $H_1 H_2 ... H_k \subseteq G$, since every H_i is subgroup of G. Thus $G = H_1 H_2 ... H_k$. Now consider

$a \in H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k)$. Then $a \in N_i$ and $a = x_1 x_2 ... x_{i-1} x_{i+1} ... x_k$ for some $x_j \in N_j$, $j = 1,..., i-1, i+1,..., k$

$\Rightarrow e...eae...e = a = a_1 ... a_{i-1} e a_{i+1} ... a_k$.

Since each such representation is unique, it follows that $a = e$. Thus $H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$ for each $i = 1,2,...,k$.

Conversely, assume the given condition satisfies by the family of normal subgroup $H_1, H_2, ..., H_k$. Then ,

$G = H_1, H_2, ..., H_k \Rightarrow \forall\, x \in G$ can be represented as $x = x_1 x_2 ... x_k$ where $x_i \in H_i$.

Now we have to prove that such representation is unique. For it, let us suppose that another representation is $x = y_1 y_2 ... y_k$ where $y_i \in H_i$. Then by lemma 1, $x_1 x_2 ... x_k = y_1 y_2 ... y_k$ implies that

$$x_i y_i^{-1} = (y_1 x_1^{-1})(y_2 x_2^{-1}) ... (y_{i-1} x_{i-1}^{-1})(y_{i+1} x_{i+1}^{-1}) ... (y_k x_k^{-1})$$

$$\in H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$$

Thus, $x_k = y_k \; \forall\, i = 1, 2, ..., k$

$\Rightarrow$representation is unique for every $x \in G$.

Corollary: Let N_1 and N_2 are normal subgroup of G. Then G is internal direct product of N_1 and N_2 if and only if $G = N_1 N_2$ and $N_1 \cap N_2 = \{e\}$.

By the definition of internal direct product we can stated it as: If $G = N_1 \times N_2$ then G is internal direct product of the normals $G \cong N_1$ and $G \cong N_2$.

Conversly, up to isomorphism, every internal direct product can also be realised as an external direct product.

Theorem 10: If G is the internal direct product of the normal subgroups $H_1, H_2, ..., H_k$, then $G \cong H_1 \times H_2 \times ... \times H_k$.

Proof: First we define, $f : G \to H_1 \times H_2 \times ... \times H_k$ by,

$f(x_1 x_2 ... x_k) = (x_1 x_2 ... x_k) \;\forall\; (x_1, x_2, ..., x_k) \in G$

By the previous theorem we know that every element in G has the unique representation $x_1 x_2 ... x_k$ for $x_i \in G$, so f is well defined and also one-one and on-to both.

Now for each $x = x_1 x_2 ... x_k, y = y_1 y_2 ... y_k \in G$,

$$f(xy) = f(x_1 x_2 ... x_k y_1 y_2 ... y_k)$$

$$= f(x_1 y_1 x_2 y_2 ... x_k y_k) \qquad \text{[By Lemma 1]}$$

$= f(x_1y_1, x_2y_2, ..., x_ky_k)$

$= (x_1, x_2, ..., x_k), (y_1, y_2, ..., y_k)$

$= f(x) f(y)$

$\Rightarrow f$ is an isomorphism.

5.5 *CAUCHY'S THEOREM*

Theorem 11: Let p is a prime and G is a finite group s.t. $p \mid O(G)$, then $\exists x \in G$ s.t., $O(x) = p$.

Proof: First we prove the result for finite abelian group G by the induction on $n = O(G)$. Since result is true for $n = 1$. Assume that it is true for all group having order less than $O(G)$. If Group has non-trivial subgroup then G is cycilc group of prime order.

Since $p \mid O(G), O(G) = p, G = < x >$ s.t. $O(x) = O(G) = p$. So result follows.

Let now H be a non-trivial subgroup of G i.e., $H \neq \{e\}$, G. Since G is abelian, H is normal in G. If $p \mid O(H)$, then, by induction hypothesis as $O(H) < O(G), H$ is abelian, $\exists x \in H$ s.t. $O(x) = p, x \in H \Rightarrow x \in G$. So, result is again true.

Let p is not divisor of $O(H)$.

Since $O(G) = O(G/H).\ O(H)$ and $p \mid O(G)$, we find $p \mid O\left(\frac{G}{H}\right).O(H)$

But p is not divisor of $O(H)$, hence $p \mid O(G/H)$. Also $O\left(\frac{G}{H}\right) < O(G)$ as $H \neq \{e\}$ and G is abelian means $\frac{G}{H}$ is abelian.

So, by induction hypothesis $\frac{G}{H}$ has an element Hy of order p.

$(Hy)^p = H$

$\Rightarrow Hy^p = H$

$\Rightarrow y^p \in H$

$\Rightarrow (y^p)^t = e$ where $t = O(H)$

$\Rightarrow (y^t)^p = e$

$\Rightarrow O(y^t) \mid p$

$\Rightarrow O(y^t) = 1$ or p

If $y^t = e$ (i.e. $(O(y^t) = 1)$ then $Hy^t = He = H$

$\Rightarrow (Hy)^t = H$

$\Rightarrow O(Hy) \mid t$

$\Rightarrow p \mid t = O(H)$, which is a contradiction

$\therefore O(y^t) = p, y^t \in G$

Hence for this case result is true.

By induction, result is true for all abelian groups.

Let now G be a any group. We again use induction on $O(G)$. The result is vacuously true for $O(G) = 1$. Assume result is true for all groups with order less then $O(G)$. If $T < G$ and $p \mid O(T)$ then by induction hypothesis $\exists x \in T$ s.t. $O(x) = p$. So, result is true in this case. Assume p is not divisor of $O(T)$ for all $T < G$. Consider the class equation of G

$$O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$

Now $a \notin Z(G) \Rightarrow N(a) < G$

$\Rightarrow p$ is not divisor of $O(N(a))$

$\Rightarrow p \mid \frac{O(G)}{O(N(a))}$ [as $O(G) = \frac{O(G)}{O(N(a))}.O(N(a))$]

$$\Rightarrow p \left| \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))} \right.$$

Since $p \mid O(G)$, we have $p \mid O(G) - \left| \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))} = O(Z(G)) \right.$

But p is not divisor of $O(T) \forall T < G$

And $Z(G) = G \Rightarrow G$ is abelian.

But result is true for abelian groups. Hence, by induction, result is true for all groups.

Example 6: Prove that an abelian group of order pq (where p, q are distinct primes) is cyclic.

Solution: Using the Cauchy's theorem, $\exists a, b \in G$ s.t., $O(a) = p, O(b) = q$. Also as $\gcd(p, q) = 1, ab = ba$

$O(ab) = O(a).O(b) = pq$

i.e., ab is an element of G having order equal to $O(G)$. Hence by theorems G is cyclic groups.

For e.g., abelian group of order 6, 10, 15 are all cyclic

Example 7: Any group (G) of order $2n$, where n is odd integer (>1), is not simple.

Solution: Let a be any element of the group G. Define,

$f_a : G \to G$ s.t.,

$f_a(x) = ax$

Then f_a is $1-1$ onto map, i.e., a permutation

Let $G' =$ Collection of such permutations then G' forms a group and $G \cong G'$.

Since $2 | O(G)$, then by Cauchy's theorem there exist an element $g \in G$, s.t., $O(g) = 2$ and $f_g \in G'$.

As we know every permutation can be written as product of disjoint cycles either 1-cycle or 2-cycle as $O(g) = 2$ i.e., $g^2 = e$

Notice $f_g{}^2(x) = f_g(fg(x)) = g^2 x = x = I(x)$

$\therefore f_g{}^2 = I$

For permutation of 3-cycle $(abc), (abc)^2 \neq I$.

Since, permutation f_g in the cycle form cannot have any 1-cycle also, as suppose (x) is a 1-cycle then $x \to x$

i.e., $f_g(x) = x \Rightarrow gx = x \Rightarrow g = e$

not true as $O(g) = 2$.

Hence f_g as permutation can be expressed as product of 2-cycles only. Since $O(G) = 2n$ there can be n two cycles.

So f_g can be expressed as product of n (odd) number of transposition or that f_g is an odd permutation.

Thus in the even permutation G' has $n/2$ elements. $f_g \in G'$, f_g is odd, so G' contains both even and odd permutations.

If H contains only even permutations then,

$$O(H) = \frac{O(G')}{2} \Rightarrow \frac{O(G')}{O(H)} = 2$$

$\Rightarrow H$ is of index 2 in G' and is, therefore, normal.

Since $G' \cong G$ and G' has a normal subgroup, G will have a normal subgroup or that G is not simple.

For e.g., any group having order 30 is not simple as $O(G) = 30 = 2.15$.

Check your progress

Problem 1: Check that the group having order 34 is simple or not?

Problem 2: Check that the abelian group having order 34 is cyclic or not?

Problem 3: Which of the following external direct product of groups are cyclic and why?

(*i*) $Z_4 \times Z_6$ (*ii*) $Z_2 \times Z_3$

5.6 *SUMMARY*

In this unit, we have studied about the external direct products, internal direct products and Cauchy's theorem for finite abelian group and also there related theorems and examples. After completions of this unit learners are able to memorise the following things:

- External direct product of groups is also a group and this direct product does not affected by the operations of each individual groups.
- External direct product of infinite cyclic groups is not cyclic group and also external direct product of finite cyclic groups may or may not be cyclic.
- Any group of order $2n$, where n is odd integer (>1), is not simple

5.7 *GLOSSARY*

- $G_1 \times G_2 \times G_3 \times ... \times G_n$ denotes the external direct product of the groups $G_1, G_2, G_3, ..., G_n$
- If $H_1, H_2, ..., H_k$ are normal subgroup of G. Then G is the internal direct product of $H_1, H_2, ..., H_k$ iff $G = H_1 H_2 ... H_k$ and $H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$ for each $i = 1,2,...,k$

5.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=ZLCHeZEhCZ8yCri36nSF3A==
- https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=ZLCHeZEhCZ8yCri36nSF3A==

5.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

5.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. If G_1 and G_2 are two finite groups. Then prove that for each element $a \in G_1$ and $b \in G_2$, the order of the element (a,b) in the group $G_1 \times G_2$ is $lcm(O(a), O(b))$.

2. If G_1 and G_2 are two groups. Then $G_1 \times G_2 / G_1 \times \{e_2\} \cong G_2$ and $G_1 \times G_2 / \{e_1\} \times G_2 \cong G_1$

3. If G_1 and G_2 are two groups and H_1, H_2 are two normals of G_1, G_2 respectively then prove that $H_1 \times H_2$ is normal in $G_1 \times G_2$ and $G_1 \times G_2 / H_1 \times H_2 \cong G_1 / H_1 \times G_2 / H_2$ and $G_1 \times G_2 / \{e_1\} \times G_2 \cong G_1$

4. Let $H_1, H_2, ..., H_k$ are normal subgroup of G. Then prove that G is the internal direct product of $H_1, H_2, ..., H_k$ iff

(*i*) $G = H_1 H_2 ... H_k$ and

(*ii*) $H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$ for each $i = 1,2,...,k$

5. If $G_1, G_2, ..., G_n$ are the family of groups s.t., $G = G_1 \times G_2 \times ... \times G_n$ and $H_i = \{(e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) \mid a_i \in G_i\}$ for each $i = 1, 2, ..., n$. Then prove that

(*i*) H_i is a normal in G and $H_i \cong G \ \forall i = 1 \ to \ n$

(*ii*) Every element of G can be expresses uniquely as $h_1 h_2 ... h_n$ where $h_i \in H_i$ for each $i = 1, 2, ..., n$.

6. Prove that if any group G is internal direct product of normal subgroups $H_1, H_2, H_3, ..., H_k$ then, $G \cong H_1 \times H_2 \times H_3 \times ... \times H_k$

7. If any prime p divides the order of any group G then $\exists x \in G$ s.t., $O(x) = p$.

8. Prove that for any group (G) having order $2n$, where n is odd integer (>1), is not simple.

9. Prove that $Z_m \times Z_n \cong Z_{mn}$ if and only if $\gcd(m,n) = 1$

Short Answer Type Question:

10. Prove that $S_3 \times Z$ non-commutative and non-cyclic infinite group.

11. Prove that the external direct product of two cyclic groups Z_4 and Z_6 is not cyclic.

12. Prove that the external direct product $G_1 \times G_2$ of two groups G_1 and G_2 is abelian if and only if G_1 and G_2 both are abelian.

13. Prove that external direct product of two infinite cyclic group is not cyclic.

14. If H and K are two normal subgroup of G. Then G is internal direct product of H and K if and only if $G = HK$ and $H \cap K = \{e\}$.

Fill in the blanks:

15. $Z_2 \times Z_3$ is isomorphic to …….

16. Group of order 74 is ……. group.

17. Any abelian group of order 35 is …….

18. The external direct product of N (set of natural numbers) and Z (set of integers) is……

19. $Z_m \times Z_n \cong Z_{mn}$ iff $\gcd(m,n) = \ldots\ldots\ldots$

5.11 *ANSWERS*

Answer of self cheque question:

1. No **2.** **Yes** **3.** $Z_2 \times Z_3$ is cyclic because gcd(2,3) = 1.

Answer of terminal question:

15. Z_6 **16.** Simple **17.** Cyclic

18. not a group **19.** 1

Unit-6: SYLOW SUBGROUPS, SYLOW'S THEOREM AND THEIR APPLICATIONS

CONTENT:

6.1 *INTRODUCTION*

Norwegian mathematician Peter Ludwig Mejdell Sylow (12 December 1832 – 7 September 1918) established key ideas in group theory.

He was born and passed away in Christiania, which is now Oslo. Sylow was the brother of Carl Sylow, a military commander and sports figure, and the son of government minister Thomas Edvard von Westen Sylow. He attended Christiania Cathedral School in 1850 and Christiania University in 1856. Sylow taught in the high school at Hartvig Nissen School before going on to lead Halden as its headmaster from 1858 to 1898.

Peter Ludwig Mejdell Sylow

12 December 1832 –7 September 1918

https://en.wikipedia.org/wiki/Peter_Ludwig_Mejdell_Sylow#:~:text=Sylow%20was%20a%20high%20school,his%20theorems%20regarding%20Sylow%20subgroups

In 1862, he taught Galois theory as a guest lecturer at Christiania University. He then raised the query that resulted in his theorems concerning Sylow subgroups. After publishing the Sylow theorems in 1872, Sylow spent the next eight years of his life working with Sophus Lie to edit his countryman's mathematical writings, Niels Henrik Abel. He was appointed as a professor at the University of Christiania in 1898.

He received the Kronprinsens gullmedalje (Crown Prince's Gold Medal) from the University of Oslo in 1853. He was chosen for admission to the Norwegian Academy of Science and Letters in 1868. He received an honorary degree from the University of Copenhagen in 1894, and he afterwards joined Acta Mathematica as an editor.

Three conclusions on the structure of finite groups were proven by the French mathematician M. L. Sylow, and they are used to describe simple groups. It's noteworthy to note that M. L. Sylow was able to demonstrate same conclusions for permutation groups. George Frobenious was inspired by the Cayley's Theorem to demonstrate the Sylow Theorems in a broader context. Here, we demonstrate the Sylow Theorems using group action methods. To do this, we must first demonstrate the following two findings on group behaviour.

We will talk about Sylow's three theorems, *p*-groups, and their applications in this unit. The concepts created are so valuable that much about a group's nature may be understood just by knowing its arrangement.

6.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the Sylow’s group which is the extension of Lagrange’s theorem.
- Implementation of Sylow’s theorems to find the number of subgroups of the group on the basis of order of the group.

- Analyze the theorems related to Sylow's theorem and Sylow groups.

6.3 *p-Group*

Definition: Any group is called *p*-group if its each element has order p^r where $p =$ prime. Here it should be remember that *p* will be same for all element of group and only *r* may different for different elements.

e.g., In the $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ group and the Quaternian group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, each elements are of order 2^r. So, these groups are called 2-group.

Here we will learn about mainly about the finite groups.

Theorem 1: Any finite group G is *p*-group *iff* $O(G) = p^n$.

Proof: Let we assume that G is *p*-group then there exist prime q s.t., $q \mid O(G)$. Then by Cauchy's theorem there exist an element $a \in G$ s.t., $O(a) = q$. But according to definition of *p*-group $O(a) = p^r$.

$\Rightarrow q = p^r$

$\Rightarrow q = p$ i.e., p is the only element s.t., $p \mid O(G)$. Thus $O(G) = p^n$

Conversely, let we consider $O(G) = p^n$ and any element $a \in G$. Then by Lagrange's theorem $O(x) \mid O(G) = p^n \Rightarrow O(x) = p^r$

Hence, order of each element of group is of the form p^r. So, G is *p*-group.

Note (*i*): Each *p*-group has non-trivial centre because each group of order p^n, $O(Z(G)) > 1$.

(*ii*): Any *p*-group may or may not be abelian. For *e.g.*, K_4 is abelian and Q_8 is not abelian while both are 2-group.

Example 1: Let H, K are two subgroup of finite group G then either $H \subseteq K$ or $K \subseteq H$. Then prove that G is *p*-group.

Solution: If G is a cyclic group of prime order and G has no proper subgroup, thus result is true.

Let us suppose that $H(\neq G)$ is a proper subgroup of G.

First we will prove that G will be cyclic.

Since $H \underset{\neq}{\subset} G, \exists\, x \in G,$ s.t., $x \notin H$.

Let $K =< x >,$ then $K \not\subset H$ as $x \in K, x \notin H$

So, according to given condition, $H \subseteq K$

If $K = G$ then G is cyclic (as K is cyclic)

Suppose $K \neq G$ then $\exists\, y \in G$ s.t., $\exists\, y \notin K$

Let $L =< y >$ then $L \not\subseteq K$ and by given condition $K \subseteq L$

If $L = G$, G will be cyclic, $L \neq G$ proceed as above and as G is finite, after a finite steps, we find that G is cyclic.

To prove that G is p-group, suppose two distinct primes p, q s.t., $p, q \mid O(G)$. Since G is cyclic, $\exists$ subgroup H and K of G with $O(H) = p, O(K) = q$ (For the cyclic group convers of Lagrange's theorem holds)

Now, $H \not\subseteq K$ as $O(H) \nmid O(K)$

$K \not\subseteq H$ as $O(K) \nmid O(H)$

Wherever there is a conflict with the claimed statement.

Hence only one prime dividing $O(G)$ or that G is a p-group.

Converse of this example also holds.

Example 2: If H and K are two subgroup of a finite cyclic p- group G then either $K \subseteq H$ or $H \subseteq K$.

Proof: Let $G =< x >$ is cyclic group and x is its generator, then $O(G) = O(x) = p^n$ where $p =$ prime.

Let $H =< x^m >$

Let $d = \gcd(m, p^n)$

Then $x^d = x^{ma+p^n b} = x^{ma}.x^{p^n b} = (x^m)^a \in H$ [as $O(x) = p^n$]

Thus, $< x^d > \subseteq H$

Again as $d \mid m$, $m = dq$

So, $x^m = (x^d)^q \in < x^d >$

Or that $H =< x^m > \subseteq < x^d >$

And hence $H =< x^d >$ where $d \mid p^n$

And so $H =< x^{p^i} >$

Let K is another subgroup of G, then $K =< x^{p^k} >$. Suppose $i \geq k$ and let $i = k + t$ where $t \geq 0$ is an integer.

Now $x^{p^i} = x^{p^{k+t}} = \left(x^{p^k}\right)^{p^t} \in K$

$\Rightarrow H = \left\langle x^{p^i} \right\rangle \subseteq K$

If $k \geq i$, then $K \subseteq H$

Hence prove the result.

Example 3: Prove that each proper subgroup is proper subgroup of its normalizer in finite p-group G.

OR

If $O(G) = p^n, H \leq G, H \neq G,$ then $\exists g \in G, g \notin H,$ s.t. $gHg^{-1} = H$

Solution: We will prove result by induction method on n. Let $n = 1$. Then $O(G) = p$. Since $H \neq G$, $O(H) = 1$.

$\therefore H = \{e\}$ or $gHg^{-1} = g\{e\}g^{-1} = \{e\} = H \; \forall e \neq g \in G.$

$g \neq e \Rightarrow g \notin H$

Thus it is true for $n = 1$. Let it is true for all groups which have order less than p^n. Let $O(G) = p^n$. Suppose $H = N(H)$.

Since $Z(G) \subseteq N(H) = H, H \neq G$

$\frac{H}{Z(G)}$ is a proper subgroup of $\frac{G}{Z(G)}$

Now, $O\left(\frac{G}{Z(G)}\right) = p^m, m < n$

For convenience, we write $Z(G) = N$, then by induction hypothesis, $\exists Ng \in \frac{G}{N}$, $Ng \notin \frac{H}{N}$, s.t.

$Ng\frac{H}{N}(Ng)^{-1} = \frac{H}{N}$

$\Rightarrow NgNhNg^{-1} \in \frac{H}{N} \; \forall h \in H$

$\Rightarrow Nghg^{-1} = Nh_1$ for some $h_1 \in H$

$\Rightarrow ghg^{-1}h_1^{-1} \in N = Z(G) \subseteq H$

$\Rightarrow ghg^{-1} \in H \; \forall h \in H$

$\Rightarrow gHg^{-1} \subseteq H$

$\Rightarrow gHg^{-1} = H$ as $\Rightarrow O(gHg^{-1}) = O(H)$

Thus $g \in N(H)$ and as $Ng \notin \frac{H}{N}, g \notin H$, or that $N(H) \neq H$, a contradiction. Hence $H \subset N(H)$

Thus result is true for n also.

By induction, result is true for all $n \geq 1$.

Example 4: Let for a prime (p) $O(G) = p^n$. If $H \leq G$ s.t. $O(H) = p^{n-1}$, then show that H is normal subgroup in G.

Solution: $H \subseteq N(H) \subseteq G$

Since $O(H) = p^{n-1} \mid N(H) \mid O(G) = p^n$

$O(N(H)) = p^{n-1}$ or p^n

If $O(N(H)) = p^n = o(G)$

Then $N(H) = G$

And so H is normal in G.

If $O(N(H)) = p^{n-1}$

Then $N(H) = H$

Since $Z(G) \subseteq N(H) = H$

$O\left(\frac{H}{Z(G)}\right) = p^{n-1-m}$, where $O(Z(G)) = p^m, m > 0$

and $O\left(\frac{G}{Z(G)}\right) = p^{n-m}$,

Now we will prove result by induction method on n. When $n = 1, H = \{e\}$ and so H is normal in G. Assume result to be true for all $p-$groups with order less then $O(G)$. Here $\frac{G}{Z(G)}$ is a $p-$group s.t., $O\left(\frac{G}{Z(G)}\right) = p^{n-m}, n-m < n$ (as $m > 0$) and $O\left(\frac{H}{Z(G)}\right) = p^{n-m-1}$. By induction hypothesis, $\frac{H}{Z(G)}$ is normal $\frac{G}{Z(G)} \Rightarrow H$ is normal in G. So $N(H) = G \Rightarrow H = G$, a contradiction. Thus, $O(N(H)) \neq p^{n-1}$.

So result is true for n also. Hence, result is true for all $n > 0$

Lemma 1: Let G be a group of order p^n, p be a prime and S be a finite G-set. If $S_0 = \{a \in S \mid ga = a \forall g \in G\}$, then $|S| \equiv |S_0| \pmod{p}$

Proof: Let $a \in S$. Then $a \in S_0$ if and only if the orbit $[a] = \{a\}$, equivalently $|[a]| = 1$. Hence S can be written as a disjoint union $S = S_0 \cup [a_1] \cup [a_2] \cup ... \cup [a_k]$ where $[a_1], [a_2], ..., [a_k]$ are distinct orbits of G on S and disjoint with S_0. Then $|S| = |S_0| + |[a_1]| + |[a_2]| + ... + |[a_k]|$. Since $a_i \notin S_0$, so there is $g \in G$ such that $ga_i \neq a_i \Rightarrow g \notin G_{a_i}$ and so $|G_{a_i}| < |G|$. Thus $|[a_i]| > \frac{|G|}{|G_{a_i}|} > 1$.

Then $|[a_i]| > 1$ and $|[a_i]| = [G : G_{a_i}] \mid |G| = p^n \Rightarrow p \mid |[a_i]| \forall 1 \leq i \leq k$. Hence $p \mid \sum_{i=1}^{k} |[a_i]|$ and it follows that $|S| \equiv |S_0| \pmod{p}$.

Recall that if every element of a group G has order $p^n; n \geq 0$ for some fixed prime p, then G

is called a p - group. With the help of Cauchy's Theorem we have proved that a finite group G is a p - group if and only if $|G| = p^n$ for some $n \geq 0$.

We call a subgroup H of a group G a p -subgroup if H is a p -group. In particular, for every prime p, $\{e\}$ is a p -subgroup of every group G, since $|\{e\}| = 1 = p^0$.

Lemma 2: If H is a p -subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] (\text{mod } p)$.

Proof: Let S be the set of all left cosets of H in G. Then $H \times S \to S$ given by $(g, aH) \to (ga)H$ is an action of H on S. Since H is a p -group, $|S| \equiv |S_0| (\text{mod } p)$.

Here $|S| \equiv [G : H]$. Now for $a \in G$,

$aH \in S_0 \Leftrightarrow gaH \; \forall \; g \in G$

$\Leftrightarrow a^{-1}ga \in H \; \forall \; g \in G$

$\Leftrightarrow a^{-1}Ha \subseteq H$

$\Leftrightarrow a \in N_G(H)$

shows that S_0 is the set of all left cosets aH such that that $a \in N_G(H)$, that is $|S_0| = [N_G(H) : H$.

Hence $[G : H] = [N_G(H) : H] (\text{mod } p)$.

Corollary 1: Let p be a prime and H be a p -subgroup of a finite group G. If $p | [G : H]$, then $N_G(H) \neq H$.

Proof: Since G is a finite group and H is a p -subgroup of G, so

$[G : H] \equiv [N_G(H) : H] (\text{mod } p)$

Then $p | [G : H] \Rightarrow p | [N_G(H) : H]$. Since $[N_G(H) : H] \neq 0$ it follows that $[N_G(H) : H] \geq p$ and the result follows.

6.4 *SYLOW'S THEOREMS*

Now we will discuss about the three main fundamental theorem of Sylow's named as Sylow's theorem and also their implementation in various examples.

6.4.1 *SYLOW'S FIRST THEOREM*

Theorem 2: (**Sylow's First Theorem**) Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(p, m) = 1$. Then G has a subgroup of order $p^i \; \forall 1 \leq i \leq n$. Moreover, for every subgroup of order $p^i \; \forall \, i < n$, there is a subgroup K of order p^{i+1} such that H is normal in K.

Proof: We prove that G has a subgroup H of order $p^i \ \forall 1 \le i \le n$ by induction on i. Since $n > 0, p \mid |G|$ and it follows from the Cauchy's Theorem that G has a subgroup H of order p.

Assume that H is a subgroup of order $p^i, 1 \le i \le n$. Since H is a subgroup of order p^i, so $[G:H] \equiv [N(H):H] (\text{mod } p)$. Then $p \mid [G:H] \Rightarrow p \mid [N(H):H] = |N(H)/H|$, and it follows from the Cauchy's Theorem that the quotient group $N(H)/H$ has a subgroup K/H of order p. Thus G has a subgroup K such that $|K| = |K/H|.|H| = p^{i+1}$. Hence, by the principle of mathematical induction, G has a subgroup of order p^i for every $1 \le i \le n$. Finally, $K \subseteq N(H)$ shows that H is normal in K.

As an immediate consequence we have following extension of Cauchy's Theorem:

Corollary: Let G be a finite group and p be a prime. If $p^n \big| |G|$, then G has a subgroup H of order p^n. The second part of the Sylow's first theorem motivates us to introduce the notion of maximal p-subgroups.

Definition: Let p be a prime, then a subgroup P of G is called a Sylow p-subgroup if it is a maximal p-subgroup of G, that is, if H is a p-subgroup of G and $P \subseteq H \subseteq G$ then $P = H$. If G is a finite group then G can have only finitely many subgroups and a maximal p-subgroup.

If G is infinite then, also G has a maximal p-subgroup, by the Zorn's Lemma. Thus, for every prime p every group G has a Sylow p-subgroup, though they may be trivial.

We have following equivalent characterization of Sylow p-subgroups.

Theorem 3: Let G be a finite group of order $p^n m, n > 0$ and $\gcd(p, m) = 1$. Then a subgroup H is a Sylow p-subgroup of G if and only if $|H| = p^n$.

Proof: First assume that H is a subgroup of G such that $|H| = p^n$. Let K be a p-subgroup of G such that $H \subseteq K$. Since K is a p-subgroup, so $|K| = p^r$ for some $r \ge 0$. Now by the Lagrange's Theorem, $|K| \big| |G|$ i.e. $p^r \ne p^n m$ and $\gcd(n, m) = 1$ together implies that $r \le n$. Also $H \subseteq K \Rightarrow n \le r$. Thus $r = n$ and $|H| == |K| = p^n$. Hence $H = K$ and H is a maximal $p-$subgroup.

Conversely, suppose that H is a Sylow p-subgroup. Then $|H| = p^r$ for some $r \ge 0$. Now, by the Lagrange's Theorem, $|H| \| G|$, that is $p^r \mid p^n m$ and $\gcd(n, m) = 1 \Rightarrow r \le n$. If $r < n$ then, the Sylow's first theorem H is contained in a subgroup K of order p^{r+1} which contradicts that H is a maximal p-subgroup of G. Thus $r = n$ and $|H| = p^n$

Following result has an important role to characterize the nilpotent groups.

Theorem 4: Let G be a finite group. If every Sylow subgroup of G is normal, then G is a direct product of its Sylow subgroups.

Proof: Let $|G| = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ where p_i are distnict primes. Since each Sylow subgroups of G is normal, so G has unique Sylow p_i-subgroup for every p_i, say P_i. Let $a_i \in P_i$ and $a_j \in P_j$, where $i \neq j$. Since both P_i and P_j are normal, so $a_i a_j a_i^{-1} a_j^{-1} \in P_i \cap P_j$.

Now $\gcd(|P_i|, |P_j|) = 1$

$\Rightarrow$by the Lagrange's Theorem, that $|P_i \cap P_j| = 1$ and so $P_i \cap P_j = \{e\}$. Thus $a_i a_j = a_j a_i$. Now let $a \in P_r \cap (P_1 P_2 ... P_{r-1} P_{r+!} ... P_k)$. Then $a = a_1 a_2 ... a_{r-1} a_{r+!} ... a_k$

where $a_i \in P_i$. Now $O(a_i) \mid |P_i|$, that is $O(a_i) \mid p_i^{n_i}$. Thus $O(a) \mid p_r^{n_r}$ and $a_i a_j = a_j a_i \; \forall \, i \neq j$

$\Rightarrow O(a) \mid p_1^{n_1} ... p_{r-1}^{n_{r-1}} p_{r+1}^{n_{r+1}} ... p_k^{n_k}$. Since $\gcd(p_r^{n_r}, p_1^{n_1} ... p_{r-1}^{n_{r-1}} p_{r+1}^{n_{r+1}} ... p_k^{n_k}) = 1$. So $O(a) = 1$ and $a = e$. Thus $P_r \cap (P_1 P_2 ... P_{r-1} P_{r+!} ... P_k) = \{e\}$

$|P_1 P_2 ... P_{r-1} P_{r+!} ... P_k| = |P_1| \, |P_2| ... |P_{r-1}| \, |P_{r+!}| ... |P_k| = p_1^{n_1} ... p_{r-1}^{n_{r-1}} p_{r+1}^{n_{r+1}} ... p_k^{n_k} = |G|$

Hence $G = P_1 P_2 ... P_{r-1} P_{r+!} ... P_k$ and G is an internal direct product of the Sylow subgroups $P_1, P_2, ..., P_{r-1}, P_{r+!}, ..., P_k$.

Lemma: Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(m, n) = 1$.

(*i*) Every conjugate of a Sylow p-subgroup is also a Sylow p-subgroup.

(*ii*) If G has unique Sylow p-subgroup P, then P is normal in G.

Proof (*i*): Let H be a Sylow p-subgroup of G and K be a conjugate of H. Then $K = aHa^{-1}$ for some $a \in G$ which implies that $|K| = |H| = p^n$. Hence K is a Sylow p-subgroup of G.

(*ii*): Let H be the unique Sylow p-subgroup of G. Then $\forall \, g \in G, gHg^{-1}$, is a Sylow p-subgroup and uniqueness of H implies that $gHg^{-1} = H$. Hence H is a normal subgroup of G.

The converse of this results is also true and can be verified by following theorems.

6.4.2 *SYLOW'S SECOND THEOREM*

Theorem 5: (**Sylow's Second Theorem**) Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(m, n) = 1$. Then any two Sylow p-subgroups of G are conjugate, and also isomorphic.

Proof: Let K and H are two Sylow p-subgroups of G.

Denote $S = \{aH | a \in G\}$ and define an action of K on S by $(k, aH) \to (ka)H$. Since K is a p-group, so it follows that

$|S| \equiv |S_0| \pmod{p}$, where

$S_0 = \{aH \in S \mid (ka)H = aH \; \forall \, k \in K\} = \{aH \in S \mid a^{-1}ka \in H \; \forall \, k \in K\} = \{aH \in S \mid a^{-1}Ka \subseteq H\}.$

Now $|S| = [G : H] = \frac{|G|}{|H|} = m \Rightarrow p \nmid |S|$, since $\gcd(p, m) = 1$ and $p \nmid |S_0|$. Thus $|S_0| > 0$. Let $aH = S_0$.

Then $a^{-1}Ka \subseteq H$. Since $|a^{-1}Ka| = |K| = p^n = |H|$, so $a^{-1}Ka = H$. Hence K and H are conjugate.

We have following useful corollaries.

Corollary: Let K be a finite group and P be a Sylow p-subgroup of G. Then P is normal in G *iff* it is the unique Sylow p-subgroup of G.

Proof: First assume that P is normal. Let Q be a Sylow p-subgroup of G. Then P and Q are conjugate, by the Sylow's second theorem. Hence there is $a \in G$ such that $Q = apa^{-1}$. Since P is normal in G, so $aPa^{-1} = P$. Therefore $Q = P$ and G has unique Sylow p-subgroup.

The converse follows from the Lemma 1.

Corollary: Let G be a finite group. Then for every Sylow p-subgroup P of G

$N(N(P)) = N(P)$

Proof: Let $a \in N(N(P))$ then $aN(P)a^{-1} = N(P)$ and so $aPa^{-1} \subseteq N(P)$.

Now $|P| = |aPa^{-1}| \Rightarrow$ both P and aPa^{-1} are Sylow p-subgroup of G and hence $N(P)$.

Since P is normal in $N(P)$, so P is the unique Sylow p-subgroup of $N(P)$, and it follows that $P = aPa^{-1}$. Thus $a \in N(P)$ and $N(N(P)) \subseteq N(P)$. Therefore $N(N(P)) = N(P)$

The number of Sylow p-subgroups within a group G has been defined via Sylow's third theorem. Assume S is the collection of all Sylow p-subgroups. Every Sylow p-subgroup's conjugate is likewise a Sylow p-subgroup, hence for any subgroup H of G,

$H \times S \to S$, given by

$(a, P) \to aPa^{-1}$, is an action of H on S. Also any two Sylow p-subgroup are conjugate on S, which implies that if G acts on S by conjugation then there is single orbit of G on S.

6.4.3 *SYLOW'S THIRD THEOREM*

Theorem 6: (**Sylow's Third Theorem**) Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(m, p) = 1$.

Then the number of Sylow p-subgroup (n_p) is of the form $1+kp$ for some $k \geq 0$ and is such that $n_p \mid p^n m$.

Proof: Let S be the set of all Sylow p-subgroups of G and P be a Sylow p-subgroup. Consider action of P on S by conjugation, that is

$(p, H) \to pHp^{-1}$

Since P is a p-group, so $|S| \equiv |S_0| (\text{mod } p)$, where $S_0 = \{H \in S \mid pHp^{-1} = H \ \forall p \in P\}$ = $= \{H \in S \mid P \subseteq N(H)\}$. Then $P \in S_0$ and $S_0 \neq \phi$. Let $Q \in S_0$ then $P \subseteq N(Q)$. Since both P, Q are Sylow p- subgroups of G, so they are Sylow p-subgroups of $N(Q)$ and are conjugate in $N(Q)$. Let $a \in N(Q)$ such that $P = aQa^{-1}$. But then $P = Q$, since $aQa^{-1} = Q$. Hence $S_0 = \{P\}$ and it follows that $|S| \equiv 1 (\text{mod } p)$, that is $|S| = 1 + kp$ for some $k \geq 0$.

To prove the second part, consider action of G on S by conjugation. Then there is only one orbit of G on S, and so $S = [p]$ for every Sylow p-subgroup P of G. Thus

$n_p = |S| = |[P]| = [G : G_p]$

and hence $n_p \mid |G|$

Applications of Sylow's theorem for finite group are given below,

Example 5: Let G be a group of order $45 = 3^2.5$. Denote the number of Sylow 3-subgroups of G by n_3. Then $n_3 = 3k+1$ for some $k \geq 0$ and $n_3 \mid 45$. Hence $n_3 = 1$ and G has unique Sylow 3-subgroup H. Thus H is a normal subgroup of G of order $3^2 = 9$.

Example 6: We will prove that each group having order 99 is abelian.

Let G be a group of order $99 = 11.3^2$. Let n_3 be the number of Sylow 3-subgroups of G. Then, $n_3 = 3k+1$ for some integer $k \geq 0$ and $n_3 \mid 99$. It follows that G has unique Sylow 3-subgroup, say H which is normal in G and $|H| = 9$. Similarly G has unique Sylow 11-subgroup, say K which is normal in G and $|K| = 11$. Then $H \cap K = \{e\}$ and $|HK| = |H||K| = 99$ implies that $G = HK$. Thus G is an internal direct product of H and K. Hence $G \cong H \times K$. Since $|H| = 3^2$, so H is abelian and $|K| = 11$ implies that K is abelian. Therefore G is abelian. Also note that $G \cong Z_{99}$ or $Z_3 \oplus Z_{33}$.

Example 7: We will prove that each group having order 15 is cyclic.

Let G be a group of order $15 = 3 \times 5$. Denote the number of Sylow 3-subgroups of G by n_3.

Then $n_3 = 1 + 3k$ for some $k \geq 0$ and $n_3 \mid 15$. Hence $n_3 = 1$ and G has unique Sylow 3-subgroup,

say H. Then H is normal in G. Similarly G has unique Sylow 5-subgroup K and so K is normal in G. Since $\gcd(|H|,|K|)=1$, so $|H\cap K|=1$ and we have

$$|HK|=\frac{|H||K|}{|H\cap K|}=15$$

Thus $G=HK$ and G becomes an internal direct product of K and H. Now $|H|=3$, a prime implies that $H\cong Z_3$. Similarly $K\cong Z_5$. Therefore,

$$G\cong H\times K\cong Z_3\times Z_5\cong Z_{15}$$

Example 8: Prove that each group having order 255 is cyclic.

Let G be a group of order $255=17.5.3$. Let n_{17} be the number of Sylow 17-subgroups. Then $n_{17}=17k+1$ for some integer $k\geq 0$ and $n_{17}\mid 255$ implies that $n_{17}=1$. Thus G has unique Sylow 17-subgroup, say H which is normal in G and $|H|=17$. Then the normalizer of H is $N(H)=G$. Since $\frac{N(H)}{C(H)}$ is isomorphic to a subgroup of $Aut(H)$, so $\left|\frac{N(H)}{C(H)}\right|$ divides $|Aut(H)|=|Aut(Z_{17})|$. Now $Aut(Z_{17})\cong U_{17}$ implies that $\left|\frac{G}{C(H)}\right|$ divides 16. Also $\left|\frac{G}{C(H)}\right||G|=255$. Then $\gcd(16,255)=1$

$\Rightarrow\left|\frac{G}{C(H)}\right|=1$ and $G=C(H)$. Thus every element of H commutes with every element of G, whence $H\subseteq Z(G)$. Then $17\big||Z(G)|$, which also divides 255. Hence $|Z(G)|=17,51,85 or 255$ and so $\frac{G}{ZG)}=15,5,3 or 1$. But every group of order $15,5,3 or 1$ is cyclic; and it follows that G is abelian. Now, by the fundamental theorem for finite abelian groups, $G\cong Z_{17}\oplus Z_5\oplus Z_3\cong Z_{255}$.

Now we characterize all groups of order $2p$, where p is a prime.

Theorem 7: Let p be an odd prime. If G is a group of order $2p$, then $G\cong Z_{2p}$ or $G\cong D_p$.

Proof: Let G be a group of order $2p$. Then Cauchy's Theorem implies that G has an element a of order p and an element b of order 2. Denote $H=<a>$. Then $[G:H]=2$ implies that H is normal in G. So $bab=bab^{-1}\in H$ which implies that $bab=a^i$ for some $0\leq i<p$. Then $a^{i^2}=(a^i)^i=(bab)^i=(bab^{-1})^i=ba^ib$. Also $bab=a^i\Rightarrow\ a=b^{-1}a^ib^{-1}=ba^ib$. Thus $a^{i^2}=a$, that is, $a^{i^2-1}=e$ and so $p\mid i^2-1=(i-1)(i+1)$, since $O(a)=p$. Since p is a prime so $p\mid i-1$ or $p\mid i+1$.

If $p\mid i-1$, then $i<p\Rightarrow i-1=0$ i.e. $i=1$. Then $bab=a;$ and so $ba=ab^{-1}=ab$, forcing $O(ab)=lcm(O(a),O(b))=lcm(2,p)=2p$, since p is an odd prime. Hence $G\cong Z_{2p}$.

If $p \mid i+1$ then $i = pk-1$ for some integer k, and we have $bab = a^i = a^{-1} = a^{p-1}$ that is, $ba = a^{p-1}b^{-1} = a^{p-1}b$. Also we have $H =< a >$ is normal in G such that $\left|\frac{G}{H}\right| = 2$. Since $O(b) = 2 \nmid p = \mid H \mid$, so $b \notin H$ and $bH \neq H$. Thus $G/H =< H, bH >$. Therefore every element of G can be written as $b^m a^n$ and so $G =< a, b >$. Since $O(a) = p, O(b) = 2$ and $ba = a^{p-1}b$, it follows that $G \cong D_p$.

Example 9: Let $O(G) = 30$. Then show that

(*i*) Either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

(*ii*) G has a normal subgroup of order 15.

(*iii*) Both Sylow 3-subgroup and Sylow 5-subgroup are normal in *G*.

Solution: $O(G) = 30 = 2 \times 3 \times 5$

The number of sylow 3-subgroup is $1+3k$ and $(1+3k) \mid 10 \Rightarrow k = 0$ or 3

If $k = 0$, then sylow 3-subgroup is normal.

Let $k \neq 0$, then $k = 3$. This gives 10 Sylow 3-subgroup H_i of order 3 and so we have 20 elements of order 3.

[For $i \neq j$, $O(H_i \cap H_j) \mid O(H_i) = 3 \Rightarrow O(H_i \cap H_j) = 1$ only and so these 20 elements are different. Each H_i has one element e of order 1 and other two of order 3. $a \in H_i \Rightarrow O(a) \mid O(H_i) = 3 \Rightarrow O(a) = 1, 3$].

The number of sylow 5-subgroup is $1+5k'$ and $(1+5k') \mid 6 \Rightarrow k' = 0$ or 1.

If $k' = 0$. Then sylow 5-subgroup is normal.

Let $k' \neq 0$. Then $k' = 1$. This gives 6 Sylow 5 subgroup each of order 5 and we get 24 elements of order 5. But we have already counted 20 elements of order 3. Thus we have more than 44 elements in G, a contradiction. So, either $k = 0$ or $k' = 0$.

i.e., either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

Which proves (*i*).

Let H be a Sylow 3-subgroup of order 3 and K, a Sylow 5-subgroup of oder 5.

By (*i*), either H is normal in G or K is normal in G.

In any case, $HK \leq G, O(HK) = 15$ as $O(H \cap K)$ divides $O(H) = 3$ and $O(K) = 5 \Rightarrow O(H \cap K) = 1$.

Since index of HK in G is 2, HK is normal in G. This proves (*ii*).

Suppose, H is normal in G, K is not normal in G. By (*i*) G has 6 Sylow 5-subgroup and so 24 element of order 5. But $O(HK) = 15 \Rightarrow HK$ is cyclic

$\Rightarrow HK$ has $\phi(15) = 8$ elements of order 15.

Thus G has $24 + 8 = 32$ elements, a contradiction.

$\therefore K$ is normal in G.

If H is not normal in G, they by (*i*), G has 10 sylow 3-subgroup and so 20 elements of order 3. From above HK has 8 elements of order 15 and K has 4 elements of order 5. This gives $20 + 8 + 4 = 32$ elements in G, a contradiction.

$\therefore H$ is normal in G. So both H and K are normal in G.

This proves (*iii*).

Check your progress

Problem 1: Check that $O\left(\frac{G}{Z(G)}\right)$ cannot be 77.

Problem 2: Check that S_4 has Sylow 2-subgroup or not?

Problem 3: Check that groups have following order must contain normal Sylow subgroup?

(***i***) 12 (***ii***) 28 (***iii***) 56

6.5 *SUMMARY*

In this unit, we have studied about the $p-$groups and three fundamental Sylow's theorem (Sylow first, second and third theorem) and also their applications and implementation on various examples. After completions of this unit learners are able to memorise the following things:

- Sylow's theorems are the extension of Lagrange's theorem.
- Using the Sylow's theorem we can find mainly normal subgroups or sugroups in any finite groups.

6.6 *GLOSSARY*

- Any group is called ***p*-group** if its each element has order p^r where $p =$ prime.
- **Sylow's First Theorem:** Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(p, m) = 1$. Then G has a subgroup of order $p^i \; \forall 1 \le i \le n$.
- **Sylow's Second Theorem:** Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(m, n) = 1$. Then any two Sylow p-subgroups of G are conjugate, and also isomorphic.

- **Sylow's Third Theorem:** Let G be a finite group of order $p^n m$, where p is a prime, $n > 0$ and $\gcd(m, p) = 1$. Then the number of Sylow p-subgroup (n_p) is of the form $1 + kp$ for some $k \geq 0$ and is such that $n_p \mid p^n m$.

6.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.
- https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=ZLCHeZEhCZ8yCri36nSF3A==

6.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

6.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. If G be a group of order p^n, p be a prime and S be finite G- set. If $S_0 = \{a \in S \mid ga = a \; \forall \; g \in G\}$, then prove that $|S| \equiv |S_0| \pmod{p}$

2. State and prove the Sylow first theorem.

3. State and prove the Sylow second theorem.

4. State and prove the Sylow third theorem.

5. If G be a finite group and every Sylow subgroup of G is normal then prove that G is direct product of its Sylow subgroup.

6. Prove that for a odd prime p, if G is a group of order $2p$, then $G \cong Z_{2p}$ or $G \cong D_p$.

7. If G be a finite group of order $p^n m, n > 0$ and $\gcd(p, m) = 1$ then prove that H is Sylow $p-$ subgroup of G if and only if $|H| = p^n$.

8. Let G be a finite group then prove that for each Sylow $p-$subgroup P of G $N(N(P)) = N(P)$

9. Let G be a finite group and P be a Sylow $p-$subgroup G. Then P is normal in G if and only if it is the unique Sylow $p-$subgroup of G.

Short Answer Type Question:

10. Prove that group G having order 30 has a normal subgroup of order 15.

11. Prove that the group G having order 255 is cyclic.

12. Prove that the group G having order 33 is cyclic.

13. Prove that group G having order 45 has unique Sylow 3-subgroup.

14. Prove that each proper subgroup is proper subgroup of its normalizer in finite *p*-group.

Fill in the blanks:

15. Any group having each element of order p^r is called …….

16. If every Sylow subgroup of finite group G is normal, then G is a direct product of its ……...

17. If G has unique Sylow $p-$subgroup P, then P is …… in G.

18. If G is a non-abelian group having order 14 then $G \cong$…….

19. $Z_m \times Z_n \cong Z_{mn}$ iff $\gcd(m, n) =$……

6.10 *ANSWERS*

Answer of self cheque question:

1. No **2.** Yes

Answer of terminal question:

15. $p-$group **16.** Sylow subgroups **17.** Normal

18. D_7 **19.** 1

BLOCK III

COMPOSITION SERIES, JORDAN HOLDER THEOREM AND SOLVABLE GROUP

Unit-7: NORMAL AND SUBNORMAL SERIES, COMPOSITION SERIES

CONTENT:

7.1 *INTRODUCTION*

A composition series in abstract algebra offers a technique to decompose an algebraic structure, such as a group or a module, into manageable parts. Since many naturally occurring modules are not semi-simple, they cannot be broken down into a straight sum of simple modules, necessitating the consideration of composition series in the context of modules. The direct sum decomposition of a module M into its simple constituents is replaced by a finite growing filtration of M by submodules such that the subsequent quotients are simple.

There may not be a composition series, and if there is, it need not be unique. However, a collection of findings together referred to as the Jordan-Hölder theorem states that wherever composition series exist, the isomorphism classes of simple pieces and their multiplicities are defined uniquely (albeit possibly not their exact locations within the composition series in issue). Thus, Artinian modules and finite groups' invariants may be defined using composition series.

A related but distinct concept is a chief series: a composition series is a maximal *subnormal* series, while a chief series is a maximal *normal series*.

7.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the maximal subgroup and simple group.
- Analyze of normal and subnormal series and composition series.
- Analyze the theorems and application of normal and composition series.

7.3 *NORMAL SERIES*

Definition: In a group G any normal subgroup $H \neq G$ is called a *maximal normal subgroup* of G if there does not exist any normal subgroup K of G such that $H \subset K \subset G$.

Thus normal subgroup $H \neq G$ is maximal in G if whenever $K \lhd G$ such that $H \subseteq K \subseteq G$ then either $K = H$ or $K = G$.

In fact, any subgroup $H \neq G$ is maximal in G whenever $H \leq K \leq G$ then either $K = H$ or $K = G$.

Similarly, any normal subgroup M of G is called minimal or minimal normal subgroup of G which are contained in M are $\{e\}$ and M. Thus, if N is normal subgroup of G s.t., $\{e\} \subseteq N \subseteq M$ then either $N = \{e\}$ or $N = M$.

Example 1: A_3 is a maximal normal subgroup of S_3. $O(A_3) = 3$ whereas $O(S_3) = 6$. Clearly there cannot be any subgroup of order 4 or 5 in S_3. We also notice that $O\left(\frac{S_3}{A_3}\right) = 2$, a prime and thus $\frac{S_3}{A_3}$ is a simple group.

Example 2: If G is a simple group then it has no non trivial normal subgroup and so {e} will be a (and only) maximal normal subgroup in G.

Theorem 1: H is maximal normal subgroup of G *iff* G/H is simple.

Proof: Let H be maximal normal in G. Any subgroup of G/H is of the form K/H where $K \leq G$ and $H \subseteq K$ and also K/H is normal in $G/H \Leftrightarrow K \lhd G$.

Thus any subgroup K/H will be non trivial normal subgroup of G/H if $H \lhd K \lhd G$, which is not true as H is maximal normal. So G/H has no non trivial normal subgroup and is, therefore simple.

Conversely, let G/H be simple. Suppose H is not maximal normal, then $\exists$ a normal subgroup K of G s.t.,

$H \subset K \subset G$ and thus K/H will be normal subgroup of G/H where $K/H \subset G/H$, a contradiction as G/H is simple.

Example 3: Any finite group G (with at least two elements) has a maximal normal subgroup.

Solution: If G is simple then it has no proper normal subgroup except $\{e\}$ and thus $\{e\}$ is a maximal normal subgroup of G.

Suppose G is not simple. Then it has at least one normal subgroup $N \neq G, N \neq \{e\}$. If N is maximal normal, we are done. If not, then there exist at least one normal subgroup M where $N \subset M \subset G$. If M is maximal normal, we are done. We continue in this way if not. Given that and only allow a finite number of subgroups, the aforementioned procedure must end after a finite number of steps. A maximal normal subgroup will thus exist.

Example 4: Illustrate example of maximal normal subgroup while it is not a maximal subgroup.

Solution: Consider $G = Z_2 \times A_5$

Then $H = Z_2 \times \{I\}$ is normal in G and $G/H \cong A_5$ and so G/H will be simple and hence maximal normal subgroup of G.

Since $H \subsetneq \{(0, I), (1, I), (0,123), (0,132)\} \subsetneq G$

Hence H is not a maximal subgroup of G.

Example 5: Let H, K be two distinct maximal normal subgroup of G then $G = HK$ and $H \cap K$ is a maximal normal subgroup of H as well as K.

Solution: Since H, K are normal, HK is normal in G.

Since $H \subseteq HK \subseteq G$ and HK is normal in G.

We must have $HK = H$ or $= G$

Similarly $HK = K$ or $HK = G$

Hence $HK = G$ (as $HK \neq G \Rightarrow HK = H, HK = K \Rightarrow H = K$).

Again by isomorphism theorem

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Thus $\frac{K}{H \cap K} \cong \frac{G}{H}$

Since H is maximal normal, $\frac{G}{H}$ is simple

i.e., $\frac{K}{H \cap K}$ is simple

$\Rightarrow H \cap K$ is maximal normal in K

Similarly, it is maximal normal in H.

Example 6: Show that $< Q, + >$ has no maximal normal subgroup.

Solution: Suppose H is a maximal normal subgroup of $< Q, + >$, then $\frac{Q}{H}$ is simple and so $\frac{Q}{H}$ has no non trivial normal subgroup i.e., it will have no non trivial subgroup (Q being abelian, all subgroups are normal). Thus $\frac{Q}{H}$ is a cyclic group of prime order p.

Let $H + x \in \frac{Q}{H}$ be any element

Then $p(H + x) = H$

i.e., $H + px = H$ or that $px \in H \ \forall x \in Q$

let now $y \in Q$ be any element, then $\frac{y}{p} \in Q$

If $\frac{y}{p} = x$ then $y = px \Rightarrow y \in H$ or that

$Q \subseteq H \subseteq Q \Rightarrow H = Q$, a contradiction

Hence the result follows.

Definition: Let G be a group and sequence of subgroups

$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq ..... \subseteq H_n = G$

is called a normal series of G if H_i is normal subgroup of H_{i+1}, $\forall i = 0, 1, 2, ..., n-1$

The factor (quotient) groups $\frac{H_{i+1}}{H_i} (\forall i)$ are called the factors of normal series.

Here each H_i is normal in H_{i+1}, although it may not be normal in G. Also it is possible that $H_i = H_{i+1}$ for some i. The number of distinct number of (1) excluding G is called the length of the normal series. The above is expressed in short by saying that $N = (H_0, H_1, ..., H_n)$ is a normal series of G. If N and M are two normal series of G s.t., $N \subseteq M$ then M is called a *refinement* of N (a proper refinement if $(N \underset{\neq}{\subset} M)$.

Remark: Some author mostly prefer to name the above **subnormal series**. It is then called a normal series if H_i is normal in $G \forall i$.

If G is any group then

$\{e\} = H_0 \subseteq H_1 = G$

Is an general example of a normal series.

Example 7: $\{I\} \subseteq A_3 \subseteq S_3$ is a normal series of S_3.

$\{I\} \subseteq E \subseteq K_4 \subseteq A_4 \subseteq S_4$ is a normal series of S_4, where

$E = \{I, (12)(34)\}$, $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

We have seen earlier that $E \trianglelefteq K_4$, but E is not normal in A_4 (and so in S_4).

7.4 *COMPOSITION SERIES*

Definition: Let G a group. A sequence of subgroup

$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq ..... \subseteq H_n = G$

of G is called a composition series of G if

(*i*) every H_i is normal subgroup of H_{i+1} $(i = 0, 1, ..., n-1)$

(*ii*) $H_i \neq H_{i+1}$ for any i and

(*iii*) $\frac{H_{i+1}}{H_i}$ is a simple group $\forall i$.

The quotient groups $\frac{H_{i+1}}{H_i}$ are called factors of the series.

By using the theorem 1 condition (iii) can be replaced by H_i is a maximal normal subgroup of H_{i+1} $\forall i$.

We notice that aforesaid composition series is a normal series. Converse of above is not true and that composition series has no gaps.

It is possible that group may have more than one composition series.

Example 8: In the group $(Z, +)$

$\{0\} \subset <8> \subset <4> \subset Z$ is a normal series while it is not a composition series as $<4>$ is not maximal in Z. It is also to be notify that $<4> \subset <2> \subset Z$.

Example 9: In the Quaternion group Q_8,

$\{1\} \subset \{1, -1\} \subset \{1, -1, i, -i\} \subset Q_8$

$\{1\} \subset \{1, -1\} \subset \{1, -1, j, -j\} \subset Q_8$

$\{1\} \subset \{1, -1\} \subset \{1, -1, k, -k\} \subset Q_8$

All are the composition series of Q_8. If we rewrite the first series as $G_0 = \{1\}, G_1 = \{1, -1\}$ $G_2 = \{1, -1, i, -i\}$ then $G_0 \subset G_1 \subset G_2 \subset G$

So, $O\left(\frac{G}{G_2}\right) = \frac{8}{4} = 2, O\left(\frac{G_2}{G_1}\right) = \frac{4}{2} = 2, O\left(\frac{G_1}{G_0}\right) = \frac{2}{1} = 2$

i.e., all quotient groups are of prime order and thus have no trivial normal subgroup and hence are simple.

Theorem 2: Each finite group G has a composition series. (Here group has more than one element)

Proof: We prove this by induction method on order of the group.

If $O(G) = 2$ then the only composition series of G is $\{e\} = G_0 \subset G_1 = G$. Since $\frac{G_1}{G_0} = \frac{G}{\{e\}} \cong G$ and as $O(G) = 2$, a prime it is simple group and therefore $\frac{G_1}{G_0}$ is simple.

Suppose for the groups with order less than $O(G)$ result holds. Now we will show results holds for G. If G is simple then $\{e\} \subset G$ is the composition series for G. Suppose G is not simple.

Although G is finite, it has a maximal normal subgroup $N \neq G$ and as $O(N) < O(G)$, results holds for N which then has a composition series, say

$\{e\} \subset N_1 \subset N_2 \subset ... \subset N$

Then the series

$\{e\} \subset N_1 \subset N_2 \subset ... \subset N \subset G$ will be a composition series for G.

Hence results holds.

Remark: If $O(G) = 1$, Sometimes, we claim that the results holds trivially since (G) is a composition series of G.

Check your progress

Problem 1: Check composition series of Z_{24}

Problem 2: Check out example of maximal normal subgroup while it is not a maximal subgroup.

7.5 *SUMMARY*

In this unit, we have studied about following major topics and their related theorems and examples.

- Maximal subgroup and on the basis of it to described the simple group.

- Illustration of normal series, subnormal series and on the basis of these to describe the composition series.

7.6 *GLOSSARY*

- Sequence of subgroup of the group G, $\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq ..... \subseteq H_n = G$ is called a normal series of G if H_i is normal subgroup of H_{i+1}, $\forall i = 0,1,2,...,n-1$
- $\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq ..... \subseteq H_n = G$ of G is called a composition series of G if

  (*i*) every H_i is normal subgroup of H_{i+1} $(i = 0,1,...,n-1)$

  (*ii*) $H_i \neq H_{i+1}$ for any i and

  (*iii*) $\frac{H_{i+1}}{H_i}$ is a simple group $\forall i$, where $\frac{H_{i+1}}{H_i}$ are called factors of the series.

7.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.
- https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=ZLCHeZEhCZ8yCri36nSF3A==

7.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

7.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Define normal series and also prove that H is maximal normal subgroup of G *iff* G/H is simple.

2. Define maximal subgroup and prove that finite group has maximal subgroup.

3. Prove that if H, K be two distinct maximal normal subgroup of G then $G = HK$ and $H \cap K$ is a maximal normal subgroup of H as well as K.

4. Prove that group of rational number has no maximal normal subgroup.

5. Define the composition series and also prove that each finite group G has a composition series.

Short Answer Type Question:

6. Prove that alternating group A_4 is maximal normal subgroup of S_4.

7. Give an example of maximal normal subgroup while it is not a maximal subgroup.

8. Define maximal subgroup, simple group, normal series, composition series.

9. Find normal series of S_3.

10. Find the composition series of Q_8.

Fill in the blanks:

11. A_3 is maximal normal subgroup of …….

12. If G is a simple group then it has no non trivial ……...

13. Each finite group has a …….

7.10 *ANSWERS*

Answer of self cheque question:

1. $\{0\} \subseteq <8> \subseteq <4> \subseteq <2> \subseteq Z_{24}, \{0\} \subseteq <12> \subseteq <4> \subseteq <2> \subseteq Z_{24}$,
$\{0\} \subseteq <12> \subseteq <6> \subseteq <2> \subseteq Z_{24}, \{0\} \subseteq <12> \subseteq <6> \subseteq <3> \subseteq Z_{24}$ **2.** See example 4

Answer of terminal question:

7. $Z_2 \times A_5$ **9.** $\{I\} \subseteq A_3 \subseteq S_3$ **17.** Normal **11.** S_3

12. Normal subgroup **13.** Composition series

Unit-8: JORDAN HOLDER THEOREM

CONTENT:

8.1 *INTRODUCTION*

German mathematician **Ludwig Otto Hölder** was born in Stuttgart on December 22, 1859, and he passed away on August 29, 1937.

Ludwig Otto Hölder
December 22, 1859 – August 29, 1937
https://en.wikipedia.org/wiki/Otto_H%C3%B6lder

In addition to being the grandson of professor Christian Gottlieb Hölder (1776–1847) and the youngest of three sons of professor Otto Hölder (1811–1890), Hölder also had two brothers who went on to become professors. He began his education at what is now the University of Stuttgart's Polytechnikum before moving to Berlin in 1877 to study under Leopold Kronecker, Karl Weierstrass, and Ernst Kummer.

He enrolled in the University of Berlin in 1877, and in 1882, he received his doctorate from the University of Tübingen. His PhD dissertation was titled "Beiträge zur Potentialtheorie" (translation: "Contributions to potential theory"). His next stop was the University of Leipzig, but he was unable to

complete his habilitation there. Instead, he earned a second doctorate and habilitation at the University of Göttingen, both in 1884.

He was given a job as an exceptional professor at Tübingen in 1889 after failing to obtain government clearance for a teaching seat in Göttingen. Despite a temporary mental impairment delaying his admission, he started working there in 1890. He assumed Sophus Lie's previous position as a full professor at the University of Leipzig in 1899. He served there as rector in 1918 after serving as dean from 1912 to 1913.

In 1899, he wed Helene, a politician's and a bank director's daughter. They have two girls and two boys. His daughter Irmgard married a mathematician named Aurel Wintner, and his son Ernst Hölder went on to become another mathematician.

Hölder ratified the German university and high school professors' oath of loyalty to Adolf Hitler and the National Socialist State in 1933.

Leonard James Rogers established Holder's inequality, which bears Hölder's name, first. It is named after a publication in which Hölder criticises it while referencing Rogers. This paper also contains a demonstration of what is now known as Jensen's inequality, along with certain side conditions that Jensen eventually deleted. Other theorems by Hölder include the Jordan-Hölder theorem, which states that every linearly ordered group satisfying an Archimedean property is isomorphic to a subgroup of the additive group of real numbers, the classification of simple groups with orders up to 200, the anomalous outer automorphisms of the symmetric group S6, and Hölder's theorem, which states that the Gamma function does not satisfy any algebraic differential equation. The Hölder condition (or Hölder continuity), another concept bearing his name, is applied in many analytical fields, including the theories of partial differential equations and function spaces.

8.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the Jordan- Hölder theorem.
- Analyze the theorems related to Jordan- Hölder theorem.

8.3 *JORDAN-HOLDER THEOREM*

Theorem 1: Let G be a finite group with two composition series

$G, H_1, H_2, ..., H_n = \{e\}$ …(1)

and $G, K_1, K_2, ..., K_m = \{e\}$ …(2)

Then $n = m$ and the two equivalent series of composition quotient groups., viz.,

$G/H_1, H_1/H_2, ..., H_{n-1}/H_n$

And $G/K_1, K_1/K_2, ..., K_{m-1}/K_m$

are abstractly identical i.e., they can be put into $1-1$ correspondence such that the corresponding quotient groups are isomorphic.

Proof: By using the induction technique on the order of the group G, we will demonstrate the theorem. We will demonstrate that the theorem also holds true for G by making the assumption that it holds true for all groups with orders lower than G. The theorem is obviously valid for every group of order one; therefore we need not be concerned about where to begin the induction.

There are two cases arise:

Case I: $H_1 = K_1$. In this case, after removing G from (1) and (2), we obtain the remaining series as two composition series for H_1. However, because H_1 is a proper normal subgroup of G, its order is lower than that of G. Therefore, the theorem holds true for H_1 according to our induction hypothesis. Since $G/H_1 = G/K_1$, therefore the theorem will remain true if we replace G in each of the series (1) and (2).

Case II: $H_1 \neq K_1$. Using the third law of isomorphism, we have

$H_1K_1/H_1 \cong K_1/H_1 \cap K_1$

And $H_1K_1/K_1 \cong H_1/H_1 \cap K_1$

Also H_1K_1 is a normal subgroup of G containing H_1. Since H_1 is maximal in G, therefore we must have $H_1K_1 = G$

$\therefore G/H_1 \cong K_1/D$ where $D \cong H_1 \cap K_1$

and $G/K_1 \cong H_1/D$

Now H_1 is a maximal in G implies that G/H_1 is simple. Therefore K_1/D is simple and this implies that D is a maximal normal subgroup of K_1. Similarly D is a maximal normal subgroup of H_1 .

Let $D, D_1, D_2, ..., D_t = \{e\}$ be a composition series for D. Then

$G, H_1, D, D_1, D_2, ..., D_t = \{e\}$ …(3)

and $G, K_1, D, D_1, D_2, ..., D_t = \{e\}$ …(4)

are two composition series for G. Let us write the composition quotient groups of (3) and (4) in the order

$G/H_1, H_1/D, D/D_1, D_1/D_2, ..., D_{t-1}/D_t$ …(5)

and $K_1/D, G/K_1, D/D_1, D_1/D_2, ..., D_{t-1}/D_t$ …(6)

The quotient groups in (5) and (6) are equal in number and the corresponding quotient groups isomorphic i.e., G/H_1 and K_1/D, H_1/D and $G/K_1, D/D_1$ and $D/D_1, ...,$ are isomorphic.

The two composition series for G at this point, (1) and (3), each have H_1 in the second position. Due to instance 1, it is possible to place the quotient groups described by (1) and (3) into 1-1 correspondence, making the respective quotient groups isomorphic. To make the respective quotient groups isomorphic, it is possible to put the quotient groups described by (2) and (4) into 1- 1 correspondence. As a result, the quotient groups defined by (1) and (2) are equal in number and are isomorphic in some order since the relation of isomorphism in the set of all groups is an equivalence relation. This completes the theorem's proof.

8.4 *SUMMARY*

After completing this unit we analyze that for any finite group (*G*) two composition series are always identical i.e., they can be put into one-one correspondence such that the corresponding quotient groups are isomorphic.

8.5 *GLOSSARY*

- For a finite group (*G*) the **Jordan- Hölder** theorem states that two composition series

$G, H_1, H_2, ..., H_n = \{e\}$ … (1)

and $G, K_1, K_2, ..., K_m = \{e\}$ … (2)

the two corresponding series of composition quotient groups,

$G/H_1, H_1/H_2, ..., H_{n-1}/H_n$

$G/K_1, K_1/K_2, ..., K_{m-1}/K_m$, where $m = n$

are abstractly identical.

8.6 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.

- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

8.7 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

8.8 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. State and prove the Jordan- Hölder theorem.

Short Answer Type Question:

2. Write the statement of Jordan- Hölder theorem.

Fill in the blanks:

3. For a finite group (G) two composition series, the two composition quotient groups are …….

8.9 *ANSWERS*

3. Identical

Unit-9: SOLVABLE GROUPS, SIMPLICITY OF $A_n\ (n \geq 5)$, NILPOTENT GROUPS

CONTENT:

9.1 *INTRODUCTION*

A group having an upper central series that ends with *G* is referred to as a nilpotent group *G* in mathematics, more especially group theory. In other words, either its lower central series ends in 1 or its central series has a limited length. A group that is "almost abelian" is what we would term a nilpotent group. The fact that nilpotent groups may be solved and that for finite nilpotent groups, two members with relatively prime orders must commute serves as the inspiration for this concept. Additionally, it is true that supersolvable finite nilpotent groups exist. The Russian mathematician Sergei Chernikov is credited with developing the idea in the 1930s. Nilpotent groups appear in both group classification and Galois theory. They play a significant role in the categorization of Lie groups as well.

A group that can be created from abelian groups via extensions is referred to as a solvable group or soluble group in mathematics, more especially in the subject of group theory. A group is solvable if its derived series terminates in the trivial subgroup, to put it another way.

9.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the Nilpotent group.
- Analyze the definition and important theorems related to Solvable groups.
- Analyze the further theorems on the alternating group $(A_n, n > 5)$.

9.3 *NILPOTENT GROUP*

On commutative groups, the converse of the Lagrange's Theorem is true. In this chapter, we characterise a broader category of groups called nilpotent groups, which satisfy the opposite of Lagrange's Theorem. Additionally, every nilpotent group is a direct result of the subgroups of Sylow, and vice versa.

Definition (*i*): Let G be a group and denote

$Z_0(G) = \{e\}, Z_1(G) = Z(G)$ and $Z_{i+1}(G) = Z(G)$ is the unique normal subgroup of G such that $Z(G) \subseteq Z_{i+1}(G)$ and $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$

Then the chain of normal subgroups

$\{e\} \subseteq Z_1(G) \subseteq Z_2(G) \subseteq ...$

is called upper central series and ascending central of G.

Definition (*ii*): A group G is defined to be nilpotent if $Z_n(G) = G$ for some $n \in N$

Example 1: Each abelian group G is also a nilpotent group, since $Z_1(G) = Z(G) = G$. Converse of this is also not true which shows in following result.

Theorem 1: Each finite p-group is nilpotent.

Proof: Let G be a finite $p-$group. If $|G| = 1$, then G is nilpotent. Suppose that $|G| > 1$. Then G being a nontrivial $p-$group, it follows that $Z_1(G) = Z(G) \neq \{e\}$. If $Z_1(G) \neq G$, then $G/Z_1(G)$ is a nontrivial $p-$group and $|Z(G/Z_1(G))| > 1$. This implies $Z_2(G)$ contains $Z_1(G)$ properly, that is $Z_1(G) \subsetneq Z_2(G)$. If $Z_2(G) \neq G$, then similarly $Z_2(G) \neq Z_3(G)$. If for all $n \in N$, $Z_n(G) \neq G$, then we get an infinite number of strictly ascending chain of subgroups

$\{e\} \subsetneq Z_1(G) \subseteq Z_2(G) \subsetneq ...$

But it is not possible because G is finite group. Thus there is $n \in Z$ such that $Z_n(G) = G$ and G is nilpotent.

Now we give an example of a subgroup which is not nilpotent.

Example 2: We know that $Z(S_3) = \{e\}$. Thus $Z_1(S_3) = \{e\}$ and $S_3 / Z_1(S_3) \approx S_3$. This implies $Z(S_3 / Z_1(S_3)) = \{\{e\}\}$. Since $Z_2(S_3)$ is the unique normal subgroup of S_3 such that $Z_2(S_3) / Z_1(S_3) = Z(S_3 / Z_1(S_3)) = \{\{e\}\}$, so it follows that $Z_2(S_3) / Z_1(S_3) = \{e\}$. Similarly, $Z_n(S_3) = \{e\} \forall n \in N$. Hence S_3 is not nilpotent.

Theorem 2: The direct product of finite number of nilpotent groups is nilpotent.

Proof: It will be sufficient to prove the result for the direct product of two groups. Let H and K be two nilpotent groups and denote $G = H \times K$.

First we prove that $Z_n(G) = Z_n(H) \times Z_n(K) \forall n \in N$ by the induction on n. We have already proved that the external direct product of groups and results holds for $n = 1$. Assume that $Z_n(G) = Z_n(H) \times Z_n(K)$ for some $n \geq 1$. Since $Z_n(H \times K) = Z_n(H) \times Z_n(K)$, so there is an isomorphism $\psi : H / Z_n(H) \times K / Z_n(K) \to \dfrac{H \times K}{Z_n(H \times K)}$.

Now we have,

$$Z(G / Z_n(G)) = Z(H \times K / Z_n(H \times K))$$
$$= Z(\psi(H / Z_n(H) \times K / Z_n(K)))$$
$$= \psi(Z(H / Z_n(H) \times K / Z_n(K)))$$
$$= \psi(Z(H / Z_n(H)) \times Z(K / Z_n(K)))$$
$$= \psi(Z_{n+1}(H) / Z_n(H)) \times Z_{n+1}(K) / Z_n(K))$$
$$= Z_{n+1}(H) \times Z_{n+1}(K) / Z_n(H) \times Z_n(K))$$
$$= Z_{n+1}(H) \times Z_{n+1}(K) / Z_n(H \times K)$$

It follows that $Z_{n+1}(G) = Z_{n+1}(H) Z_{n+1}(K)$ because $Z_{n+1}(G)$ is the only normal subgroup of G such that $Z_{n+1}(G) / Z_n(G) = Z(G / Z_n(G))$.

Accordingly, for all $n = 0, 1, 2, ...$ $Z_n(G) = Z_n(H) \times Z_n(K)$ according to the principle of mathematical induction.

There is a positive integer n such that $Z_n(H) = H$ and $Z_n(K) = K$ since H and K are both nilpotent. Hence

As $H \times K$ is nilpotent, $Z_n(H \times K) = Z_n(H) \times Z_n(K)$.

Using a descending central series, we now provide an alternate equivalent characterisation of nilpotent groups. Assume G is a group and H and K are its two subgroups. The subgroup produced by all elements of the form $hkh^{-1}k^{-1}$ for every $h \in H$ and all $k \in K$ is denoted by $[H\,K]$. Next, we have

Lemma 1: Let G be a group, H, K be two subgroups of G and K normal in G. Then $[H,G] \subseteq K$ if and only if $HK/K \subseteq Z(G/K)$.

Definition: Let G be a group. Define inductively

$G^{[1]} = G$

$G^{[i+1]} = [G^{[i]}, G]$ for all $i \geq 1$

Then the chain of normal subgroups

$G = G^{[1]} \supseteq G^{[2]} \supseteq ...$

is called the descending central series of G.

Theorem 3: Let G be a group. Then G is nilpotent if and only if $G^{[n+1]} = \{e\}$ for some integer $n \geq 0$.

Proof: First assume that there is an integer $n \geq 0$ such that $G^{[n+1]} = \{e\}$. Consider the series

$\{e\} = G^{[n+1]} \subseteq G^{[n]} \subseteq ... \subseteq G^{[1]} = G$

it is easy to check that $G^{[i]}/G^{[i+1]} \subseteq Z(G/G^{[i+1]})$ for all $i = 1,2,...,n$ and $G^{[n+1-i]} \subseteq Z_i(G)$ for all $i = 1,2,...,n$. Thus $G = G^{[1]} \subseteq Z_n(G)$, and so G is nilpotent.

Conversely, suppose that G is nilpotent. Then there is an integer $n \geq 1$ such that $Z_n(G) = G$ Thus we have a series of normal subgroups

$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq ... \subseteq Z_n(G) = G$

Then it follows that $G^{[i]} \subseteq Z_{n+1-i}(G) \forall\, i = 1,2,...,n+1$. Thus $G^{[n+1]} \subseteq Z_0(G) = \{e\}$, and so $G^{[n+1]} = \{e\}$.

Theorem 4: Each subgroup of a nilpotent group is nilpotent.

Proof: Let G be a group and H be a subgroup of G. Since G is nilpotent, so there is an integer $n \geq 0$ such that $G^{[n+1]} = \{e\}$. Now we show that $H^{[i]} \subseteq G^{[i]}$ by the induction on i. Now $H^{[1]} = H \subseteq G = G^{[1]}$. Assume that $H^{[i]} \subseteq G^{[i]}$. Then $H^{[i+1]} = [H^{[i]}, H] \subseteq [G^{[i]}, G] \subseteq G^{[i+1]}$ and hence, by the principle of mathematical induction, $H^{[i]} \subseteq G^{[i]}$ for all $i = 1,2,...,n+1$. Hence $H^{[n+1]} \subseteq G^{[n+1]} = \{e\}$, and so H is nilpotent.

Example 3: Let $G = S_3 \times Z$. Since S_3 is not nilpotent, so G is not nilpotent. Thus G is an infinite group which is not nilpotent.

Theorem 5: A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.

Proof: Let G be a nilpotent group. First we show that every Sylow subgroup of G is normal. If possible, let P be a Sylow subgroup of G such that $N(P) \neq G$. Denote $H = N(P)$. Since G nilpotent, there is $n \in N$ such that

$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq ... \subseteq Z_n(G) = G$

Since H is proper and $Z_0(G) \subseteq H$, so there is the largest index $m < n$ such that $Z_m(G) \subseteq H$. Then $Z_{m+1}(G) \subset_{\neq} H$. Consider $a \in Z_{m+1}(G) \setminus H$, then $Z_{m+1}(G) \setminus Z_m(G)$ implies that $aZ_m(G) \in Z(G/Z_m(G))$ and so $haZ_m(G) = ahZ_m(G)$ for every $h \in H$. Hence $h^{-1}a^{-1}ha \in Z_m(G) \subseteq H$ which implies that $a^{-1}ha = h(h^{-1}a^{-1}ha) \in H$. Thus $a^{-1}Ha \subseteq H$ and $a \in N(H)$. Therefore $H \subset_{\neq} N(H)$ that is $N(P) \subset_{\neq} N(N(P))$, which contradicts that P is a Sylow subgroup. Thus $N(P) = G$ and every Sylow subgroup of G is normal. Hence, G is a direct product of its Sylow subgroups.

Conversely, let G be a direct product of its Sylow subgroups $P_1, P_2, ..., P_k$. Since P_i is a p_i-group for some prime p_i, so P_i is nilpotent for every $i = 1,2,...,k$ Hence their direct product G is also nilpotent.

The result that follows now demonstrates that the converse of Lagrange's Theorem is true for all nilpotent groups.

Corollary 1: Let G be a finite nilpotent group. Then for every positive divisor m of $|G|$, G hasa subgroup of order m.

Proof: Let $|G| = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$. Since G is nilpotent, so $G = P_1 \times P_2 \times ... \times P_k$, where P_i is the sylow $p_i -$subgroup of G for $i = 1,2,...,k$. Also $|P_i| = p_i^{k_i}$. Let m be a positive integer such that $m \mid |G|$. Then $|G| = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$, where $0 \leq m_i \leq n_i$. Since P_i is $p_i -$group of order $p_i^{n_i}$ and $m_i \leq n_i$, so P_i has a subgroup H_i of order $p_i^{m_i}$, by the Sylow's first theorem. Then $H = H_1 \times H_2 \times ... \times H_k$ is a subgroup of G of order $|H_1||H_2|...|H_k| = p_1^{m_1} p_2^{m_2} ... p_k^{m_k} = m$.

9.4 *SOLVABLE GROUP-I*

Solvable groups first appeared in the setting of Galois theory. Galois developed this idea to explore the quintics' radical solvability over an extended period of time. Solvable groups are a class of groups that are fascinating in and of themselves, particularly in relation to the idea of finite groups. Here, we treat the solvable groups using only group theory.

Definition 1: Let G be a group. Then a chain

$G = H_0 \supseteq H_1 \supseteq ...H_{n-1} \supseteq H_n = \{e\}$

of subgroups is called a solvable series of G if H_{i+1} is normal in H_i and H_i / H_{i+1} is commutative for every $i = 0,1,...,n-1$.

A group G is called a solvable group if G has a solvable series.

Each abelian group is solvable. For, if G is abelian, then $G = H_0 \supseteq H_1 = \{e\}$ is a solvable series for G

Example 4: $S_3 = H_0 \supseteq \{e,(123),(132)\} \supseteq \{e\}$ is a solvable series for S_3. Thus S_3 is a solvable group while S_3 is not nilpotent.

Theorem 6: Every nilpotent group is solvable.

Proof: Let G be a nilpotent group. Then $Z_n(G) = G$ for some positive integer n. Then the series of normal subgroups

$G = Z_n(G) \supseteq Z_{n-1}(G) \supseteq ... \supseteq Z_0(G) = \{e\}$

is a solvable series, since $Z_i(G) / Z_{i-1}(G) = Z(G / Z_{i-1}(G))$ which is abelian for every $i = 1,2,...,n$. Hence G is a solvable group.

Now, taking into account subgroups and homomorphic images, we demonstrate that the class of all solvable groups is closed under finite direct product.

Theorem 7: Each finite direct product of solvable group is solvable.

Proof: This is adequate to establish the conclusion regarding the direct product of two solvable groups. Let G and H be two solvable groups. Then both G and H have a series of subgroups that can be solved, say

$G = G_0 \supseteq G_1 \supseteq ... \supseteq G_n = \{e\}$

And $H = H_0 \supseteq H_1 \supseteq ... \supseteq H_m = \{e\}$

Consider following series of subgroups of $G \times H$:

$G \times H = G_0 \times H_0 \supseteq G_1 \times H_0 \supseteq ... \supseteq \{e\} \times H_0 \supseteq \{e\} \times H_1 \supseteq ... \supseteq \{e\} \times H_m \supseteq \{e\}$.

This is a solvable series for $G \times H$, since $G_{i+1} \times H_0$ is normal in $G_i \times H_0$ and $\{e\} \times H_{i+1}$ is normal in $\{e\} \times H_i$, and both $\frac{G_i \times H_0}{G_{i+1} \times H_0} \cong G_i / G_{i+1}$ and $\frac{\{e\} \times H_i}{\{e\} \times H_{i+1}} \cong H_i / H_{i+1}$ are abelian.

Hence $G \times H$ is a solvable group.

Theorem 8: Let G be a solvable group. Then every subgroup of G is solvable.

Proof: Let H be a subgroup of G. Since G is solvable, so it has a solvable series, say

$G = G_0 \supseteq G_1 \supseteq ... \supseteq G_n = \{e\}$

Then G_{i+1} is a normal subgroup of G_i which implies that $H \cap G_{i+1}$ is normal subgroup of $H \cap G_i$.

Denote $H_i = H \cap G_i$ and consider the series

$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_n = \{e\}$

Of subgroup of H. Now

$H_{i+1} = H \cap G_{i+1} = H \cap G_i \cap G_{i+1} = H_i \cap G_{i+1}$

Then using the second isomorphism theorem, that $\frac{H_i}{H_{i+1}} = \frac{H_i}{H_i \cap G_{i+1}} \cong \frac{H_i G_{i+1}}{G_{i+1}}$. Since the quotient group $\frac{H_i G_{i+1}}{G_{i+1}}$ is a subgroup of the abelian group G_i / G_{i+1}, so it is abelian group. Thus

Is a solvable series for H and the subgroup H is a solvable group.

Theorem 9: Let G be a solvable group. Then the quotient group G/H is solvable for every normal subgroup H of G.

Proof: Let $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_n = \{e\}$ be a solvable series of G. Since H is a normal subgroup, so $G_i H$ is a subgroup of G and $H \subseteq G_i H$ for each i. Consider the series

$G/H = G_0 / H \supseteq G_1 H / H \supseteq G_2 H / H \supseteq ... \supseteq G_n H / H = \{H\}$

Of subgroup of G/H. Also G_{i+1} is normal in G_i and hence $G_{i+1} H$ is a normal subgroup of $G_i H$. Thus $G_{i+1} H / H$ is a normal subgroup of $G_i H / H$.

Now using the third isomorphism theorem

$\frac{G_i H / H}{G_{i+1} H / H} \cong G_i H / G_{i+1} H$.

Define $\psi : G_i / G_{i+1} \to G_i H / G_{i+1} H$ by

$\psi(aG_{i+1}) = aG_{i+1} H$.

Then $G_{i+1} \subseteq G_{i+1} H$ implies that ψ is well-defined and for every $ah \in G_i H$,

$ahG_{i+1} H = (aG_{i+1} H)(hG_{i+1} H) = aG_{i+1} H = \psi(aG_{i+1})$

$\Rightarrow \psi$ is onto.

Also ψ is a homomorphism. Since G_i / G_{i+1} is abelian it follows that $G_iH / G_{i+1}H = \psi(G_i / G_{i+1})$ is abelian. Thus the series

$G/H = G_0/H \supseteq G_1H/H \supseteq G_2H/H \supseteq ... \supseteq G_nH/H = \{H\}$ is a solvable series and the quotient group G/H is solvable group.

Corollary 2: Each homomorphic image of solvable group is solvable.

Proof: Let G be a solvable group and $f : G \to \overline{G}$ be an epimorphism. Then by the first isomorphism theorem $G/\ker f \cong \overline{G}$. Since G is solvable, the quotient $G/\ker f$ is a solvable group. Hence $\overline{G}$ is solvable.

Theorem 10: If H be a normal subgroup of a group G. If both H and G/H are solvable, then G is solvable.

Proof: The correspondence theorem implies that every subgroup of G/H is of the form K/H, where K is a subgroup of G such that $H \subseteq K$, and K/H is normal in G/H if and only if K is normal in G. Since G/H is a solvable group, so it has a solvable series, say

$G/H = K_0/H \supseteq K_1/H \supseteq ... \supseteq K_m/H = \{H\}$.

Since K_{i+1}/H is normal in K_i/H, so K_{i+1} is normal in K_i and $\dfrac{K_i/H}{K_{i+1}/H} \cong \dfrac{K_i}{K_{i+1}}$, by the third isomorphism theorem. Thus K_i / K_{i+1} is abelian.

Since H is a solvable group, it has a solvable series, say

$H = H_0 \supseteq H_1 \supseteq ... \supseteq H_n = \{e\}$

Hence

$G = K_0 \supseteq K_1 \supseteq ... \supseteq K_m = H \supseteq H_1 \supseteq ... \supseteq H_n = \{e\}$

is solvable series for G and G is solvable.

Now we have the following two intersection consequences.

Corollary 3: Let G be a group, H and K be two subgroup of G and H be normal in G. If both H and K are solvable then HK is solvable.

Proof: First note that HK is a subgroup of G, since H is normal in G. Now, using the second isomorphism theorem, we have $HK/H \cong K/H \cap K$. Since $H \cap K$ is a subgroup of the solvable group K, it is solvable; and so $K/H \cap K$ is a solvable group. Then both H and HK/H are solvable, whence HK is solvable.

Corollary 4: Let G be a solvable group and H, K be two normal subgroup of G such that both the quotients G/H and G/K are solvable. Then G is solvable if and only if $H \cap K$ is solvable.

Proof: Let G be a solvable group. Since $H \cap K$ is a subgroup of G, so it is solvable.

Conversely, assume that $H \cap K$ is a solvable group. Both H and K are normal. Now using second isomorphism theorem, $HK/H \cong K/H \cap K$. Since HK/H is a subgroup of the solvable group G/H, so it is and hence $K/H \cap K$ is solvable. Then it follows that K is solvable, Since $H \cap K$ is solvable. Thus both G/K and K are solvable, and hence G is solvable.

Example 5: Let G be a group of order $14 = 7 \times 2$. Then it follows from the Sylow theorems that G has a normal Sylow 7-subgroup $7-$subgroup H. Since $|H| = 7$ which is a prime, so H is a solvable group. Similarly, $|G/H| = 2 \Rightarrow$ the quotient G/H is solvable. Hence G is solvable.

Example 6: Let G be a group of order $2002 = 143 \times 7 \times 2$. Then it follows from the Sylow theorem that G has a normal Sylow $143-$subgroup H. Since $|H| = 143$ which is a prime, so H is asolvable group. Now $|G/H| = 14$ and hence it is solvable. Thus G is a solvable group.

9.5 *SOLVABLE GROUP-II*

In this section, we characterise solvable groups in a way that is equivalent to the series of derived subgroups. This similar characterization aids in our demonstration that S_n cannot be solved for all $n \geq 5$. A discussion of the opposite of Lagrange's Theorem on solvable groups marks the end of this section.

Definition: Let G be a group. Then subgroup generated by the set $\{aba^{-1}b^{-1} \mid a, b \in G\}$ is called the commutator subgroup of G.

It is denoted by G' and the elements of the form $aba^{-1}b^{-1} \mid a, b \in G$ are called commutators.

If G is an abelian group, then for each $a, b \in G, aba^{-1}b^{-1} = e$ and hence $G' = \{e\}$. Conversely, if $G' = \{e\}$ then $aba^{-1}b^{-1} = e \Rightarrow ab = ba \; \forall \, a, b \in G$. Thus G is abelian. Hence G is abelian if and only if $G' = \{e\}$. In some sense G' is a reverse measure of how much G is commutative.

Theorem 11: Let G be a group. Then the derived subgroup G' is a normal subgroup of G and the quotient group G/G' is abelian.

Proof: Let $x \in G'$ and $g \in G$. Then $gxg^{-1}x^{-1} \in G'$. Since G' is a subgroup, $gxg^{-1} = \left(gxg^{-1}x^{-1}\right)x \in G'$. Hence G' is a normal subgroup of G.

Let $a,b \in G$. Then $ab(ba)^{-1} = aba^{-1}b^{-1} \in G' \Rightarrow abG' = baG'$, i.e., $(aG')(bG') = (bG')(aG')$. Hence G/G' is abelian.

Theorem 12: Let G be a group and N be a normal subgroup of G. Then G/N is abelian if and only if $G' \subseteq N$.

Proof: Initialy first we assume that G/N is abelian, then $(aN)(bN) = (bN)(aN) \forall a,b \in N$, and so $abN = baN$. Hence $aba^{-1}b^{-1} = ab(ba)^{-1} \in N \forall a,b \in G$

$\Rightarrow N$ contains all commutators of G and so $G' \subseteq N$

Conversely, if $G' \subseteq N$, then $aba^{-1}b^{-1} \in N \Rightarrow abN = baN \forall a,b \in G.$ Hence G/N is abelian.

Definition: Let G be a group and we define the following,

$G^{(1)} = G'$

$G^{(i+1)} = G^{(i)'}$

Then $G^{(i)}$ is called the $i-th$ commutator subgroup or derived subgroup of G.

Thus a sequence of subgroups $G \supseteq G^{(1)'} \supseteq G^{(2)'} \supseteq \ldots$, where each $G^{(i+1)'}$ is a normal subgroup of $G^{(i)'}$ and $G^{(i)'}/G^{(i+1)'}$ is abelian for every $i = 1,2,...$

Theorem 13: Let G be a group. Then G is solvable if and only if there is a positive integer n such that $G^{(n)'} = \{e\}$.

Proof: If $G^{(n)'} = \{e\}$, then the chain $G \supseteq G^{(1)'} \supseteq G^{(2)'} \supseteq \ldots G^{(n)'} = \{e\}$ become a solvable series for G. Hence G is solvable.

Conversely assume that G is a solvable group. Then G has a solvable series, say $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots G_n = \{e\}$. Since for every i, G_i is normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian, so $G'_{i-1} \subseteq G_i$. Hence

$G^{(1)} = G' = G_0' \subseteq G_1, G^{(2)} = G_1' \subseteq G_2$ and so on.

Thus we get $G^{(n)} \subseteq G_n = \{e\}$ and so $G^{(n)} = \{e\}$.

Now we will prove that permutation group S_n is not solvable for $n \geq 5$.

Lemma 2: If H is a subgroup of S_n $(n \geq 5)$ that contains all 3-cycles, then H' contains all 3-cycles in S_n.

Proof: Let $\sigma = (abc)$ be a 3-cycle in S_n. Since $n \geq 5$, we have two symbols x and y such that a,b,c,x,y are distinct. Denote $\alpha = (abx)$ and $\beta = (acy)$. Then

$\alpha, \beta \in H \Rightarrow \sigma = (abc) = (abx)(acy)(axb)(ayc) = \alpha\beta\alpha^{-1}\beta^{-1} \in H'$

Hence H' contains all 3-cycles in S_n.

Theorem 14: S_n is not solvable for $n \geq 5$.

Proof: Let A be the set containing all $3-$cycle in S_n. Since $n \geq 5$, so by the above lemma $A \subseteq S_n'$. Applying the same repeatedly, we get $A \subseteq S_n^{(k)}$ for each $k \in N$. Hence $S_n^{(k)} = \{e\}$ for each $k \in N$ and S_n is not solvable.

The Sylow theorems, which are valid for finite solvable groups, are now generalised as follows. P. Hall demonstrated this outcome in 1928.

Definition: Let G be a group. A subgroup H of G is called a characteristic in G if $\phi(H) \subseteq H$ for every automorphism $\phi : G \to G$; and H is called fully invariant if $f(H) \subseteq H$ for all endomorphism $f : G \to G$.

Let H be a characteristic of G and $\phi : G \to G$ be an automorphism. Then $\phi(H) \subseteq H$. Also $\phi^{-1} : G \to G$ is an automorphism and hence $\phi^{-1}(H) \subseteq H$. Then $H = \phi\left(\phi^{-1}(H)\right) \subseteq \phi(H)$ and hence $\phi(H) = H$.

Lemma 3: Let G be a group and H, K be two subgroup of G.

(*i*) If H is characteristic in K and K is normal in G, then H is normal in G.

(*ii*) Every normal Sylow subgroup is fully invariant.

(*iii*) If G is solvable and N is a minimal normal subgroup of G, then N is an abelian $p-$group for some prime p.

Proof (*i*): Let $a \in G$. Then $\phi : G \to G$ defined by $\phi(g) = aga^{-1}$ is an automorphism. Since K is normal in G, so $\phi|_K : K \to K$ is an automorphism. Then $\phi|_K (H) \subseteq H$, since H is a characteristic in K. Thus $aha^{-1} \subseteq H \; \forall \, h \in H$ and so H is normal in G.

(*iii*): Since the commutator subgroup N' is fully invariant in N and N is normal in G, so it follows that N' is normal in G. Then, the minimality of N implies that $N' = \{e\}$ or $N' = N$. Since N is solvable, $N' \neq N$ and so $N' = \{e\}$. Hence N is an abelian group. Also, by the minimality of $N, |N| > 1$. Let p be a prime such that $p \,||\, N|$ and P be a Sylow $p-$subgroup of N. Then $|P| > 1$. Since N is abelian, so P is normal; and it follows that P is fully invariant. Hence P is normal in G. Then minimally of N implies that $N = P$.

We also require the conclusion regarding Sylow subgroups, which we declare here without providing any evidence.

Lemma 5: (Frattini Argument) Let K be a normal subgroup of a finite group G. If P is a Sylow $p-$ subgroup of K and $M = N_G(P)$, then $G = KM$.

Proof: We prove this result by induction on $|G|$. The result is trivial for all groups G with $|G| \leq 5$. Consider a group G and assume that the result holds for all groups of order $< |G|$. Let $|G| = mn$ and $\gcd(m, n) = 1$.

Now two cases are arises:

Case I: G has a proper normal subgroup N such that $n \nmid |N|$. By Lagrange's theorem, $|N| = m_1 n_1$ where $m_1 \mid m$ and $n_1 \mid n$. Also $n \nmid |N|$ implies that $n_1 < n$. Since G is solvable, so G/N is a solvable group and $|G/N| = \frac{m}{m_1}.\frac{n}{n_1} < mn$ together with $\gcd\left(\frac{m}{m_1}, \frac{n}{n_1}\right) = 1$ implies, by the induction hypothesis that, G/N has a subgroup K/N of order $\frac{m}{m_1}$, where K is a subgroup of G. Then K is solvable, and

$$|K| = |K/N|.|N| = \frac{m}{m_1}.m_1 n_1 = mn_1 < mn$$

K has a subgroup H of order m.

Case II: n divides the order of every normal subgroup of G. Since G is finite, it has a minimal normal subgroup, say H. Then H is abelian and $|H| = p^r$ for some prime p, Since G is solvable. Now, using Lagrange's theorem, $p^r \,||\, G| = mn$. Then $n \mid p^r$ and H is a Sylow $p-$subgroup of G. Since H is normal in G, it is the unique Sylow $p-$subgroup of G. If K is minimal normal subgroup of G, then arguing similarly we have $|K| = q^8$ for some prime q and K is the unique Sylow $q-$ subgroup of G. Since $n \,||\, H|$ and $n \,||\, K|$, so p, q cannot be distnict. Thus H is the unique minimal normal subgvroup of G, that is H is contained in every proper normal subgroup of G.

Let K/H be a minimal normal subgroup of G/H. Since G/H is solvable, $|G/H| = q^8$ for some prime $q \neq p$. Then K is a normal subgroup of G such that $|K| = p^r q^8$. If Q is a Sylow $q-$ subgroup of K, then $HQ \subseteq K$ and $|HQ| = \frac{|H|.|Q|}{|H \cap Q|} = |H|.|Q| = p^r q^8 = |K|$

$\Rightarrow K = HQ$. Let $M = N_G(Q)$. We shall show that $|M| = m$.

Set $N = M \cap K = N_K(Q)$. Then Fratini argument gives us us $G = KM$ and we have $G/K = KM/K \cong M/K \cap M = \frac{M}{N}$. Then $|M| = \frac{|G|.|N|}{|K|}$. Now $Q \subseteq N \subseteq K$

$\Rightarrow K = HQ \subseteq HN \subseteq K$, that is $K = HN$. Thus,

$$|M| = \frac{|G|.|N|}{|K|}$$

$$= \frac{|G|.|N|}{|HN|}$$

$$= \frac{|G|.|H \cap N|}{|H|}$$

$$= |H \cap N|.$$

$$= m.|H \cap N| \quad [\because |H| = p^r = n]$$

Thus it is only to show $|H \cap N| = 1$, which will prove in two parts

(*i*) $H \cap N \subseteq Z(K)$ and **(*ii*)** $Z(K) = \{e\}$

(*i*) Let $a \in H \cap N$. Since $K = HQ$, every element of K is of the form hb where $h \in H, b \in Q$. Since H is abelian, a commutes with h. So it suffices to show that a commutes with every $b \in Q$. Now $(aba^{-1})b^{-1} \in Q$, since $a \in N = N_k(Q)$ and $(aba^{-1})b^{-1} \in H$, since H is normal in G. Thus $aba^{-1}b^{-1} \in H \cap Q = \{e\}$ and hence $ab = ba$.

(*ii*) Since $K \lhd G$, so $Z(K) \lhd G$, if $Z(K) = \{e\}$. Then it contains a minimal subgroup, say U. Since $U \subseteq Z(K)$, so U is normal in G and becomes a minimal normal subgroup of G. Since H is unique subgroup which is normal in G. Thus $U = H \subseteq Z(K)$. Now $K = HQ$,

$\Rightarrow P$ is a character subgroup of K.

Since $K \lhd G$, it follows by Lemma that $Q \lhd G$.

Since H is the unique minimal normal subgroup of G, so $H \subseteq Q$

Which is a contradiction. Hence $Z(K) = \{e\}$.

Check your progress

Problem 1: Check that for which value of n, S_n is solvable.

Problem 2: Check that Z_{14} is solvable or not?

Problem 3: Give an example of a group which is solvable group but not nilpotent group?

9.6 *SUMMARY*

In this unit, we have studied about major topics in group theory like nilpotent group, solvable group and symmetric groups S_n for $(n \geq 5)$ and their related theorems and examples. After completion of this unit we have learned the following important concepts:

- Each abelian group G is also a nilpotent group and solvable group.
- Each finite *p*-group is nilpotent.
- Direct product of finite number of nilpotent groups is nilpotent.
- Each subgroup of a nilpotent group is nilpotent.
- Each nilpotent group is solvable.
- Finite direct product of solvable group is solvable.
- Each subgroup of solvable group is solvable.
- Homomorphic image of solvable group is solvable.
- S_n is not solvable for $n \geq 5$.

9.7 *GLOSSARY*

- **Nilpotent group:** Any group is nilpotent if $Z_n(G) = G$ for some $n \in N$
- **Solvable group:** Let G be a group. Then a chain $G = H_0 \supseteq H_1 \supseteq ...H_{n-1} \supseteq H_n = \{e\}$ of subgroups is called a solvable series of G if H_{i+1} is normal in H_i and H_i / H_{i+1} is commutative for every $i = 0,1,...,n-1$.

  A group G is called a solvable group if G has a solvable series.

9.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

9.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

9.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that every finite $p-$group is abelian.

2. Prove that a finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.

3. If G be a solvable group. Then the quotient group G/H is solvable for every normal subgroup H of G.

4. If G be a group, H and K be two subgroup of G and H be normal in G. If both H and K are solvable then HK is solvable.

5. If G be a group, H and K be two normal subgroup of G such that both the quotients G/H and G/K are solvable. Then G is solvable if and only if $H \cap K$ is solvable.

6. S_n is not solvable for every $n \geq 5$.

Short Answer Type Question:

7. Prove that direct product of a finite number of nilpotent groups is nilpotent.

8. Prove that every subgroup of a nilpotent group is nilpotent.

9. If G be a finite nilpotent group then prove that for every positive divisor m of $|G|$, G has a subgroup of order m.

10. Prove that every nilpotent group is solvable.

11. Every homomorphic image of a solvable group is solvable.

12. If H be a normal subgroup of a group G. If both H and G/H are solvable, then G is solvable.

13. If G be a solvable group. If $|G| = mn$ such that $\gcd(m,n) = 1$, then G has a subgroup of order m.

14. If G be a group. Then prove that G is solvable if and only if there is a positive integer n such that $G^{(n)} = \{e\}$.

Fill in the blanks:

15. Every finite $p-$group is…….

16. S_3 is …….. nilpotent group

17. Direct product of finite number of nilpotent group is ……..

18. Every subgroup of nilpotent group is ……..

19. S_n is not solvable for every ……..

20. Every nilpotent group is ……

21. Every finite direct product of solvable groups is ……..

22. Every subgroup of solvable group is ……

9.11 *ANSWERS*

Answer of self cheque question:

1. $n = 1, 2, 3, 4$ **2.** Solvable **3.** S_3

Answer of terminal question:

15. Nilpotent **16.** Not **17.** Nilpotent

18. Nilpotent **19.** $n \geq 5$ **20.** Solvable

21. Solvable **22.** Solvable

BLOCK IV

COMPOSITION SERIES, JORDAN HOLDER THEOREM AND SOLVABLE GROUP

UNIT-10: RING AND IDEALS

CONTENTS:

10.1 *INTRODUCTION*

In algebra, the study of rings is known as ring theory. In rings, addition and multiplication are defined and have characteristics in common with those of the operations specified for integers. Ring theory explores the structure of rings, their representations, or in other words, modules, special classes of rings (such as group rings, division rings), as well as a variety of properties that have proven useful both for the theory's own purposes and for its practical applications, such as homological properties and polynomial identities. Rings that are commutative are significantly easier to understand than those that are not.

Commutative ring theory, often known as commutative algebra, is a significant branch of modern mathematics that has its roots in algebraic geometry and algebraic number theory, which offer several natural instances of commutative rings. The relationship between these three disciplines

algebraic geometry, algebraic number theory, and commutative algebra is so close that it is sometimes impossible to determine which discipline a given result belongs to. A basic theorem for algebraic geometry is, for instance, Hilbert's Nullstellensatz, which is formulated and proven in terms of commutative algebra.

Noncommutative rings have a very distinct character since they have a greater potential for strange behaviour. Although the theory has grown on its own, a relatively recent tendency has attempted to mirror the commutative growth by geometrically modelling the theory of some classes of noncommutative rings as if they were rings of functions on (inexistent) "noncommutative spaces." With the advancement of noncommutative geometry and the discovery of quantum groups, this movement began in the 1980s. Noncommutative rings, particularly noncommutative Noetherian rings, have been better understood as a result.

An ideal of a ring in mathematics, and more specifically in ring theory, is a unique subset of its constituent parts. Certain subsets of the integers, such as the even numbers or the multiples of 3, are generalized by ideals. The defining characteristics of an ideal are closure and absorption: adding and subtracting even numbers maintains evenness, and multiplication an even number by any integer (even or odd) yields an even number. Similar to how a normal subgroup may be used to create a quotient group in group theory, an ideal can be used to create a quotient ring.

The ideals are the non-negative integers that correspond one-to-one with the integers; each ideal in this ring is a main ideal made up of multiples of a single non-negative number. However, in other rings, the ideals might not exactly match the ring components, and when certain integer qualities are generalized to rings, they tend to attach to the ideals rather than the ring components more naturally. For instance, the Chinese remainder theorem may be used to ideals and the prime ideals of a ring are comparable to prime integers. The ideals of a Dedekind domain, a significant type of ring in number theory, have a variant of unique prime factorization.

10.2 *OBJECTIVES*

The study of rings is a deep and multifaceted field with applications in various areas of mathematics and beyond, the importance of ideals in the study of rings and algebraic structures. Ideals provide a powerful framework for understanding the algebraic properties of rings and their connections to various mathematical fields.

10.3 *RING*

Let R be a non empty set and $a, b, c \in R$ be arbitrary.The set R with two binary operations addition and multiplication is called a ring if the following conditions are satisfied:

i. $(R, +)$ is an abelian group.

ii. $(R, .)$ is semi group.

iii. Distributive laws holds, i.e.,

$$a(b + c) = ab + ac \quad \text{[Right dstributive law]}$$

$$(b + ca)a = ba + ca \quad \text{[Left DISTRIBUTIVE law]}$$

10.4 *RING WITH UNITY*

A ring having multiplicative identity element is called Ring with Unity or Ring with identity element.

10.5 *COMMUTATIVE RING*

A ring for which multiplicative is commutative is called commutative ring.

Example:

1. $(Z, +, .)$ is a ring. This ring is called ring of integers.
2. $(mZ, +, .)$ is a ring, m being fixed integer. This ring is Commutative ring.
3. $(R, +, .)$ is a ring. This ring is called ring of real numbers.This ring is a commutative ring with unity element.
4. $(Q, +, .)$ is a commutative ring. This ring is called ring of rational numbers.

10.6 *BOOLEAN RING*

A ring $(R, +, .)$ is called Boolean ring if all elements are indempotent.i.e.,

$$a.a = a, i.e., a^2 = a \; \forall a \in R.$$

10.7 *p- RING*

A ring $(R, +, .)$ is called p-ring if

$$a^p = a \;\; and \; pa = 0 \forall a \in R.$$

Similarly we define 2-ring.

10.8 *ZERO DIVISOR*

The non zero elements a,b of a ring R are knows as proper divisors of zero or zero divisors if $ab = 0$ or $ba = 0$.

Example:

1. The ring has matrices has zero divisors, for example if

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0, & 0 \\ 1 & 1 \end{bmatrix}$$

Then

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

Hence the ring $R = \{0,1,2,3,4,5,6,7\}$ of matrices has zero divisors.

2. The rings of a number do not have zero divisors. For∃ no two non-zero numbers such that their product is zero.

10.9 *RING WITHOUT ZERO DIVISORS*

A ring is called without zero divisors if product of two non-zero elements of R is not zero if $ab = 0$ where $a, b \in R$, $a = 0$ or $b = 0$ both $a = 0$ and $b = 0$.

If we say that R is aring with zero divisors $\{a \neq 0\ b \neq 0\ then\ ab = 0\}$

10.10 *CHARACTERISTIC OF A RING*

The characteristic of a ring R is explained as the smallest positive in integer$n$. s.t. $na = 0 \forall a \in R$. If their exist no positive integer, then R is called characteristic zero. Therefore R is of characteristic zero if $na \neq 0 \forall a \in R$ and for any positive integer$n$.

Theorem 1: (Elementary properties of ring) If a, b, c are arbitrary elements of a ring R, then Prove that.

i. $a0 = 0a = 0$

Solution: Let

$$0 + 0 = 0$$

$$a(0 + 0) = a0 \qquad \text{by left distribution law}$$

$$a0 + a0 = a0$$

$$a0 + a0 = a0 + 0 \quad as\ x + 0 = x$$

Now we get

$$a0 = 0 \qquad \ldots (1)$$

Again

$$0 + 0 = 0$$

$$(0 + 0)a = 0a \qquad \text{by right distribution law}$$

$$0a + 0a = 0a$$

$$0a + 0a = 0a + 0$$

By cancellation law in (R,+), we obtain

$$0a = 0 \qquad \ldots (2)$$

ii. $a(-b) = -(ab) = (-a)b$

Solution: From (1) and (2) ,we obtain the results

$$a(-b + b) = a(-b) + ab \qquad \text{For } -b + b = 0$$

$$a(0) = a(-b) + ab$$

$$0 = a(-b) + ab$$
$$a(-b) = -(ab) \quad \ldots(3)$$

Since the additive inverse of ab is a$a(-b)$

Similarly

$$(-a + a)b = b(-a) + ba$$
$$(-a + a) = 0 \text{ and } 0b = 0$$
$$0 = (-a)b + ba$$

Since the additive inverse of ab is a$(-a)b$.

$$-(ab) = (-a)b \quad \ldots(4)$$

From (3) and (4), we obtain

$$-(ab) = (-a)b = a(-b)$$

iii. $(-a)(-b) = ab$

Solution: Let $(-a)(-b) = -[a(-b)]$, by (ii)

$= -[-(ab)]$ again by (ii)

$= ab$ For – $(-x) = x \ \forall x \in R$.

iv.

Solution: $a(b - c) = a[b + (-c)]$

$= ab + a(-c)$

$= ab + [-ac]$

$= ab - ac$

v.

Solution: $(b - c)a = [b + (-c)]a$

$= ba + (-c)a$

$= ba + [-ca]$

$= ba - ca$

Theorem 2: If R is a ring with unity element 1, then
$(-1)a = -a = a(-1) \quad \forall a \in R$ and $(-1)(-1) = 1$.

Proof: $(-1 + 1)a = (-1)a + 1.a$

$0.a = (-1)a + 1.a$

$0 = (-1)a + a$

Since $(-1)a = -a$, [For $a + x = 0, a = -x$]

Again $a(-1 + 1) = a(-1) + a.1$

$a.0 = a(-1) + a.1$

$0 = a(-1) + a$

This implies $a(-1) = -a$ Also $(-1)a = -a$

$(-1)a = -a = a(-1)$

Now taking $a = -1$in above equation

$(-1)(-1) = (-1)(-1) = -(-1)$

$(-1)(-1) = -(-1) = 1$

For $-(-x) = x$ in additive group or $(-1)(-1) = 1$.

Theorem 3: A ring without zero divisors iff the cancellation laws hold in R.

Proof: Suppose R be a ring without zero divisors.

To prove that cancellation laws hold in R.

Since let $a, b, c \in R \ s.t. ab = ac \ and \ a \neq 0$.

Then $ab = ac \Rightarrow a(b - c) = 0$

Also $a \neq 0$ and R has no zero divisors.

Hence $b - c = 0 \Rightarrow b = c$

Thus $ab = ca, a \neq 0 \Rightarrow b = c$

Similarly we can show that $ba = ca, a \neq 0 \Rightarrow b = c$

Conversely, Let R be a ring s.t. cancellation laws hold in R.

To prove that R has no zero divisors.

Suppose the contrary. Then R has zero divisors, then

$\exists a, b \in R\ s.t.\ ab = 0$ and $a, b \neq 0$

$ab = 0, a \neq 0 \Rightarrow ab = a.0$ for a.0=0 $\Rightarrow b = 0$. By left cancellation law

A Contradiction, for $b \neq 0$

Similarly$ab = 0, b \neq 0 \Rightarrow a = 0$. A Contradiction, for $a \neq 0$.

Theorem 4: If R is a Boolean ring then

(i) $2a = 0\ \forall\ a \in R$

(ii) $ab = ba\ \ i.e.\ R$ is commutative.

PROOF:

(i) Suppose

$$2a = a + a$$

$= (a + a)^2$ $\because R$ is Boolean ring, $x^2 = x\ \forall\ x \in R$

$= (a + a)(a + a)$

$= a^2 + a^2 + a^2 + a^2$

$= 4a^2$

$2a = 4a$ $a^2 = a$ (R is Boolean)

$4a - 2a = 0$

$2a = 0$ or $a + a = 0$.

(ii) Now

$(a + b)^2 = a + b$ $\because R$ is Boolean

$(a + b)(a + b) = a + b$

$a(a + b) + a(a + b) = a + b$

$(a^2 + ab) + (ba + b^2) = a + b$ By distributive law

$(a + ab) + (ba + b) = a + b$ $\because\ a^2 = a, b^2 = b$

Finally, $(a + b) + (ab + ba) = a + b$

$(a + b) + (ab + ba) = a + b + 0$.

Left cancellation law of addition in R gives$ab + ba = 0$.

Taking$ab = a'$, $ba = b'$, we get

$a' + b' = 0$

$a' + b' = 0 \Longrightarrow a' + b' = 0 = a' + a'$

$\Longrightarrow a' + b' = a' + a'$

$\Longrightarrow b' = a'$, by left cancellation law

$\Longrightarrow ba = ab.$

Theorem 5: If R is any ring with identity 1, show that R has positive characteristic n iff n is the at least positive integer for which$n\,.1 = 0$, 0 being additive identity of R.

Proof: Let R be a ring with unity element e.

$o(e) = 0 \Longrightarrow$ characteristic of R is 0.

Suppose $o(e) = n = a$ finite number so that n is at least positive integer s.t. $ne = 0$. Let a be any element of R. Then

$na = n(ea)$. For $ea = a = ae$.

$(ne)a = 0a = 0$.

Thus n is the least positive integer s.t. $na = 0$.

This proves that the characteristic of R is n.

SOLVED EXAMPLE

Example 1: Let a and b be arbitrary elements of a ring R whose characteristic is two and $ab = ba$.

Then prove that, $(a + b)^2 = a^2 + b^2 = (a - b)^2$

Solution: Suppose $ab = ba = x \in R$

The characteristic of R is two $\Rightarrow 2x = 0 \ \forall x \in R$

$$\Rightarrow x + x = 0$$

$$(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b)$$

$$= a^2 + ab + ba + b^2 = a^2 + (x + x) + b^2 = a^2 + 0 + b^2$$

$$= a^2 + b^2$$

$$(a - b)^2 = (a - b)(a - b) = a(a - b) - b(a - b)$$

$$= a^2 - ab - ba + b^2 = a^2 - (x + x) + b^2 = a^2 - 0 + b^2$$

$$= a^2 + b^2$$

Hence, $(a + b)^2 = a^2 + b^2 = (a - b)^2$

Example 2: If any element a has the multiplicative inverse, then a cannot be a divisor of zero, where the underlying set of a ring.

Solution: Suppose let R be a ring and $a \in R$ s.t. a has the inverse $a^{-1} \in R$ so $a \neq 0$

To prove that a is not zero divisor of zero. Suppose not then

a is divisor of zero so $\exists$ the element $b \in R \quad s.t.\ b \neq 0$ and $ab = 0$.

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = 0$$

$$\Rightarrow 1b = 0 \Rightarrow b = 0$$

Contrary$b \neq 0$. Hence required the solution.

10.11 *SUBRING*

Let R be a ring. A non empty subset s of the set R is said to be a subring of R if S is closed under addition and multiplication in R and S itself is a ring for those operations.

iff S is closed for compositions in R

iff $\forall\ a, b \in S \Longrightarrow a + b \in S, ab \in S$.

Theorem 1: The necessary and sufficient conditions for a non empty subset S of a ring R to be a subring of R are (i) a,b ∈ S ⟹ a-b∈S. (ii)) a,b ∈ S ⟹ ab∈ S.

Proof: Let S be a Subring of a ring R so that S itself is a ring.

To prove that

(i) a,b ϵ S ⟹ a-b ∈ S. (ii) a,b ϵS ⟹ ab ∈S.

S is ring ⟹ (S, +) is an abelian group.

Hence a,b ϵ S ⟹ a, -b ∈ S [Each elemant of S has additive inverse in S]

⟹ a+(-b)∈ S [S is closed w.r.t.(+)]

⟹ a-b ∈ S. Hence the condition (i)

Again S is ring ⟹(S, ·) is a semi group

⟹ S is closed w.r.t. multiplication

⟹ab∈S ∀ a,b∈S. Hence the condition (ii)

Conversely, let S is non empty subset of R s.t. the conditions (i) and (ii) hold.

To prove that S is a subring of R, it is enough to show that S is a ring.

The condition (i) says that

a,a ∈ S ⟹ a-a ∈S ⟹0 ∈S.

Again 0∈ S, a∈S ⟹ 0-a ∈S ⟹-a∈S.

i.e. a ∈ S ⟹-a ∈ S.

Consequently, a, b ∈S ⟹a, -b ∈S

⟹a-(-b) ∈S by condition (i)

⟹ a+b ∈S

a,b∈ S⟹ a,b∈ R

⟹a+b= b+a. Fot (R, +) is a abelian group.

Similarly, we can show that

a+ (b+c) = (a+b)+c ∀ a,b, c ∈S.

Hence the above facts prove that (S, +) is an abelian group. Associatively of multiplication over addition holds in S. Since they hold in R. Finally we have show that (S, +, ·) is a ring.

Theorem 2: The intersection of two subring is again a subring.

Proof: Let S_1 and S_2 be two subring of ring R.

Since 0∈ $S_1$and 0∈ S_2 at least 0∈ $S_1 \cap S_2$. Therefore $S_1 \cap S_2$ is non-empty.

Let a,b ∈ $S_1 \cap S_2$, then

$a \in S_1 \cap S_2 \Rightarrow a \in S_1$ and $a \in S_2$

and $b \in S_1 \cap S_2 \Rightarrow b \in S_1$and $b \in S_2$.

But S_1 and S_2 are subring of R, therefore

$a, b \in S_1 \Rightarrow a-b \in S_1$ and $ab \in S_1$

and $a, b \in S_2 \Rightarrow a-b \in S_2$ and $ab \in S_2$.

Consequently, $a,b \in S_1 \cap S_2 \Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$.

Hence $S_1 \cap S_2$ is a subring of R.

10.12 *PROPER AND IMPROPER SUBRING*

If R is any ring, then {0} and R are always subring of R. These are said to be improper subrings. The subrings of R other than these two, if any, are said to be proper subrings of R.

Example:

(i) The ring of Gaussian integers is a subring of ring of complex numbers.

(ii) The ring of rational numbers is a subring of ring of real numbers.

The ring of integers is a subring of a ring of rational numbers.

10.13 *IDEALS*

A non empty Subset S of a ring R is called a **left ideal** of R if:

(i) S is additive Subgroup of R.

(ii) ∀ r∈ R, ∈ s∈ S⟹ rs∈ S.

A non empty subset S of a ring R is called a **right ideal** of R if:

(i) S is additive subgroup of R.

(ii) ∀ r∈R, ∀ s∈S ⟹ rs∈ S.

A non empty subset of a ring R is called an **ideal** or two sides ideal if it is both **left ideal** and **right ideal**, i.e. if:

(i) S is additive Subgroup of R.

(ii) $\forall$ r$\in$ R, $\forall$ s$\in$ S $\Longrightarrow$ rs $\in$S, sr $\in$S.

Example:

(i) The subring of even integers is an ideal of ring integers.

(ii) The set $\{mx: x \in Z\}$ is an ideal of the ring of integers. M being any fixed integer.

(iii) If R is a ring, then the set $\{x \in R: ax = 0\}$ is a **right ideal** of R. a being any fixed element of R.

(iv) If R is a ring, then the set $\{x \in R: xa = 0\}$ is a **left ideal** of R. a being any fixed element of R.

10.14 *IMPROPER AND PROPER IDEALS*

Let $(R, +, \cdot)$ be a ring. The ideal R and $\{0\}$ are called improper or trivial ideals of R. Any ideal other than these two ideals is called a proper (or non trivial) ideal of R.

10.15 *PRINCIPAL IDEAL*

A **left ideal** generated by single element a $\in$R is also called **principal left ideal** of R. The set

$$\{ra + ma: r \in R, m \in Z\}$$

is a **principal left ideal** of R. a being fixed element of R.

If R is a ring with unity element e, and a $\in$R, then Ra is **principal left ideal** of R.

A **right ideal** generated by single element a $\in$R is also called **right principal ideal** of R. The set

$$\{ar + ma: r \in R, m \in Z\}$$

is a **principal right ideal** of R. a being fixed element of R.

If R is a ring with unity element e, then aR is defined as right ideal generated by an element a $\in$R. aR is also defined as **principal right ideal** of R.

An ideal of a ring R is called **principal ideal** of R, if it is generated by single element of R.

That is to say, the set

$$\{ra + as + ma: r, s \in R, m \in Z\}$$

is a principal ideal of R, generated by single element a$\in$ R. This set is also called **ideal** generated by an element a$\in$ R. The expression for principal ideal can be simplified if R is a ring with unity element e.

In this case

$$ra + as + ma = ra + as + m(ea). \quad \text{For } a = ea$$
$$= ra + as + r'a, \text{ where } r' = me \in R$$
$$= (r + r')a + as$$

$=s'a + as$, where $s' = r + r' \in R$.

Hence a principal ideal of R is the set $\{s'a + as : s, s' \in R\}$ if R is a ring with unity element e.

10.16 *PRINCIPAL IDEAL RING*

A commutative ring with unity for which every ideal is a principal ideal is said to be a principal ideal ring.

10.17 *PRIME IDEAL*

Let R be a commutative ring. An ideal S of ring R is said to be a prime ideal of R if

$ab \in S \Rightarrow a \in$ S or $b \in S$.

If an ideal S of a ring R is generated by an element $a \in R$, then we write

$S = (a)$.

Similarly if an ideal S of a ring R is generated by elements $a, b \in R$, then we write

$S = (\{a, b\})$.

Example: The ideal $S = \{3r : r \in Z\}$ is prime.

Solution: Let $S = \{3r : r \in Z\}$ is prime ideal of R generated by 3 and we also write $S = (3)$.

Here $ab \in S \Longrightarrow 3|ab$. Also 3 is prime

$\Longrightarrow 3|a$ and $3|b$

$\Longrightarrow a \in S$ or $b \in S$

$\Longrightarrow S$ is prime

Theorem: If R is a commutative ring with unity and $a \in R$, then $Ra = \{ra : r \in R\}$ is a principal ideal of R, generated by a.

Proof: Let R be a commutative ring with unity element e and $a \in R$,

$$Ra = \{ra : r \in R\}$$

(i) To prove that Ra is ideal of R.

(ii) To prove that Ra = (a), i.e., the ideal Ra is generated by a.

Let S be an ideal generated by an element of a, so that $S = (a)$

$$S = (a) = \{ra + as + ma : r, s \in R, m \in Z\}$$

$ra + as + ma = ra + sa + ma$. For R is commutative.

$= ra + sa + (me)a$.

$= ra + sa + r'a$, where $me = r' \in R$

$= (r + s + r')a$

$= xa$, where $x = r + s + r' \in R$.

Finally, $ra + as + ma = xa, x \in R$.

Hence, $S = \{xa: x \in R\} = Ra$.

But $S = (a)$.

Hence $Ra = (a)$.

Now we have shown that Ra is an ideal generated by a single element a. By definition, Ra is a principal ideal of R.

10.18 *QUOTIENT RING*

Let R be a ring and S be an ideal of R. Let R/S denote the family of cosets of S in R, i.e.,

$$\frac{R}{S} = \{S + a: a \in R\}.$$

Let $S + a, S + b$ be arbitrary elements of R/S. Define the operations of addition and multiplication on R/S as follows:

$$(S + a)(S + b) = S + (a + b)$$

$$(S + a)(S + b) = S + ab.$$

Then R/S is a ring w.r.t. these operations. This ring $(R/S, +, \cdot)$ is called **quotient ring or factor ring**.

Theorem: The intersection of two ideals is an ideal.

Proof:

(i) S_1 and S_2 both are additive subgroups of R.

(ii) $r \in R, a \in S_1 \Longrightarrow ra, ar \in S_1$

and $r \in R, a \in S_2 \Longrightarrow ra, ar \in S_2$.

To prove that $S_1 \cap S_2$ is an ideal of R. For this we have to prove the following:

(iii) $S_1 \cap S_2$ is additive subgroup of R.

(iv) $r \in R, a \in S_1 \cap S_2 \Longrightarrow ra, ar \in S_1 \cap S_2$

Evidently $(i) \Longrightarrow (iii)$

$r \in R, a \in S_1 \cap S_2 \Longrightarrow r \in R, a \in S_1$ and $a \in S_2$

$\Longrightarrow r \in R, a \in S_1$ and $r \in R, a \in S_2$

$\Longrightarrow ra, ar \in S_1$ and $ra, ar \in S_2$, by (ii)

$\Longrightarrow ra, ar \in S_1 \cap S_2 \Longrightarrow (iv)$.

Check your progress

Problem 1: Check that the singleton set $\{0\}$ is ring or not?

Problem 2: Check that the singleton set contain the identity element form a ring?

Problem 3: Check that the set $\{0,1\}$ is ring with unity or not?

10.19 *SUMMARY*

In this unit, we have studied the basic terminology used in ring theory. We have also read about the basic idea of ring with some theorems and examples. We have defined commutative and non commutative. In this unit first we have defined subring, Boolean ring, characteristic of ring with examples. After that we have described the definition of ideal, prime ideal, principal ideal and quotient ring with examples then important theorem related to these topic described. This unit is basic outlook of ring theory and concepts of this unit will be beneficial for the learners in the upcoming units.

10.20 *GLOSSARY*

- Ring
- Characteristic of ring
- Subring
- Ideal
- Principal ideal
- Quotient ring

10.21 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

10.22 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

10.23 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that set of integers is a commutating ring 'or' $(Z,+,.)$ is a commutative ring.

2. Prove that set of rational numbers is a commutative ring.

3. Prove that ring without zero divisors *iff* the cancellation laws hold in R

4. State and prove the necessary and sufficient condition for any subset of ring to be a subring.

5. Prove that set of rational numbers is a subring of set of real number.

6. Prove that subring of even integers is an ideal of ring of integers.

Short Answer Type Question:

7. If R is any ring with identity 1, then prove that R has positive characteristic n iff n is the at least positive integer for which $n.1 = 0$, 0 being additive identity of R.

8. In any ring (R) any element a has the multiplicative inverse, then prove that a cannot be a divisor of zero.

9. Prove that intersection of two subring of a ring is also a subring.

10. Prove that intersection of two ideal of a ring is also an ideal of ring.

11. Define the ring and subring with example.

12. Define the ideal, prime ideal and principal ideal with example.

13. Define proper and improper ideal with example.

14. Let a and b be arbitrary elements of a ring R whose characteristic is two and $ab = ba$. Then prove that,

$$(a+b)^2 = a^2 + b^2 = (a-b)^2$$

Fill in the blanks:

15. Intersection of two subring of any ring is also a …….

16. Intersection of two ideal of any ring is also an …….

17. Set of rational number is subring of set of ……..

18. A ring (R) without zero divisors *iff* the cancellation laws …….. in R.

19. Set of integers is a …….. ring with unity

10.24 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes **3.** Yes

Answer of terminal question:

15. Subring **16.** Ideal **17.** Real **18.** R **19.** Commutative

Unit-11: INTEGRAL DOMAIN AND FIELDS

CONTENT:

11.1 *INTRODUCTION*

In this unit we will learned about the more important tools used in the ring theory like integral domain, field and division ring or skew field. A field in mathematics is a set on which the operations addition, subtraction, multiplication, and division are defined and function in the same manner as they do for rational and real numbers. As a result, a field is a basic algebraic structure that is often utilised in number theory, algebra, and many other branches of mathematics.

The domains of rational numbers, real numbers, and complex numbers are the most well-known ones. Mathematicians frequently utilise and study a variety of different fields, notably in number theory and algebraic geometry, including fields of rational functions, algebraic function fields, algebraic number fields, and p-adic fields. On finite fields, or fields with a finite number of elements, the majority of cryptographic procedures are based.

The idea of a field extension expresses the relationship between two fields. The goal of the Galois theory, which Évariste Galois founded in the 1830s, is to comprehend the symmetries of field extensions. This theory demonstrates, among other things, that it is impossible to square a circle and trisect an angle with a compass and straightedge. Additionally, it demonstrates that quintic equations are typically algebraically intractable.

In many areas of mathematics, fields are fundamental concepts. This comprises many mathematical analysis disciplines that are based on fields with extra structure. Analysis's fundamental theorems rely on the real numbers' structural characteristics. What's more, any field may be utilised as the scalars for a vector space, which is the usual generic setting for linear algebra. In-depth research is done on number fields, the siblings of the subject of rational numbers. Geometric object attributes may be described with the use of function fields.

11.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the integral domain which is the extension of ring.
- Analyze about the field which further essential tool used is Linear Algebra.
- Memorized the concept of division ring or skew field.
- Implementation of the concept of integral domain, field and division ring or skew field.

11.3 *INTEGRAL DOMAIN*

Definition: Any ring (R) is called integral domain, if it satisfies the following conditions

(i) R should be commutative ring

(ii) R has unit element

(iii) R should be without zero divisors.

Some authors defining to integral domain in a different way that an integral domain is a commutative ring without zero divisors. They do not demand that an integral domain have the unit element without a doubt.

Set of integer (I) is a most common example of a ring to be an integral domain. We know that I is a commutative ring with unity and also I does not possess zero divisors. We know that if a, b are integers such that $ab = 0$, then either a or b must be zero.

The other rings which are examples of infinite integral domains are $(C,+,.),(Q,+,.),(R,+,.)$ and the example of finite integral domain is $(\{0,1,2,3,4\},+_5,\times_5)$.

Inversible elements in a ring with unity: In a ring (R) each element possess additive inverse. Therefore when we talking about inversible of an element, we only asking about invertiablity with respect to the operation multiplication. If R is a ring with unity, then an element $a \in R$ is called inversible, if there exist $b \in R$ such that $ab = 1 = ba$. Then we rewrite $b = a^{-1}$.

Examples (i): In the ring of integers 1 and -1 are the only two inversible elements.

(ii): In the set of $n \times n$ non singular matrices with real numbers as elements are the only inversible elements of the ring of all $n \times n$ matrices with elements as real numbers.

Theorem 1: A commutative ring R is an integral domain *iff* $\forall a,b,c \in R(a \neq 0)$

$$ab = ac \Rightarrow b = c$$

Proof: Let R is an integral domain.

Also let $ab = ac \ (a \neq 0)$

Then $ab - ac = 0$

$\Rightarrow a(b-c) = 0$

$\Rightarrow a = 0 \, or \, b - c = 0$

Since $a \neq 0$, we get $b = c$

Conversely, let the given condition holds good.

Let $a,b \in R$ be a arbitrary elements with $a \neq 0$.

Suppose $ab = 0$

Then $ab = a.0$

$\Rightarrow b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark: Any ring (R) is said to satisfy left cancellation law if $\forall a,b,c \in R(a \neq 0)$

$ab = ac \Rightarrow b = c$

Similarly we can talk of right cancellation law. It is to notify that cancellation is of only non zero elements.

11.4 *FIELD*

Definition: A ring (R) with at least two elements is called a field (F) if it satisfies following conditions,

(i) It should be commutative

(*ii*) It has unity

(*iii*) Each non-zero element possess multiplicative inverse.

For example, ring of rational numbers $(Q,+,.)$ is a field because it satisfies aforementioned following conditions. Similarly, rings of real numbers $(R,+,.)$ and complex numbers $(C,+,.)$ are also common example of fields.

$(\{0,1,2,3,4\},+_5,\times_5)$ is an example of finite fields

If $a, 0 \neq b$ are elements of a finite field F, then we shall often write

$ab^{-1} = \frac{a}{b} = b^{-1}a$. In a field F, we have

$$\frac{a}{b} + \frac{c}{d} = (ab^{-1}) + (cd^{-1}) = (bd^{-1})(bd)[(ab^{-1}) + (cd^{-1})]$$

$$= (bd^{-1})[(bd)(ab^{-1}) + (bd^{-1})(bd)(cd^{-1})] = (bd^{-1})(ad + bc) = \frac{ad + bc}{bd}$$

[Because in the field (F) multiplication is commutative]

Also $\frac{a}{b}\frac{c}{d} = (ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1} = \frac{ac}{bd}$.

11.4.1 *SUBFIELDS*

Definition: A non-empty subset K of a field F is said to be subfield if K is closed w.r.to. operation addition and multiplication in F and K itself is a field for these operation.

Conditions for a subfield: The necessary and sufficient condition for a non-empty subset K of field F to be subfield are

(*i*) $a \in K, b \in K \Rightarrow a - b \in K$

(*ii*) $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$

Proof: Necessary condition: Let the subset K of field F is itself a field.

$\Rightarrow K$ is a group w.r.to. addition i.e. for each $a, b \in K \Rightarrow a - b \in K$

Now each non-zero element of K possesses multiplicative inverse. Therefore $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$

Hence condition is necessary.

Sufficient condition: Suppose K is non-empty subset of F and satisfying the condition **(*i*)** and **(*ii*)**. As similar we have proved in case of subring that $(K,+)$ is abelian group, in similar we will prove (i) that $(K,+)$ is abelian group.

Now let a be any non-zero element of K. Then from (ii) we have

$$a \in K, 0 \neq a \in K \Rightarrow aa^{-1} \in K \Rightarrow 1 \in K$$

Now $1 \in K$, therefore again from (ii), we have

$1 \in K, 0 \neq a \in K \Rightarrow 1a^{-1} \in K \Rightarrow a^{-1} \in K$.

$\therefore$ Each non-zero element of K possesses multiplicative inverse.

Now let $a \in K$ and $0 \neq b \in K$. Then $b^{-1} \in K$. From (ii), we have

$a \in K, 0 \neq b^{-1} \in K \Rightarrow a(b^{-1})^{-1} \in K \Rightarrow ab \in K$

Also if $b = 0$, then $ab = 0$ and $0 \in K$

$\therefore ab \in K \; \forall \, a, b \in K$

Associativity of multiplication and distributivity of multiplication over addition must hold in K since they hold in F

11.5 *DIVISION RING AND SKEW FIELD*

Definition: A ring (R) with at least two elements is called a division ring or a skew field if is satisfies following conditions

(i) Has unity

(ii) Each non-zero element possesses its multiplicative inverse.

Thus a commutative division ring is a field.

A division ring is a field if it is also commutative but every field is also a division ring.

Theorem: Every field is an integral domain.

Proof: As we know that a field (F) is a commutative ring with unity, therefore to prove that every field is an integral domain we have only to prove that a field has no zero divisors.

Let a, b be elements of F with $a \neq 0$ such that $ab = 0$

Since $a \neq 0, a^{-1}$ exists and we have

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = 0$$

$$\Rightarrow 1b = 0 \qquad [\because a^{-1}a = 1]$$

$$\Rightarrow b = 0 \qquad [\because ab = b]$$

Similarly, let $ab = 0$ and $b \neq 0$

Since $b \neq 0, b^{-1}$ exists and we have

$$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$$

$\Rightarrow a(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0$

Hence in a field $ab = 0 \Rightarrow a = 0$ or $b = 0$. Since field has no zero divisors therefore every field is an integral domain.

The converse of this theorem is not true i.e., every integral domain is not a field. For example, ring of integer is an integral domain while it is not a field because only inversible element in the ring of integer are 1 and -1.

Note: In the field unity and zero are different elements i.e., $1 \neq 0$. Let a be any non-zero element of a field. Then a^{-1} exists and is also non-zero. For, $a^{-1} = 0 \Rightarrow aa^{-1} = a0 \Rightarrow 1 = 0 \Rightarrow a1 = a0 \Rightarrow a = 0$

This is a contradiction. Now, field has no zero divisors. Therefore, $1 = a^{-1}a \neq 0$.

Remarks: As we know field has no zero divisors. Therefore in the field product of two non-zero elements will again a non-zero element. Also each non-zero element and unit element possesses non-zero multiplicative inverse. Since multiplication is commutative as well as associative, therefore the non-zero elements of a field form abelian group w.r.to. multiplication.

Theorem 2: A skew field (D) has no zero divisors.

Proof: Let D be a skew-field. Then D is a ring with unit element 1 and each non-zero element of D possesses multiplicative inverse.

Let a, b be elements of D with $a \neq 0$ s.t. $ab = 0$

Since $a \neq 0, a^{-1}$ exists and we have

$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$

$\Rightarrow (a^{-1}a)b = 0 \Rightarrow 1b = 0 \Rightarrow b = 0$

Similarly, let $ab = 0$ with $b \neq 0$

Since $b \neq 0, b^{-1}$ exists and we have

$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$

$\Rightarrow a(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0$

Hence a skew field has no zero divisors.

Theorem 3: Every finite integral domain is a field '*OR*' A finite commutative ring without zero divisor is a field.

Proof: Let D be a finite commutative ring without zero divisor having n elements $a_1, a_2, ..., , a_n$. In order to prove that D is a field, we must produce an element $1 \in D$ such that $1a = a \; \forall \; a \in D$. Also we should show that for every element $a \neq 0 \in D$ there exist an element $b \in D$ such that $ba = 1$.

Let $a \neq 0 \in D$. Consider the n products $aa_1, aa_2, aa_3, ..., aa_n$.

All these are element of D. Also they are all distinct. For suppose that $aa_i = aa_j$ for $i \neq j$.

Then $a(a_i - a_j) = 0$ … (1)

Since D is without zero divisors and $a \neq 0$, therefore (1) implies

$a_i - a_j = 0 \Rightarrow a_i = a_j$, contradicting $i \neq j$.

$\therefore aa_1, aa_2, aa_3, ..., aa_n$ are all n distinct elements of D placed in some order. So one of these elements will be equal to a. Thus there exists an element, say, $1 \in D$ such that

$a1 = a = 1a$ [$\because D$ is commutative]

We shall show that this element 1 is the multiplicative identity of D. Let y be any element of D.

Then from the above discussion for some $x \in D$, we shall have $ax = y = xa$

Now, $1y = 1(ax)$ [$\because ax = y$]

$= (1a)x$

$= ax$ [$\because 1a = a$]

$= y$ [$\because ax = y$]

$= y1$ [$\because D$ is commutative]

Thus $1y = y = y1, \forall\, y \in D$. Therefore 1 is the unit element of the ring D.

Now $1 \in D$. Therefore from the above discussion one of the n products $aa_1, aa_2, aa_3, ..., aa_n$ will be equal to 1. Thus there exists an element, say $b \in D$ such that

$ab = 1 = ba$

$\therefore b$ is the multiplicative inverse of the non-zero element $a \in D$. Thus every non-zero element of D is inversible.

$\Rightarrow D$ is a field.

Definition: In a ring R any element a is said to be idempotent if $a^2 = a$. Any ring R will be called Boolean Ring if and only if all of its elements are idempotent i.e., if $a^2 = a \,\forall\, a \in R$.

Example 1: In the ring of set M of 2×2 matrices over the field of real number with respect to matrix addition and multiplication evaluate the following:

(*i*) Is it a commutating ring with unity elements?

(*ii*) Find the zero elements.

(*iii*) Does this ring possess zero divisors?

Solution: Let $A, B \in M$. Then $A + B \in M$ and $AB \in M$. Therefore M is closed with respect addition and multiplication of matrices.

As we know that both addition and multiplication of matrices are associative composition.

$\therefore A+(B+C)=(A+B)+C \forall A,B,C \in M$

and $A(BC)=(AB)C \ \forall A,B,C \in M$

Commutative property holds in addition of matrices. Hence, $\forall A,B \in M$, we have $A+B=B+A$.

If O be the null matrix of the type 2×2, then $O \in M$ and $O+A=A \forall A \in M$.

Further multiplication of matrices is distributes w.r.to. addition.

$\therefore A(B+C)=AB+AC$

and $(B+C)A=BA+CA \forall A,B,C \in M$

$\therefore M$ is a ring with respect to the given compositions.

Multiplication of matrices is not in general a commutative composition. For example, if

$$A=\begin{bmatrix}2 & 4\\ 3 & 5\end{bmatrix}, B=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$$

Then, $AB=\begin{bmatrix}2 & 8\\ 3 & 11\end{bmatrix}$ and $BA=\begin{bmatrix}8 & 14\\ 3 & 5\end{bmatrix}$

Thus $AB \neq BA$ and so the ring is a non-commutative ring

If I be the unit matrix of the type 2×2 i.e., $I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ then $I \in M$. Also we have

$AI=A=IA \forall A \in M$

$\therefore I$ is the multiplicative identity.

Thus the ring possesses the unit element and we have $I=1$ (the unit element of the ring)

The ring possesses zero divisors. For example if

$$A=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}, B=\begin{bmatrix}2 & 3\\ 0 & 0\end{bmatrix}, \text{then } AB=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring.

Example 2: DO the following sets from integral domains w.r.to. ordinary addition and multiplication? If so state if they are fields.

(*i*) The set of numbers of the form $b\sqrt{2}$ with b rational.

(*ii*) The set of even integers.

(*iii*) The set of positive integers.

Solution (*i*): Let $A=\{b\sqrt{2}: b \in Q\}$.

We have $3\sqrt{2} \in A$ and $5\sqrt{2} \in A$. Then $(3\sqrt{2})(5\sqrt{2})=30$. Now 30 can not be put in the form $b\sqrt{2}$ where b is rational number. Therefore $30 \notin A$. Thus A is not closed with respect to multiplication. Therefore the question of A becoming a ring does not arises.

(*ii*): Let R be set of all even integers. Then R is a ring with respect to addition and multiplication of integers. Additionally, the composition of multiplication is commutative. Since the product of two non-zero even integers cannot equal zero, which is the zero element of this ring, R has no zero divisors. Since the integer $1 \notin R,$ therefore R is a ring without unity. If the presence of the unit clement is not a requirement for an integral domain, then R will be one. However, since the multiplicative identity does not exist, R is not a field.

(*iii*): N should be the collection of positive integers. The additive identity does not exist since the number $0 \notin N$. N won't be a ring, then.

Example 3: Show that collection of numbers of the form $a + b\sqrt{2}$, with a and b as rational numbers is a field.

Solution: Let $R = \{a + b\sqrt{2} : a, b \in Q\}$

Let $a_1 + b_1\sqrt{2} \in R$ and $a_2 + b_2\sqrt{2} \in R$ where $a_1, b_1, a_2, b_2 \in Q$

We have $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in R$. Since $(a_1 + a_2), (b_1 + b_2) \in Q$

Also $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in R$.

Since $a_1a_2 + 2b_1b_2, a_1b_2 + a_2b_1 \in Q$

Thus R is closed w.r.to. addition and multiplication.

We know that addition and multiplication are both associative and commutative compositions in the set of real numbers since all the components of R are real numbers.

Further we have $0 + 0\sqrt{2} \in R$ since $0 \in Q$.

If $a + b\sqrt{2} \in R$, then

$0 + 0\sqrt{2} + (a + b\sqrt{2}) = (0 + a) + (0 + b)\sqrt{2} = a + b\sqrt{2}$

$\therefore$ $0 + 0\sqrt{2}$ is the additive identity.

Now again if $a + b\sqrt{2} \in R$, then $(-a) + (-b)\sqrt{2} \in R$ and we have

$[(-a) + (-b)\sqrt{2}] + [a + b\sqrt{2}] = 0 + 0\sqrt{2}$

$\therefore$ each element of R posses its own additive inverse.

Since multiplication is distributive w.r.to. addition in the set of real number.

Again $1 + 0\sqrt{2} \in R$ and we have

$(1 + 0\sqrt{2})(a + b\sqrt{2}) = a + b\sqrt{2} = (a + b\sqrt{2})(1 + 0\sqrt{2}) \in R$

So, $\left(1+0\sqrt{2}\right)$ is the multiplicative identity. Thus R is commutative ring with unity and the zero element of the ring is $0+0\sqrt{2}$ and $1+0\sqrt{2}$ is the unit element. If each non-zero element of R has a multiplicative inverse, then R will now be a field.

Let $a+b\sqrt{2}\neq 0+0\sqrt{2}$ be any element of this ring i.e., one of the element a and b is not zero.

Then $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}$

$=\left(\dfrac{a}{a^2-2b^2}\right)+\left(-\dfrac{b}{a^2-2b^2}\right)\sqrt{2}$

Now if a, b are rational numbers, then we can have $a^2=2b^2$ only if $a=0,b=0$. As we know that at least one of the rational numbers a and b is not 0. There we cannot have $a^2=2b^2$ i.e., $a^2-2b^2=0$.

$\therefore$ Both numbers $\dfrac{a}{a^2-2b^2}$ and $-\dfrac{b}{a^2-2b^2}$ are rational number and not both of them are zero.

$\therefore\left(\dfrac{a}{a^2-2b^2}\right)+\left(--\dfrac{b}{a^2-2b^2}\right)\sqrt{2}$ is non-zero multiplicative inverse of $a+b\sqrt{2}$. Hence the given system is a field.

Example 4: Give an example of an infinite commutative ring without zero divisors which is not a field.

Solution: Let Z be the set of integers. Then $(Z,+,.)$ is an infinite commutating ring without zero divisors and is not a field.

Example 5: If $(R,+,.)$ be a ring with n elements, $n>2$ with no zero divisors, show that R is a division ring.

Solution: Let R be a finite consisting of n elements, where $n\geq 2$ s.t., R has no divisor of zero.

To prove that R is a division ring we have enough to prove that.

(i) R has a unit element 1.

(ii) Every non-zero element of R has multiplicative inverse in R.

(i) Prove of (i) is the part of Theorem 3.

(ii) $1\in R\Rightarrow \exists\, a\, x_j\in R$ s.t. $a\, x_j=1, 1\leq j\leq n$

$\Rightarrow a$ is left inverse of x_j in R.

But left inverse = Right inverse.

$\Rightarrow a$ is the multiplicative inverse of x_j in R

Theorem 4: In the ordered integral domain D, the unity element is a positive element of D.

Proof: Let P be the collection of positive elements of integral domain D. We have to prove that $1 \in P$, for it we assume that $1 \notin P$.

Since $1 \notin P$, $1 \neq 0 \Rightarrow -1 \in P$ [By definition of P]

$\Rightarrow (-1)(-1) \in P$

$\Rightarrow 1 \in P$, which is a contradiction.

Hence the unity element is positive element of D.

Theorem 5: The field $(I_p, +_p, \times_p)$ is not ordered, where $I_p = \{0,1,2,..., p-1\}$ and $p =$ prime.

Proof: To prove $(I_p, +_p, \times_p)$ is not ordered.

Suppose the contrary. Then $(I_p, +_p, \times_p)$ is ordered. Let P be the set of positive element of I_p. Since additive identity of I_p is '0'. By definition of P, $1 \in I_P$

$\Rightarrow$only one of the following is true:

$1 = 0, 1 \in P$ or additive inverse of $1 \in P$.

Evidently $1 \neq 0$. Hence $1 \in P$ or additive inverse of $1 \in P$. Since P is closed w.r.to $+_p$.

$\therefore 1 \in P \Rightarrow 1 +_p 1 \in P \Rightarrow 2 \in P \Rightarrow 2 +_p 1 \in P \Rightarrow 3 \in P$

Repeating this process, we find that $1 \in P \Rightarrow p-1 \in P$, i.e., $1 \in P$

$\Rightarrow$additive inverse of 1 belongs to P. Which is a contradiction.

For both the possibilities $1 \in P$, $p-1 \in P$ cannot holds simultaneously.

Here our initial assumption is wrong.

Therefore the required result follows.

Theorem 6: The set of complex number is not ordered integral domain.

Proof: Let C be the set of complex numbers. We know that $(C,+,.)$ is an integral domain. Let P be the set of positive element of C. Evidently $i \in C$ and $i \neq 0$.

Hence either $i \in P$ *or* $-i \in P$.

$i \in P \Rightarrow i.i \in P$, by definition of P

$\Rightarrow -1 \in P.$ For $i^2 = -1$.

A contradiction . For $-1 \in P$, by theorem 4.

$\therefore i \notin P$.

Again, $-i \in P \Rightarrow (-i)(-i) \in P \Rightarrow i^2 \in P \Rightarrow -1 \in P$.

Again we get a contradiction, $-i \notin P$.

Thus $i \neq 0, i \neq P, -i \notin P,$ i.e., any one of the following:

$i = 0, i \in P, -i \in P,$

does not hold. Hence C is not an ordered integral domain.

Theorem 7: The characteristic of a ring with unity is zero or $n > 0$ according as the unity element regarded as a member of additive group of R of order 0 or n.

OR

If R is any ring with identity 1, shows that R has positive characteristic n *iff* n is the least positive integer for which $n.1 = 0, 0$ being additive identity of R.

Proof: Let R be a ring with unity element e.

$O(e) = 0 \Rightarrow$ Characteristic of R is 0.

Suppose $O(e) = n = a$ finite number so that n is the least positive integer s.t. $ne = 0$. Let a be any element of R. Then

$na = n(ea).1$ For $ea = a = ae$

$= (ne)a = 0a = 0$

Thus n is the least positive integer s.t. $na = 0$. Hence the characteristics of R is n.

Theorem 8: Every finite integral domain D is of finite characteristics.

Proof: Let $(D, +, .)$ be a finite integral domain so that $(D, +, .)$ is a finite abelian group. We also known that characteristic of D is the order of unity element e of $(D, +, .)$.

$(D, +, .)$ is finite group $\Rightarrow O(e)$ finite.

$\Rightarrow$ Characteristic of D is finite.

Theorem 9(a): The characteristic of an integral domain is either 0 or a prime number according as the unity element *e* regarded as a member of the additive group of integral domain is of order 0 or a prime number.

Proof: (i) Let D be an integral domain. Then we prove that characteristic of D is either 0 or $p > 0$. [Proved in theorem 8]

(ii) If the characteristic is zero, the proof is complete.

Let the characteristic be $p > 0$. We have to show that p is a prime number.

Suppose p is not prime. Then *p* is composite integer. So we can write $p = p_1 p_2$: where $1 < p_1, p_2 < p$.

Characteristic of D is $p \Rightarrow$ order of e of the group $(D, +)$ is p. [e is unity element of D]

$\Rightarrow o(e) = p \Rightarrow pe = 0$

$\Rightarrow p_1 p_2 e = 0 \Rightarrow p_1(p_2 e) = 0$

$\Rightarrow (p_1 e)(p_2 e) = 0$

$\Rightarrow p_1 e = 0 \, or \, p_2 e = 0$ [For D has no zero divisor]

$\Rightarrow$ Characteristic of D is either p_1 or $p_2 < p$

$\Rightarrow Ch.D < p$. A contradiction.

Hence p is not composite.

Therefore p is prime.

Theorem 9(b): The characteristic of an integral domain is 0 or $n > 0$ according as the order of any non-zero element regarded as member of the additive group of the integral is either 0 or n.

Proof: Let $(D, +, .)$ be an integral domain and $a \in D$ and $a \neq 0$ and $O(a) = 0$ or n regarded as a member of $(D, +)$.

Then $na = 0, \; 0a = 0$ ...(1)

Aim: Characteristic of D is 0 or n.

For this have to show that $nx = 0 \; \forall \; x \in D$.

If $x \in D$, then (1) $\Rightarrow (na)x = 0 \Rightarrow (a + a + ... + a \, to \, n \, terms)\, x = 0$

$\Rightarrow (ax + ax + ... + a \, to \, n \, terms) = 0$

$\Rightarrow a(x + x + ... to \, n \, terms) = 0 \Rightarrow a(nx) = 0, a \neq 0$

$\Rightarrow nx = 0$ as D is free from zero divisors. Hence n is the least positive integer, according to (1).

Example 6: If there exist a positive integer m such that $ma = 0 \, \forall \, a \in F$, then show that m is a prime. What is this integer? F being a field.

Answer: Let F be a field and $a \in F$ be arbitrary. Also let

$ma = 0$ …(1)

where m is a positive integer. Let e be the multiple identity of F.

Then $ae = ea = 0$

(1) $\Rightarrow m(ea) = 0 \Rightarrow (me)(a) = 0 \Rightarrow me = 0 \, or \, a = 0$

$\Rightarrow$ in particular $me = 0$ …(2)

For F has no divisor of zero

F is field $\Rightarrow F$ is integral domain s.t. (2) holds.

It means that m is the characteristic of F. To prove that m is *prime*.

Now write proof of theorem 9a.

Theorem 10: Each non-zero element of an integral domain D, regarded as an element of the additive group D, is of the same order.

Proof: Let a, b be arbitrary non-zero elements of an integral domain D s.t. $a \neq b$.

Let $O(a) = n, O(b) = m$, where a, b are regarded as element of $(D, +)$ so that $na = 0, mb = 0$,

D is an integral domain $\Rightarrow D$ has no zero divisors.

$\Rightarrow$ cancellation law hold in D.

$na = 0 \Rightarrow a + a + ...upto\, n\, terms = 0$

$\Rightarrow b(a + a + ...upto\, n\, terms) = b.0 = 0$

$\Rightarrow ba + ba + ...upto\, n\, terms = 0$

$\Rightarrow n(ba) = 0 \Rightarrow (nb)a = 0 = 0a \Rightarrow (nb)a = 0a$

$\Rightarrow nb = 0$, by cancellation law

$\Rightarrow O(b) \leq n \Rightarrow m \leq n.$ For $O(b) = m$

$mb = 0 \Rightarrow b + b + ...upto\, n\, terms = 0$

$\Rightarrow a(b + b + ...upto\, n\, terms) = a.0 = 0$

$\Rightarrow ab + ab + ...upto\, n\, terms = 0$

$\Rightarrow m(ab) = 0 = 0b$

$\Rightarrow (ma)b = 0b$. Also $b \neq 0$

$\Rightarrow ma = 0$, By cancellation law

$\Rightarrow O(a) \leq m \Rightarrow n \leq m$. For $O(a) = n$

Thus we have shown that $n \leq m, m \geq n$.

$\therefore m = n,$ i.e., $O(a) = O(b)$.

When considered as members of an additive group, any two non-zero components of D have the same order.

Therefore, when considered a member of $(D, +)$, every non-zero element of D is of the same order.

Example 7: Give an example of skew-field which is not field.

Solution: Let R be a set of matrices of the form,

$$A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

Where a and b are complex numbers.

Let $B = \begin{bmatrix} c & d \\ -\bar{d} & \bar{c} \end{bmatrix}$,

$C = \begin{bmatrix} p & q \\ -\bar{q} & \bar{p} \end{bmatrix}$ be any two member of R. Then

$$A + B = \begin{bmatrix} a+c & b+d \\ -(\bar{b}+\bar{d} & \bar{a}+\bar{c} \end{bmatrix}$$

$$AB = \begin{bmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -(\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \overline{ac} \end{bmatrix}$$

If we take $\alpha = a + c, \beta = b + d, \gamma = ac - b\bar{d}, \delta = ad + b\bar{c}$, then we have

$$A + B = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in R$$

$$AB = \begin{bmatrix} \gamma & \delta \\ -\bar{\delta} & -\bar{\gamma} \end{bmatrix} \in R$$

(*i*) $(R, +)$ is an abelian group.

Closure axiom: $A + B \in R$ (already proved)

Commutativity: $A + B = B + A$.

This flows from the fact that $a + b = b + a$

Existence of identity: $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$

is additive identity s.t. $A + O = O + A = A$

Associative law: $A + (B + C) = (A + B) + C$

It follows from the fact that

$$a + (b + c) = (a + b) + c$$

Existence of inverse: $-A = \begin{bmatrix} -a & -c \\ \bar{c} & -\bar{a} \end{bmatrix} \in R$

is inverse of A s.t. $A + (-A) = O$

(*ii*) $(R, .)$ is a group

Closure axioms: $AB \in R$ (already proved)

Existence of identity: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$ is identity s.t. $AI = IA = A$.

Associative law: $(AB)C = A(BC)$

For $(ab)c = a(bc)$

Existence of inverse: If $A \neq O$, then

$$A^{-1} = \frac{adjA}{|A|} = \frac{1}{(a\bar{a} + b\bar{b})}\begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} \in R$$

is inverse of A s.t. $AA^{-1} = A^{-1}A = I$

Commutative law: $AB = BA$ is not satisfied here.

For $BA = \begin{bmatrix} c & d \\ -\bar{d} & \bar{d} \end{bmatrix}\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$

$$= \begin{bmatrix} ac - \bar{b}d & bc - \bar{a}d \\ -a\bar{d} - \bar{b}\bar{c} & -b\bar{d} + \bar{a}\bar{c} \end{bmatrix} \neq BA, \text{ by (1)}$$

Or $BA \neq AB$

(*iii*) Distributive law: $A(B + C) = AB + AC$

$$(B + C)A = BA + CA$$

It is true in general in case of matrices.

These fact show that $(R, +, .)$ is askew field but not field.

Example 8: Prove that the set $I_7 = \{0, 1, 2, ..., 6\}$ forms a field w.r.t. addition and multiplication modulo 7.

Solution: Let $I_7 = \{0, 1, 2, ..., 6\}$.

Let $a, b, c \in I_7$

We define $a +_7 b = \begin{cases} a + b & if \ \ a + b < 7 \\ r & if \ \ a + b \geq 7 \end{cases}$

Where r is remainder when $a + b$ is divided by 7,

$\therefore \ \ 0 \leq r \leq 6$

Evidently, $a +_7 b \in I_7$

(*i*) First, we have to prove that $(I_7, +_7)$ is an abelian group.

Closure axioms: $a +_7 b \in I_7$ (already proved)

Existence of identity: $\exists 0 \in I_7$, called additive identity s.t.

$$a +_7 0 = 0 +_7 a = a$$

Commutative law: $a +_7 b = b +_7 a$.

This follow from the fact that, $a + b = b + a$

Associative law: $(a +_7 b) +_7 c = a +_7 (b +_7 c)$

Since $(a + b) + c = a + (b + c)$

Therefore each side leaves the same remainder when divided by 7.

$\therefore \quad (a + b) +_7 c = a +_7 (b + c)$

Or $\therefore \quad (a +_7 b) + c = a +_7 (b +_7 c)$

Existence of inverse: $\forall \quad a \in I_7, \exists$ its inverse

$(7 - a) \in I_7$ (if $a \neq 0$) s.t.

$(7 - a) +_7 a = a +_7 (7 - a) = 0$.

Inverse of 0 is 0 itself.

(ii) Write $I'_7 = \{1, 2, 3, ..., 6\} = I_7 - \{0\}$.

Let $a, b, c \in I'_7$. Define

$$a \times_7 b = \begin{cases} ab \ if \ \ ab \leq 7 \\ s \quad if \ \ ab \geq 7 \end{cases}$$

Where s is the remainder when ab is divisible by 7.

$$0 \leq s \leq 6$$

$s = 0 \Rightarrow ab$ is divisible by 7.

But 7 has divisor $\Rightarrow a$ or b is divisible by 7

$$\Rightarrow a \geq 7, b \geq 7.$$

A contradiction as $a, b < 7$.

$\therefore s \neq 0.$ Consequently $0 < s \leq 6$.

This $\Rightarrow s \in I'_7 \Rightarrow a \times_7 b \in I'_7$

Aim: Now we have to prove that $(I'_7, \times_7)$ is an abelian group.

Closure axioms: $a \times_7 b \in I'_7$ (already proved)

Commutative law: $a \times_7 b = b \times_7 a$

Associative law: $(a \times_7 b) \times_7 c = a \times_7 (b \times_7 c)$.

Since $(ab)c = a(bc)$

Existence of identity: $1 \in I_7'$ is identity element s.t.

$$1 \times_7 a = a \times_7 1 = a .$$

Existence of inverse: $\forall\, a \in I_7'$, we have its inverse $x \in I_7'$ s.t.

$$a \times_7 x = x \times_7 a = 1.$$

For the equation $ax \equiv 1 \pmod{p}$ has a solution x if p is prime.

[Inverse of 1, 2, 3, 4, 5, 6 are respectively 1, 4, 5, 2, 3, 6]

Thus $(I_7', \times_7)$ is an abelian group.

(*iii*) Distributive law: $a \times_7 (b +_7 c) = (a \times_7 b) +_7 (a \times_7 c)$

$$(b +_7 c) \times_7 a = (b \times_7 a) +_7 (c \times_7 a)$$

This follows from the fact that

$a(b+c) = ab + ac$ and $(b+c)a = ba + ca$

Above arguments lead to the fact that $(I_7, +_7, \times_7)$ is a field.

Similar example 9: Let p be a positive prime number. Prove that the set $I_p = \{0, 1, ..., p-1\}$ forms a field w.r.t. addition and multiplication modulo p '*OR*'Ring of integers modulo a prime number p, is a field.

Example 10: If $I_5 = \{0, 1, 2, 3, 4\}$ then prove that $(I_5, +_5, \times_5)$ is a field, where $+_5$ and $\times_5$ respectively denote addition and multiplication modulo 5.

Answer: The composition tables for two operations are given below:

(*i*) Closure axiom: From the two composition tables it is quite clear that all the entries in both composition tables belong to I_5. Hence I_5 is closed w.r.to. both operation

(*ii*) Commutative law: The entries in the 1st, 2nd, 3rd, 4th rows are coincident with the corresponding element of the 1st, 2nd, 3rd, 4th columns respectively relative to the both operations. Hence $+_5$ and $\times_5$ both are commutative in I_5.

(*iii*) Associative law: It is easy to verify that the associative law holds for $+_5$,

i.e., $a +_5 (b +_5 c) = (a +_5 b) +_5 c \quad \forall\, a, b, c \in I_5$.

Similarly, $a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c \quad \forall\, a, b, c \in I_5$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(*iv*) 0 is the additive identity and 1 is the multiplicative identity for I_5.

For $0 +_5 a = a \forall a \in I_5$

$1 \times_5 a = a \forall a \in I_5$ s.t. $a \neq 0$

This follows from the composition tables.

(*v*) Existence of inverse: The additive inverse of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively. The multiplicative inverses of non-zero elements 1, 2, 3, 4 are 1, 3, 2, 4 respectively.

(*vi*) Distributive law: Multiplication is distributive over addition, i.e.,

$a \times_5 (b +_5 c) = a \times_5 b +_5 a \times_5 c \quad \forall a, b, c \in I_5$

$(b +_5 c) \times_5 a = b \times_5 a +_5 a +_5 c \times_5 a \quad \forall a, b, c \in I_5$

For $a \times_5 (b +_5 c) = a \times_5 (b + c)$. For $b +_5 c = b + c \pmod 5$

$=$ least positive remainder when $a \times (b + c)$ is divided by 5.

$=$ least positive remainder when $ab + ac$ is divided by 5.

$= ab +_5 ac$

$= a \times_5 b +_5 a \times_5 c$. For $a \times_5 b \equiv a \times b \pmod 5$

In similar way, we can prove other distributive law.

Hence $(I_5, +_5, \times_5)$ is a field.

Example 10: The set of all residue classes modulo a positive integer p is an integral domain *iff* p is prime.

Solution: Let R denote the set of all residue classes modulo a positive integer p so that

$R = \{[x] : x = 0, 1, 2, 3, ..., p-1\}$

Then we know that R is a commutative ring with unity element [1], [0] being the zero element of R. Let $[a], [b] \in R$ be arbitrary so that

$0 \leq a, b \leq p-1$

R will be an integral domain iff it is free from zero divisors, i.e., iff

$[a][b]=[0]\Rightarrow[a]=[0]\ or\ [b]=0$

So we have to show that p is prime iff

$[a][b]=[0]\Rightarrow[a]=[0]\ or\ [b]=0$

(*i*) p is prime, $[a][b]=[0]\Rightarrow p$ is prime, $ab\equiv 0(\text{mod } p)$

$\Rightarrow a\equiv 0(\text{mod } p)$ or $b\equiv 0(\text{mod } p)$

$\Rightarrow[a]=[0]\ or\ [b]=[0]$ or $b\equiv 0(\text{mod } p)$

(*ii*) Conversely supplies,

$[a][b]=[0]\Rightarrow[a]=[0]\ or\ [b]=[0].$

Now we have to prove that p is prime. For it let p is of composite order.

If p is of composite order $\Rightarrow p$ is expressible as, $p=p_1p_2$, where $1<p_1, p_2<p$

$\Rightarrow[p]=[p_1.p_2],[p_1]\neq[0],[p_2]\neq[0]$

$\Rightarrow[p_1.p_2]=[0]$. For $[p]=[0]$

$\Rightarrow[p_1]=0\ or\ [p_2]=[0],$ by assumption.

Which is a contradiction.

For $[p_1]\neq 0$ and $[p_2]\neq[0].$

Which shows our assumption is wrong. Therefore p is prime.

Similar problem 11: The set of all integers modulo a positive integer p is an integral domain *iff* p is prime.

Hint: $(I_p,+_p,\times_p)$ is integral domain, where $I_p=\{0,1,2,3,...,p-1\}$.

Check your progress

Problem 1: Check $I_4=\{0,1,2,3\}$ is field or not?

Problem 2: Check that the set $\{0,1\}$ form a field?

Problem 2: Check that the singleton set $\{0\}$ form a field and why?

11.6 *SUMMARY*

In this unit, we have studied about the integral domain, field, division ring or skew field in a ring. Throughout the all units we have learned about the basic definitions and their related theorems and examples on these major topics. In many areas of mathematics, fields are fundamental concepts. This

comprises many mathematical analysis disciplines that are based on fields with extra structure. Analysis's fundamental theorems rely on the real numbers' structural characteristics. What's more, any field may be utilised as the scalars for a vector space, which is the usual generic setting for linear algebra. In-depth research is done on number fields, the siblings of the subject of rational numbers. Geometric object attributes may be described with the use of function fields. The overall summarization of this units are as follows:

- A nonzero commutative ring without any nonzero zero divisors is referred to as an integral domain.
- Having no nonzero zero divisors, an integral domain is a nonzero commutative ring.
- Every field is an integral domain.
- Every finite integral domain is field.

11.7 *GLOSSARY*

- **Integral Domain:** Any ring without zero divisor is called integral domain
- **Field:** A commutative ring with unity having each non-zero element possess its multiplicative inverse is called field.
- **Division ring:** A ring with unity having each non-zero element possess its multiplicative inverse is called division ring.

11.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

11.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

11.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Show that in an integral domain all non-zero elements generate additive cyclic groups of the same order which is equal to the characteristic of the integral domain.

2. Give without proof, an example of an integral domain which contains only five elements. Is this an ordered integral domain? Give reason?

3. Show that the matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, a, b real, forms a field.

4. Prove that a non-zero finite integral domain is a field.

5. Prove that $(I_7, +_7, \times_7)$ is a field, where $+_7$ and $\times_7$ respectively denote addition and multiplication modulo 5.

6. Give an example of skew-field which is not field.

7. Show that collection of numbers of the form $a + b\sqrt{2}$, with a and b as rational numbers is a field

Short Answer Type Question:

8. If D is a non-zero integral domain, then characteristic of D is either zero or a prime number.

9. The set of complex number is not ordered integral domain

10. Prove that a skew field has no zero divisor.

11. Write the definition of following with suitable example.

(*i*) Field

(*ii*) Integral domain

(*iii*) Skew-field

12. A commutative ring R is an integral domain *iff* $\forall\, a, b, c \in R (a \neq 0)$

$ab = ac \Rightarrow b = c$

Fill in the blanks:

13. A commutative R is an integral domain iff …….

14. Every field is an ……..

15. A skew field has no …….

16. Every finite integral domain is ……

17. The set of all residue classes modulo a positive integer p is an integral domain *iff* p is ……..

11.11 *ANSWERS*

Answer of self cheque question:

1. No 2. Yes **3.** No, because it does not contain unity element

Answer of terminal question:

13. Cancellation law holds **14.** Integral domain **15.** Zero divisor

16. Field **17.** Prime

Unit-12: UNIQUE FACTORIZATION DOMAIN, PRINCIPAL IDEAL DOMAIN, EUCLIDEAN DOMAIN

CONTENT:

12.1 *INTRODUCTION*

In this unit we will learn about the more important tool in ring theory is that isomorphic relation between two rings, ideals of the ring and their applications and theorems.

The existence of gcd, Euclid's Lemma and Unique Factorization Theorem in Z and in F[x], where F is a field, all are consequences of the Division Algorithm. In this unit, we consider integral

domains having a division algorithm. In this we will learn the fundamental theorem of arithmetic states that every integer n > 1 is a product of primes and this product is unique up to the order of the prime factors. Here we characterize the integral domains D such that every nonzero non unit element of D can be expressed as product of irreducible elements uniquely in some sense. We call such integral domains UFD. In a UFD, irreducible and prime elements are precisely the same. Thus every nonzero non unit element of a UFD is a product of prime elements also.

12.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the isomorphism of two rings.
- Analyze about the ideals of the ring.
- Memorized about the Euclidean domain (ED), principal ideal domain (PID) and unique factorization domain (UFD).
- Analyze the relation between ED, PID and UFD.

12.3 *ISOMORPHISM OF RINGS*

Definition: Any ring R is said to be isomorphic to other ring R' if there exists a one-one and onto mapping f from R to R' such that

(*i*) $f(a+b) = f(a) + f(b)$

(*ii*) $f(ab) = f(a)f(b) \forall a, b \in R$.

Also such a mapping f is said to be an isomorphism of R onto R'. Symbolically it is denoted as $R \cong R'$, also R is said to be isomorphic image of R'.

Note: The compositions in the two rings have been represented by the identical symbols in the aforementioned definition of ring isomorphism. The constituent parts of any composition are revealed to us by the elements. For example, $a, b \in R$. When we write $a+b, ab$ then the respective compositions are addition and multiplication of R. Again $f(a), f(b) \in R'$. When we write $f(a) + f(b), f(a)f(b)$ then the respective compositions are addition and multiplication of R'

Relation of isomorphism in the set of all rings.

We can demonstrate that the relation of isomorphism in the set of all rings is an equivalence relation, as we have done in groups. In order to ensure that rings of the same class are all isomorphic to one another and rings of other classes are not, the set of all rings will be divided into disjoint equivalence classes. One can say that any two rings in the same equivalence class are abstractly similar.

Properties of isomorphism of rings:

Theorem 1: If f is an isomorphism of a ring R onto a ring R', then

(*i*) The image of $0 \in R$ is $0 \in R'$ *i.e.*, the additive identity element of ring R map into additive identity of the ring R'.

(*ii*) The negative of the image of an element of R is that element's image of its negative i.e., $f(-a) = -f(a) \forall a \in R$.

(*iii*) If R is the commutative ring, then R' is also a commutative a commutative ring.

(*iv*) If R is without zero divisors, then R' is also without zero divisors.

(*v*) If R is with unit element, then R' is also with unit element.

(*vi*) If R is field, then R' is also a field.

(*vii*) If R is skew field, then R' is also a skew field.

Proof (*i*): Let $a \in R$. Then $f(a) \in R'$. Let $0'$ denote the zero element of R'. To prove that $f(0) = 0'$.

We have $f(a) + 0' = f(a) = f(a+0) = f(a) + f(0)$. By cancellation law for addition in R', we get from $f(a) + 0' = f(a) + f(0)$, the result that $0' = f(0)$.

(*ii*) We have $f(a) + f(-a) = f[a + (-a)] = f(0) = 0'$

$\therefore f(-a)$ is the additive inverse inverse of $f(a)$ in R'. Thus $f(a) = -f(-a)$

(*iii*) Let $f(a)$ and $f(b)$ be any two elements of R'. Then $a, b \in R$

We have $f(a)f(b) = f(ab) = f(ba)$ [R is commutative $\Rightarrow ab = ba$]

$= f(b)f(a)$.

$\therefore R'$ is also commutative.

(*iv*) We have $f(0) = 0'$. Also f is one-one. Therefore 0 is the only element of R whose f-image is $0'$

.

(*v*) Let 1 be the unit element of R. Then $f(1) \in R'$. If $f(a)$ is any element of R', we have

$f(1)f(a) = f(1a) = f(a)$ and $f(a)f(1) = f(a1) = f(a)$.

$\therefore f(1)$ is the unit element of R'.

(*vi*) R is commutative with unity if R is a field, and each non-zero element of R will have a multiplicative inverse. Now that this has been shown in (iii) and (v), R' will be commutative and possess the unit element *i.e.*, $f(1)$.

Let $f(a)$ be any non-zero element of R'. Then

$f(a) \neq 0' \Rightarrow a \neq 0 \Rightarrow a^{-1}$ exists.

Now $f(a^{-1}) \in R'$ and we have

$f(a^{-1})f(a) = f(a^{-1}a) = f(1)$ and $f(a)f(a^{-1}) = f(aa^{-1}) = f(1)$.

$\therefore f(a^{-1})$ is the multiplicative inverse of $f(a)$.

Hence R' is a field.

(*vii*) As shown in (v) R' will be with unit element i.e., $f(1)$ as shown in (vi) each non-zero element of R' will be inversible. Therefore R' is a skew-field.

Imbedding of a ring: A ring R is said to be imbedded in a ring R' if there is a subring S' of R' s.t. R is isomorphic to S'.

Any ring R is imbedded to other ring R' if there exists a one-one and onto mapping f from R to R' such that,

$f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b) \forall a, b \in R$.

Theorem 2: Any ring R without a unity element may be imbedded in a ring that contains a unity element.

Proof: Let R be any ring without unity element. Let Z is the ring of integers and $R' = R \times Z = \{(a, m) : a \in R, m \in Z\}$.

When appropriate binary operations have been specified in $R \times Z$, then it becomes a ring with a unity element containing a subring, isomorphic to R.

If (a, m) and (b, n) are any two elements of $R \times Z$, then we define addition in $R \times Z$ by the equation

$(a, m) + (b, n) = (a + b, m + n)$ …(1)

And multiplication in $R \times Z$ by the equation

$(a, m)(b, n) = (ab + na + mb, mn)$ … (2)

Since $a + b \in R$ and $m + n \in Z$, therefore $(a + b, m + n) \in R \times Z$. Thus $R \times Z$ is closed w. r. to addition. Further, $ab, na, mb \in R \Rightarrow ab + na + mb \in R$. Also $mn \in Z$. Therefore $(ab + na + mb, mn) \in R \times Z$ and $R \times Z$ is closed w. r. to. multiplication.

Now let $(a, m), (b, n), (c, p)$ be any element of $R \times Z$. Then we observe:

Associativity in addition: We have

$[(a, m) + (b, n)] + (c, p) = (a + b, m + n) + (c, p)$

$= ([a + b] + c, [m + n] + p) = (a + [b + c], m + [n + p])$

$= (a, m) + (b + c, n + p) = (a, m) + [(b, n) + (c, p)]$

Commutativity in addition: We have

$(a,m)+(b,n)=(a+b,m+n)$

$=(b+a,n+m)$ [$\because$ Commutativity holds in addition]

$=(b,n)+(a,m)$.

Existence of identity: We have $(0,0)\in R\times Z$. Here the first 0 is the zero element of R and the second 0 is the zero integer.

Since, $(0,0)+(a,m)=(0+a,0+m)=(a,m)$

$\therefore (0,0)$ is the additive identity.

Existence of inverse: If $(a,m)\in R\times Z$, then

$(-a,-m)\in R\times Z$ and we have

$(-a,-m)+(a,m)=(-a+a,-m+m)=(0,0)$.

$\therefore (-a,-m)$ is additive inverse of (a,m)

Associativity of multiplication: We have

$[(a,m)(b,n)](c,p)=(ab+na+mb,mn)(c,p)$

$=((ab+na+mb)c+p(ab+na+mb)+(mn)c,(mn)p)$

$=(abc+n(ac)+m(bc)+p(ab)+(pn)a+(pm)b+(mr)c,(mn)p)$

Also $(a,m)[(b,n)(c,p)]=(a,m)(bc+pb+nc,np)$

$=(a(bc+pb+nc)+(np)a+m(bc+pb+nc),m(np))$

$=(abc+a(pb)+a(nc)+(np)a+m(bc)+m(pb)+m(nc),(mn)p)$

$=(abc+a(pb)+a(nc)+(np)a+m(bc)+m(pb)+m(nc),(mn)p)$

$=(abc+p(ab)+n(ac)+(np)a+m(bc)+(mp)b+(mn)c,(mn)p).$

We see that, $(a,m)[(b,n)](c,p)=(a,m)[(b,n)(c,p)]$

Distributive law: We have

$(a,m)[(b,n)+(c,p)]=(a,m)(b+c,n+p)$

$=(a(b+c)+(n+p)a+m(b+c),m(n+p))$

$=(ab+ac+na+pa+mb+mc,mn+mp)$

$=(a,m)(b,n)+(a,m)(c,p)$

In a similar manner, we may demonstrate that the other distributive law is equally valid.

In light of the operations described on it, $R\times Z$ is a ring.

Existence of identity: We have

$(0,1)\in R\times Z$. If $(a,m)\in R\times Z$, then

$(0,1)(a,m)=(0a+m0+1a,1m)=(0+0+a,m)=(a,m)$

Also $(a,m)(0,1) = (a\,0 + 1a + m0, m1) = (0 + a + 0, m) = (a,m)$.

$\therefore (0,1)$ is the multiplicative identity. So, $R \times Z$ is a ring with unity element (0, 1).

Now consider the subset $S' = R \times \{0\}$ of $R \times Z$ which consists of all pairs of the form $(a,0)$. We shall show that $R \times \{0\}$ is a subring of $R \times Z$. Let $(a,0),(b,0)$ be any two elements of $R \times \{0\}$.

Then $(a,0) - (b,0) = (a,0) + (-b,-0) = (a-b,0) \in R \times \{0\}$.

Also, $(a,0)(b,0) = (ab + 0a + 0b, 00) = (ab + 0 + 0, 0) = (ab, 0) \in R \times \{0\}$.

$\therefore R \times \{0\}$ is a subring of $R \times Z$.

Finally we have to show that $R \cong R \times \{0\}$. Let ϕ be a mapping from R to $R \times \{0\}$ defined as

$\phi(a) = (a,0) \forall\, a \in R$.

ϕ **is one-one:** For it, let $\phi(a) = \phi(b) \Rightarrow (a,0) = (b,0) \Rightarrow a = b \Rightarrow \phi$ is one-one.

ϕ **is onto:** Let $(a,0) \in R \times \{0\}$. Then $a \in R$ and we have $\phi(a) = (a,0)$. Therefore ϕ is onto.

ϕ **preserves addition and multiplication:** If $a,b \in R$, then

$\phi(a+b) = (a+b,0) = (a,0) + (b,0) = \phi(a)\phi(b)$.

Hence ϕ preserve the composition. *i.e.,* $R \cong R \times \{0\}$.

12.4 *FIELD OF QUOTIENT*

Definition: If ring S has a subset S' such that ring R is isomorphic to ring S, then the two rings can be embedded.

We shall demonstrate that D can be embedded in a field F, i.e., there exists a field F that includes a subset D' isomorphic to D, if D is a commutative ring without zero divisors. The elements of D will be used to build a field F, and this field F will have a subset D' such that D and D' are isomorphic. The "field of quotients" of D, or simply the "quotient field" of D, is referred to as this field F.

We can claim that D and D' are abstractly the same since D is isomorphic onto D'. We can then state that the quotient field F of D is a field containing D if we identify D' with D. We will also see that the smallest field that contains D is F.

Construction of quotient field: The ring of integer I is well known to all of us. Additionally, the set of quotients of the components of I is the same as our familiar set Q of rational numbers.

Thus $Q=\left\{\frac{p}{q}: p \in I, 0 \neq q \in I\right\}$. Since set of rational numbers (Q) are $\ldots, \frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \ldots$ with the integers (I) $\ldots,-3,-2,-1,0,1,2,3, \ldots$ then $I \subseteq Q$. Also $(Q,+,.)$ is a field. It is the smallest field containing I. Also if $\frac{a}{b}$ and $\frac{c}{d} \in Q$, then we remember that

(i) $\frac{a}{b}=\frac{c}{d}$ *iff* $ad=bc$ (ii) $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ (iii) $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$

These facts serve as our inspiration as we move on with creating the quotient field of any integral domain. The following theorem applies.

Theorem 3: A commutative ring without zero divisors can be imbedded in a field.

OR

Each integral domain can be imbedded in a field.

OR

It is feasible to create a field F from the components of an integral domain D that has a subset D' that isomorphic to D.

Proof: Let us suppose that D is a commutative ring without zero divisors. Let D_0 be the collection of all non-zero elements of D. Let $S=D\times D_0$ i.e., let S be the set of all ordered pairs (a,b) where $a,b \in D$ and $b \neq 0$. Let us define a relation $(\sim)$ in S s.t.,

$(a,b) \sim (c,d)$ *iff* $ad=bc$. Now we have to show that this relation is an equivalence relation.

Reflexivity: As we know D is commutative, therefore $ab=ba \forall a,b \in D$

Thus, $(a,b) \sim (b,a) \forall (a,b) \in S$

Transitivity: Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

$\Rightarrow ad=bc$ and $cf=de$

$\therefore adf=bcf$ and $bcf=bde$.

$\therefore adf=bde$

$\Rightarrow adf=bde$ [$\because D$ is a commutative ring]

$\Rightarrow adf-bde=0 \Rightarrow (af-be)d=0$

$\Rightarrow af-be=0$ [$\because d \neq 0$ and D is without zero divisors]

$\Rightarrow af=be \Rightarrow (a,b) \sim (e,f)$.

$\Rightarrow$ given relation is an equivalence relation $\sim$ in S.

$\Rightarrow S$ can be partitioned into disjoint equivalence classes and we denote the equivalence classes containing (a,b) by $\frac{a}{b}$ and other notations are $\overline{(a,b)}$ or $[a,b]$.

Then $\frac{a}{b} = \{(c,d) \in S \mid (c,d) \sim (a,b)\}$.

Obviously, $\frac{a}{b} = \frac{c}{d}$ *iff* $(c,d) \sim (a,b)$ i.e., *iff* $ad = bc$

Also, $\frac{a}{b} = \frac{ax}{bx} \forall\, x \in D_0$. The reason is that $(a,b) \sim (ax,bx)$ since $abx = bax$.

These equivalence classes are quotients. Let F be the set of all such quotients i.e., $F = \left\{\frac{a}{b} : (a,b) \in S\right\}$

Now defines operations addition and multiplication in F as follows:

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}$

Since D is without zero, therefore $b \neq 0, d \neq 0 \Rightarrow bd \neq 0$. Since both the element $\frac{ad+bc}{bd}$ and $\frac{ac}{bd}$ are belongs to field. F is therefore closed in terms of addition and multiplication. Now, we'll demonstrate that addition and multiplication in F have clear definitions. For it we have to show that if,

$\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ and $\frac{a}{b}\frac{c}{d} = \frac{a'}{b'}\frac{c'}{d'}$

We have $\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = ba'$ and $\frac{c}{d} = \frac{c'}{d'} \Rightarrow cd' = dc'$

Now to show that $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, we are to show that

$\frac{ad+bc}{bd} = \frac{a'd' + b'c'}{b'd'}$ *i.e.*, $(ad+bc)b'd' = bd(a'd' + b'c')$.

Now $(ad+bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd'$

$= ba'dd' + bb'dc'$ $[\therefore ab' = ba'$ and $cd' = dc']$

$= bda'd' + bdb'c' = bd(a'd' + b'c')$, which was desired.

Again we have to show that $\frac{a}{b}\frac{c}{d} = \frac{a'}{b'}\frac{c'}{d'}$ we have to show

$\frac{ac}{bd} = \frac{a'c'}{b'd'}$ *i.e.*, $\therefore acb'd' = bda'c'$

Now $acb'd' = ab'cd' = ba'dc' = bda'c'$, which was desired.

Hence both operations addition and multiplication are well defined on F. Now we have that F is a field.

Associativity of addition: We have,

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+bde}{bdf}$$

$$=\frac{adf+bcf+bde}{bdf}=\frac{adf+b(cf+de)}{bdf}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

Commutativity in addition: We have

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}$$

Existence of identity: We have

$\frac{0}{a}\in F$ where $a\neq 0$. If $\frac{c}{d}$ is any element of F, then

$$\frac{0}{a}+\frac{c}{d}=\frac{0d+ac}{ad}=\frac{0d+ac}{ad}=\frac{ac}{ad}=\frac{c}{d} \qquad [\because acd=adc]$$

So, $\frac{0}{a}\in F$ is the identity element. It is also noted tthat,

$\frac{0}{a}=\frac{0}{b}\forall\, a,b\in D_0$. Also $\frac{c}{d}=\frac{0}{b} iff\ ca=d0$ *i.e.*, $c=0$

Existence of inverse: If $\frac{a}{b}\in F,$ then $\frac{-a}{b}\in F.$

Also we have, $\frac{-a}{b}+\frac{a}{b}=\frac{(-a)b+ba}{b^2}=\frac{0}{b^2}=\frac{0}{a} \qquad [\because 0a=b^2 0]$

$\because \frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$

Associativity of multiplication: $\left(\frac{a}{b}.\frac{c}{d}\right)\frac{e}{f}=\frac{ace}{bdf}=\frac{(ac)e}{(bd)f}=\frac{a(ce)}{b(df)}=\frac{a}{b}\frac{ce}{af}=\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)$

Commutativity of multiplication: We have

$$\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\frac{a}{b}.$$

Existence of multiplicative identity: We have

$\frac{a}{a}\in F$ where $a\neq 0$. Also if $\frac{c}{d}\in F$, then

$\frac{a}{a}\frac{c}{d}=\frac{ac}{aa}=\frac{c}{d}$ $[\because (ac,ad)\sim(c,d)$ because $\because acd=adc]$

$\therefore \frac{a}{a}$ is the multiplicative identity. It is also notify that

$\frac{a}{a}=\frac{b}{b}\forall\, a,b\in D_0$

Existence of multiplicative inverse: Let $0\neq\frac{a}{b}\in F$. Then $a\neq 0$.

$\therefore\ \frac{b}{a}\in F$. Since we have

$\therefore\ \frac{a}{b}\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=\frac{a}{a}=$ the unity element

$\therefore\ \frac{b}{a}$ is the inverse of $\frac{a}{b}$ w.r. to. the operation multiplication.

Distribution of multiplication over addition: We have

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\frac{(cf+de)}{df}=\frac{acf+ade}{bdf}=\frac{(acf+ade)bdf}{bdf\ bdf}=\frac{acfbdf+adebdf}{bdf\ bdf}$$

$$=\frac{acf}{bdf}+\frac{ade}{bdf}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\frac{c}{d}+\frac{a}{d}\frac{e}{f}$$

In similar way other distributive law also holds.

Under the definitions of addition and multiplication given above, *F* is a field. The field of quotients of *D* is the name given to this field, *F*. We will now demonstrate that the field *F* includes a subset *D′* such that *D* and *D′* are isomorphic.

Let $D'=\left\{\frac{ax}{x}\in F: a,\ 0\neq x\in D\right\}$. Then $D'\subseteq F$. If $x\neq 0, y\neq 0$ are element of *D*, then $\frac{ax}{x}=\frac{ay}{y}$

Since $axy=xay$. Therefore if x is any non-zero fixed element of *D*, we re-write

$D'=\left\{\frac{ax}{x}\in F: a\in D\right\}$.

Let us defined the function $\phi: D\to D'$ s.t.,

$\phi(a)=\frac{ax}{x}\forall\, a\in D$ is an isomorphism of *D* onto D'.

ϕ is one-one: Since we have, $\phi(a)=\phi(b)\Longrightarrow\frac{ax}{x}=\frac{bx}{x}\Longrightarrow axx=xbx\Longrightarrow ax^2=bx^2$

$$\Longrightarrow (a-b)x^2=0$$

$$\Longrightarrow a-b=0, \text{ since } x^2\neq 0$$

$$\Longrightarrow a=b$$

$\Longrightarrow \phi$ is one-one.

ϕ is onto: If $\frac{ax}{x}\in D'$, then $a\in D$. Also we have $\phi(a)=\frac{ax}{x}$. Thus ϕ is onto D'.

Also $\phi(a+b) = \frac{(a+b)x}{x} = \frac{(a+b)x^2}{x^3} = \frac{ax^2+bx^2}{x^3} = \frac{axx+xbx}{x^3}$

$= \frac{ax}{x} + \frac{bx}{x} = \phi(a) + \phi(b)$

and $\phi(ab) = \frac{(ab)x}{x} = \frac{(ab)x^2}{x^3} = \frac{(ax)(bx)}{x^2} = \frac{ax}{x}\frac{bx}{x} = \phi(a)\phi(b).$

$\Longrightarrow \phi$ is an isomorphism from D onto D' i.e., $D \cong D'$.

12.5 *IDEALS*

Definition (a): In a ring (R) a non empty subset (S) is said to be left ideal of R if:

(*i*) S should be subgroup of R w.r.to addition.

(*ii*) $rs \in S \; \forall \, r \in R, s \in S$

Definition (b): In a ring (R) a non empty subset (S) is said to be right ideal of R if:

(*i*) S should be subgroup of R w.r.to addition.

(*ii*) $sr \in S \; \forall \, r \in R, s \in S$

Definition (Ideal): A non-empty subset S of a ring R is said to be an ideal (also a two-sided ideal or left ideal/right ideal) if and only if it is both a left ideal and a right ideal. As a result, it may be claimed that a non-empty subset S of a ring R is an ideal of R. If,

(*i*) S is a subgroup of the additive group of R, or a subgroup of R under addition.

(*ii*) $rs \in S$ and $rs \in S \; \forall \, r \in R, s \in S$.

S is a subring of R if S is an ideal of the ring R because S is a subgroup of R under addition and from condition (ii), we have $xs \in S \; \forall \, x, s \in S$ because $x \in S \Rightarrow x \in R$. S is hence closed in terms of multiplication. S is a subring of R as a result. Each ideal of a ring R is a subring of R as a result. However, not all subrings are perfect. A stronger closure feature than the subring is necessary for an ideal. If S is a subgroup of R under addition, then S will be a subring if S is closed under multiplication, meaning that the result of two components of S is once more contained in S. However, S will be an ideal if S contains the result of any element of S and any element of R.

Every left ideal will also be a right ideal if R is a commutative ring. Thus, every left (right) ideal is an ideal in a commutative ring.

Note: Every ring R always has two improper ideals: one that is R itself and the other that is made up entirely of zeros. These are referred to as the **unit ideal** and the **null ideal**, respectively. Other ideals are called **proper ideal**. Any ring having no proper ideals is called **simple ring**.

Theorem 4: The intersection of two left ideals/right ideals of a ring is again left ideals/right ideals of the ring.

Proof: Let R be a ring and I_1, I_2 be two ideals of the ring. Then we have to prove that $I_1 \cap I_2$ is also an ideal of R. For it, we will first show that $I_1 \cap I_2$ is left ideal of R *i.e.*,

$r \in R, s \in I_1 \cap I_2 \Rightarrow rs \in I_1 \cap I_2$.

We have, $s \in I_1 \cap I_2 \Rightarrow s \in I_1, s \in I_2$.

Since both I_1, I_2 are left ideals of the ring (R). Therefore,

$r \in R, s \in I_1 \Rightarrow rs \in I_1$ and $r \in R, s \in I_2 \Rightarrow rs \in I_2$

Now, $rs \in I_1, rs \in I_2 \Rightarrow rs \in I_1 \cap I_2$

Hence, $I_1 \cap I_2$ is a left ideal of R.

In a similar way we can prove that $I_1 \cap I_2$ is also a right ideal of R.

Theorem 5: Arbitrary intersection of left ideal/right ideal of a ring is also left ideal/right ideal of the ring.

Proof: Let R be a ring and let $\{S_t : t \in T\}$ be the family of left ideal of R where T is the index set such that $t \in T$. S_t be the left ideal of R. Let $S = \underset{t \in T}{\cap} \{x \in R : x \in S_t \forall\, t \in T\}$ be the intersection of family of left ideal of R. **We will prove this theorem same as theorem 4.**

Example 1: The set N of all 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, where a, b are integers is a left ideal but not a right ideal in the ring (R) of all 2×2 matrices with elements as integers. In this case, N is the portion of R that consists of all the entries with zeros in the second column.

Answer: Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$ be any two elements of N.

Then, $A - B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in N$.

$\therefore N$ is a subgroup of R under addition.

Now let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of R and $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ be any element of N.

Then $UA = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of R and $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ be any element of N.

Then $UA = \begin{bmatrix} w & x \\ y & z \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} wa + xb & 0 \\ ya + zb & 0 \end{bmatrix} \in N$

Therefore N is a left ideal of R. It is not a right ideal, since

$\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix} \in N, \begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix} \in R,$

And the product $\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 2\\ 1 & 2\end{bmatrix}$ is not an element of N.

Theorem 6: A field has no proper ideals *i.e.*, any field (F) has only two ideals (0) and F is itself.

Proof: Let S be any non-zero ideal of the field F and let a be any non-zero element of S. We have $a^{-1} \in F$. Since S is an ideal, therefore

$a \in S, a^{-1} \in F \Rightarrow aa^{-1} \in S \Rightarrow 1 \in S$

Now let $x \in F$. Then

$1 \in S, x \in F \Rightarrow 1x \in S \Rightarrow x \in S$

Thus each element of field (F) belongs to S. Therefore $F \subseteq S$. Since we know that $S \subseteq F$.

Therefore $S = F$

Hence the only ideals of the field (F) are 0 and F itself.

Theorem 7: If R is a commutative ring and $a \in R$, then

$Ra = \{ra : r \in R\}$ is an ideal of R.

Proof: In order to prove that Ra is an ideal of R, we should prove that Ra is a subgroup of R under addition and that if $u \in Ra$ and $x \in R$ then xu and ux are also in Ra. Since R is a commutative ring, therefore $xu = ux$. Thus we only need to check that xu is in Ra.

Now, let $u, v \in Ra$. Then $u = r_1 a, , v \in r_2 a$ for some $r_1, r_2 \in R$.

We have $u - v = r_1 a - r_2 a = (r_1 - r_2)a \in Ra$ since $r_1 - r_2 \in R$. Thus $u, v \in Ra \Rightarrow u - v \in Ra$.

$\Rightarrow Ra$ is a subgroup of R under addition.

Now again, $x \in R$.

Then $xu = x(r_1 a) = (xr_1)a \in Ra$. Since $xr_1 \in R$.

$\therefore Ra$ is an ideal of R.

Theorem 8: A commutative ring with unity is a field if it has no proper ideals.

Proof: Assume that R is a commutative ring of unity with no appropriate ideals, meaning that the only two ideals of R are (0) and R. We must demonstrate that each nonzero element of R has a multiplicative inverse in order to prove that R is a field.

Let a be any non-zero element of R.

The set $Ra = \{ra : r \in R\}$ is an ideal of R. Since $1 \in R$, therefore $1a = a \in Ra$. Thus $0 \neq a \in Ra$. Therefore the ideal $Ra \neq (0)$. Since R has no proper ideals, therefore the only possibility is that

$Ra = R$. Thus each element of R is a multiple of a by some element of R. In particular, $1 \in R$ so it can be realised as a multiple of a. Thus there exist an element $b \in R$ such that $ba = 1$.

$a^{-1} = b$. Hence each non-zero element of R possesses multiplicative inverse.

Hence R is a field.

12.5.1 *MORE ABOUT IDEALS*

In a ring (R) ideal generated ideal generated by given subset of R : We can locate ideals containing M if M is any subset of a ring. As an illustration, the ring R is an ideal that may include any subset of R.

Smallest ideal containing subset: Let M represent any arbitrary subset of a ring. The smallest ideal of R containing M if is therefore an ideal S of if,

$M \subseteq S$ **,**

and if every ideal of R containing M contains S.

Definition: Let M be any arbitrary subset of R and let R be a ring. The ideal created by M is stated to be the smallest ideal of R containing M, and it is indicated by the symbol (M).

In particular, we write (a) in instead of M if M only consists of one element, let's say a, of the ring R. A principal ideal is an ideal like (a) that is produced by just one ring element.

12.6 *PRINCIPAL IDEAL*

Definition: Any ideal S of a ring R will be called principal ideal if there exist an element $a \in S$ s.t. any ideal T of R that contain a also contains S *i.e.*, $S = (a)$.

Therefore, the principal ideal is an ideal generated by a single element in itself.

In a ring (R) if $1 \in R$, then the ideal generated by 1 is whole ring i.e., $(1) = R$, since each element of R can be expressed as $r1$. Ring itself is referred to be the unit ideal for this reason. The null ideal is the ideal produced by the zero element of R, or (0), which only contains the zero element. Every ring R has (0) as at least one of its primary ideals. Every ring with unity has two primary ideals at a minimum, namely (0) and (1).

Theorem 9: If a is an element in a commutative ring R with unity, then the set $S = \{ra | r \in R\}$ is a principal ideal of R generated by the element a *i.e.*, $S = (a)$.

Proof: First we have to prove that $a \in S$. Since R is ring with unit element 1, therefore $1a = a \in S$.

We must now demonstrate that S is an ideal of R. Therefore, we must first demonstrate that S is a subgroup of R under addition. Let the two element of S are u, v. Then $u = r_1 a, v = r_2 a$ for some $r_1, r_2 \in R$.

We have $u - v = r_1 a - r_2 a = (r_1 - r_2)a \in S$. Since $r_1 - r_2 \in R$.

Since S is a subgroup of R under addition.

Now we have to prove that $x \in R, u \in S \Rightarrow xu \in S$ and $ux \in S$. But R is a commutating ring then, $xu = ux$ and thus we have only to prove that $xu \in S$.

We have $xu = x(r_1 a) = (xr_1)a \in S$.

As we know $xr_1 \in R$

$\therefore S$ is an ideal of R and $a \in S$.

Now to prove that S is an ideal which is generated by the element a, We have only to show that if T is an ideal of R and $a \in T$, then $S \subseteq T$.

Let $ra \in S$ then $r \in R$. If T is an ideal of R s.t. $a \in T$ then $r \in R, a \in T \Rightarrow ra \in T$. Thus $S \subseteq T$.

Hence S is principal ideal of R s.t. $S = (a)$.

Example 2: To find the principal ideal in the ring (R) of integer generated by 5.

Solution: Since we know ring of integer (I) is a commutative ring with unity.

Since $(5) = \{5r \mid r \in I\}$

Thus, principal ideal of R generated by 5 is

$(5) = \{..., -10, -5, 0, 5, 10, ...\}$

and obviously, $(-5) = (5)$

12.7 *EUCLIDEAN AND PRINCIPAL IDEAL DOAMIN (PID)*

Definition: Let E be an integral domain. A function $v : E^* \to Z^\#$ is called a Euclidean valuation on E if

(*i*) for all $a, b \in E$ with $a \neq 0$, there exist $q, r \in E$ such that $b = aq + r$, where either $r = 0$ or $v(r) < v(a)$ and

(*ii*) $v(r) \leq v(ab)$, for all $a, b \in E^*$

An integral domain E together with a valuation v on E is called a Euclidean domain. It is denoted by (E, v).

Example 3: The ring Z of all integers can be considered as a Euclidean domain with the valuation $v : Z^* \to Z^\#$ defined by $v(a) = |a|, \forall a \neq 0$.

Example 4: Consider polynomial ring F[x], where F is a field. Then F[x] is an integral domain.

Define as $v : F[x] \setminus \{0\} \to Z^{\#}$ by

$v(f(x)) = \deg f(x), \forall\ f(x) \in F[x] \setminus \{0\}$.

Let $f(x), g(x) \in F(x), g(x) \neq 0$. Since F is a field, so every nonzero element in F and hence the leading coefficient of g(x) is a unit. It follows, by the Division Algorithm for polynomials, that there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Hence, we have $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ *or* $v(r(x)) < v(g(x))$.

Since there is no zero divisors in F, so for any two nonzero elements f(x) and g(x) in F[x], we have $\deg(f(x)g(x)) = \deg f(x) + \deg g(x) \geq \deg f(x), i.e.\quad v(f(x)g(x)) \geq v(f(x))$. Hence, F[x] is a Euclidean domain.

Now we show that every field is a Euclidean domain. In search of a suitable Euclidean valuation on a field, we first prove the following result:

Theorem 10: Let E be a Euclidean domain with the valuation *v*. Then for every $a \in E^*, v(a) = v(1)$ if and only if a is *a* unit in E.

Proof: For all $a \in E^*, v(a) = v(1a) \geq v(1)$.

Suppose a is a unit. Then there exists an element $b \in E$ such that $ab = 1$which implies that $v(1) = v(ab) \geq v(a)$. Hence $v(a) = v(1)$.

Conversely, suppose that $v(a) = v(1) \forall\ a \in E^*$. Now $a \neq 0$ implies that there exist $q, r \in E$ such that $1 = qa + r$, where $r = 0$ *or* $v(r) < v(a) = v(1)$ r = 0 . Since $v(r) < v(1)$ is impossible, we have r = 0. Thus $1 = qa$ and hence a is a unit. Hence, if it is possible to define a Euclidean valuation *v* on a field F, then $v(a) = v(1)$ for every $a \in F^*$, since every nonzero element of F is a unit. Thus *v* is a constant mapping.

Example 5: Let F be a field. Then $v : F^* \to Z^{\#}$ given by:

$v(a) = 2 \forall\ a \in F^*$

is a Euclidean valuation. (Note that image of v may be any nonnegative integer.) Thus C, R and Q all are Euclidean domain. Every ideal of Z is a principal ideal. Now we consider the integral domains such that every ideal is a principal ideal.

Definition: An integral domain R is called a principal ideal domain (PID) if every ideal of R is a principal ideal. Thus Z is a PID. Also every field is a PID.

Theorem 11: Every Euclidean domain is a principal ideal domain.

Proof: Let (E, v) be a Euclidean domain. Consider an ideal I of E. If $I = \{0\}$, then $I =< 0 >$. Let $I \neq \{0\}$. Then $N = \{v(x) \mid x \in I, x \neq 0\}$ is a nonempty set of non negative integers; and so, by the well-ordering principle, it has the least element. Let $a \in I, a \neq 0$ be such that $v(a)$ is the least element of N, i.e. $v(a) \leq v(x) \forall\, x \in I, x \neq 0$. We show that I = Ea. Since $a \in I$, it follows that $E(a) \subseteq I$. Let $b \in I$ b 2 I. Since E is a Euclidean domain, there exist $q, r \in E$ such that $b = qa + r$, where $r = 0$ *or* $v(r) < v(a)$. If $r \neq 0$, then $r = b - aq \in I$ shows that $v(r) \in N$; and since $v(r) < v(a)$ this contradicts the minimality of $v(a)$ in *N*. Therefore, r = 0 and so $b = aq \in Ea$. Thus $I \subseteq Ea$, and hence $I = Ea$.

Now we characterize the polynomial rings which are Euclidean domains.

Theorem 12: Let F be a commutative ring with 1. Then the following conditions are equivalent:

1. F is a field;

2. F[x] is a Euclidean domain;

3. F[x] is a principal ideal domain.

Proof $(1) \Rightarrow (2)$: Follows from Example 4.

$(2) \Rightarrow (3)$: Follows from Theorem 11.

$(3) \Rightarrow (1)$: First note that F[x] is an integral domain, since F is so. Let $a \in F$ be a nonzero element of F. Consider $I =< a, x >$, the ideal of F[x] generated by *a* and *x*. Since F[x] is a principal ideal domain, there exists $u(x) \in F[x]$ such that $I =< u(x) >= \{u(x) f(x) \mid f(x) \in F[x]\}$. Now $a, x \in < u(x) >$ implies that there exist $g(x), h(x) \in F[x]$ such that $u(x)g(x) = a$ and $u(x)h(x) = x$.

Since F is an integral domain, $u(x)g(x) = a$ shows that $u(x)$ is nonzero and $\deg(u(x)) = 0$ which implies that $u(x) = b \in F$. Again, $bh(x) = x \Rightarrow bc = 1$ for some $c \in F$. Thus b is a unit and so $I =< b >= F[x]$. Then $1 \in I \Rightarrow 1 = af_1(x) + xf_2(x)$ for some $f_1(x), f_2(x) \in F[x]$. This implies that $1 = da$ for some $d \in F$. Thus a is a unit in F and hence F is a field.

Since Z is not a field, It follows that Z[x] is not a principal ideal domain. In the following example we give an example of an ideal of Z[x], which is not principal.

Example 6: In Z[x], we show that the ideal $< x, 2 >$ is not a principal ideal. On the contrary, if possible, assume that $< x, 2 >$ is a principal ideal and $< x, 2 >=< u(x) >, u(x) \in Z[x]$. Now $2 \in < u(x) >$ implies that $2 = u(x) f(x)$ for some $f(x) \in Z[x]$. Since Z is an integral domain, so $\deg u(x) = 0$ and $u(x) = a \in Z$. Since $x \in < a >$, there is $g(x) \in Z[x]$ such that $x = ag(x)$. It follows that $ab = 1$ for some $b \in Z$, and so $1 \in < a >=< x, 2 >$. Hence there are $h(x), k(x) \in Z[x]$ such that $1 = xh(x) + 2k(x) \Rightarrow 1 = 2c$ for some $c \in Z$, a contradiction. Therefore $< x, 2 >$ is not a principal ideal.

Theorem 13: Let R be a Euclidean domain (principal ideal domain) and $a,b \in R$ not both zero. Then *a* and *b* have a gcd *d*.

Proof: For every gcd *d* of *a* and *b*, there exist $s,t \in R$ such that $d = sa + tb$. *a*, *b* are relatively prime if and only if there exist $s,t \in R$ such that $1 = sa + tb$. Now we show that the irreducible elements and the prime elements coincide in a PID.

Theorem 14: Let R be a principal ideal domain and $p \in R$. Then *p* is irreducible if and only if it is prime.

Proof: As we know that every prime element is irreducible in an integral domain. Suppose that p is an irreducible element in R. Consider $a,b \in R$ and assume that $p \mid ab$. Then $ab = pc$ for some $c \in R$. Since R is a principal ideal ring, there is $d \in R$ such that $< p,b >=< d >$. Then there exists $q \in R$ such that $p = dq$. Since p is irreducible, either d or q must be a unit. If d is a unit, then $< p,d >=< d >= R$. Hence $1 \in < p,b >$ and so $1 = sp + tb$ for some $s,t \in R$. This implies that $a = asp + atb = asp + tcp = (as + tc)p$. Thus $p \mid a$. If q is a unit, then $d = q^{-1}p \in < p >$. This implies that $< d > \subseteq < p > \subseteq < p,b >=< d >$. Hence $< p >=< p,b >$ and so $b \in < p >$. Thus $p \mid b$. Recall that if F is a field then a polynomial p(x) is irreducible if and only if $F[x]/ < p(x) >$ is a field. Hence p(x) is irreducible if and only if $< p(x) >$ is a maximal ideal in F[x]. We show that this result holds in every PID.

Theorem 15: Let R be a principal ideal domain. Then M is a maximal ideal of R if and only if $M =< q >$ for some irreducible element $q \in R$.

Proof: Already we know that if $M =< q >$ is a maximal ideal then q is an irreducible element.

Conversely, suppose that q is an irreducible element and $M =< q >$. Consider an ideal I of R such that $M \subseteq I \subseteq R$. Since R is a principal ideal domain, there exists $a \in R$ such that $I =< a >$. Now $q \in M \subseteq < a >$ shows that $q = ab$ for some $b \in R$. Irreducibility of q implies that either *a* or *b* is a unit. If *a* is a unit then $I =< a >= R$. If b is a unit then $a = qb^{-1} \in < q >= M$. This implies that $< a > \subseteq M$ and hence $M = I$. Thus M is a maximal ideal of R.

If a ring R becomes a PID then primality and irreducibility are no longer different, and as a consequence we have the following important corollary.

Corollary: Let *R* be a principal ideal domain. Then a nonzero proper ideal *P* of *R* is prime if and only if it is maximal.

12.8 *UNIQUE FACTORIZATION DOAMINS (UFDs)*

Definition : An integral domain D is called a factorization domain if every nonzero non unit element a of D can be expressed as a product $a = p_1 p_2 p_3 ... p_m$ of irreducible elements.

2: A factorization domain D is called a unique factorization domain (UFD) if for every nonzero non unit element a of D, $a = p_1 p_2 p_3 ... p_m = q_1 q_2 q_3 ... q_m$ are two irreducible factorizations of a then $m = n$ and there is a permutation σ such that each p_i is an associate of $q_{\sigma(i)}$.

The fundamental theorem of arithmetic shows that the ring Z of integers is a unique factorization domain. Later we see that every principal ideal domain is a unique factorization domain.

Recall that in an integral domain every prime element is irreducible. Now we have the following theorem:

Theorem 16: In a unique factorization domain, every irreducible element is prime.

Proof: Suppose that D is a unique factorization domain and let p be an irreducible element of D.

Consider $a, b \in D$ and assume that $p \mid ab$. Then $ab = pc$ for some $c \in D$. If $a = 0$ then $p \mid a$ and if a is a unit then $b = pa^{-1}c$ shows that $p \mid b$. Similarly for b. Now we assume further that a and b are neither zero nor units. Then $c \neq 0$. Also c is not a unit, otherwise pc is irreducible and then either a or b becomes a unit which is against our assumption. Since D is a unique factorization domain, a, b and c have irreducible factorizations, say $a = a_1 a_2 a_3 ... a_r, b = b_1 b_2 b_3 ... b_s$ and $c = c_1 c_2 c_3 ... c_t$. Then $a = a_1 a_2 a_3 ... a_r b_1 b_2 b_3 ... b_s = pc_1 c_2 c_3 ... c_t$ implies that p is associate of one of the irreducible elements $a_1, a_2, a_3, ..., a_r, b_1, b_2, b_3, ... b_s$. If p is associate of some a_i, say $a_i = pu$, u is a unit, then $a = pua_1 a_2 a_3 ... a_{i-1} a_{i+1} ... a_r$ shows that $P \mid a$. Similarly, if p is associate of some b_j, then $p \mid b$. Thus p is a prime element.

Theorem 17: Let a and b be two nonzero elements in a unique factorization domain D. Then $\gcd(a, b)$ exists in D.

Proof: If either of a and b, say a is a unit, then $a \mid b$ implies that a is a $\gcd(a, b)$. Suppose that neither a nor b is a unit and $a = P_1^{l_1} P_2^{l_2} ... P_r^{l_r}$ and $b = P_1^{m_1} P_2^{m_2} ... P_r^{m_r}$ where $p_1, p_2, p_3, ..., p_r$ are irreducible elements, $l_1, l_2, ..., l_r, m_1, m_2 ..., m_r$ are nonnegative integers (most likely some of them are zero). Let $n_i = \min\{l_i, m_i\}$. We show that $d = P_1^{n_1} P_2^{n_2} ... P_r^{n_r}$ is a $\gcd(a, b)$. It follows directly that $d \mid a$ and $d \mid b$. Let $c \mid a$ and $c \mid b$. If c is a unit, then $c \mid d$. Otherwise the uniqueness of the irreducible factorizations

of a and b implies that $c = up_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ where $0 \le k_i \le l_i, m_i \forall i$. Then $k_i \le n_i$ and it follows that $c \mid d$. Hence $d = \gcd(a, b)$

Now we show that every principal ideal domain is a unique factorization domain. For this let us first prove a series of lemmas:

Lemma 1: Every ascending chain of ideals in a principal ideal domain is finite.

Proof: Let D be a principal ideal domain. Let $< a_1 > \subseteq < a_2 > \subseteq < a_3 > ...$ be an ascending chain of ideals in D. Then $I = \cup_i < a_i >$ is an ideal of D and so, since D is a principal ideal domain, there is $a \in D$ such that $I = < a >$. Now $a \in \cup_i < a_i >$ implies that $a \in < a_k >$ for some $k \in N$. Then $a \in < a_j >$ and so $< a > \subseteq < a_j >$ for all $j \ge k$. Also $< a_j > \subseteq < a >$. Thus $< a > = < a_j >$ for all $j \ge k$. Thus the sequence of ideals is finite.

Lemma 2: A factorization domain is a unique factorization domain if and only if every irreducible element is prime.

Proof: The necessary part follows from the Theorem 16.

Conversely, suppose that D is a factorization domain in which every irreducible element is a prime element. Since D is a factorization domain, every nonzero nonunit element of D has an irreducible factorization. We prove that this factorization is unique (up to associates and order of the factors) by induction on the number n of irreducible factors in irreducible factorization of an element. If $n = 1$ then the result follows from the definition of irreducible elements. Assume that the result is true for $n < s$. Suppose $a \in D$ and assume that $a = p_1 p_2 ... p_s = q_1 q_2 ... q_t$ be two irreducible factorizations of *a*. Now p_s is prime; and so $p_s \mid q_1 q_2 ... q_t$ which implies that $p_s \mid q_t$, upon rearrangement. Since both p_s and q_t are irreducible elements in *D*, this implies that $q_t = up_s$ for some unit *u*. Then we have

$$p_1 p_2 ... p_{s-1} = q_1 q_2 ... q_{t-1} u$$

which implies, by the induction hypothesis, that $s - 1 = t - 1$ and each p_i is associate to some q_j, $1 \le i \le s-1, 1 \le j \le t-1$. Also p_s is associate to q_t. Thus the result follows.

Now we prove the main theorem.

Theorem 18: Every principal ideal domain is a unique factorization domain.

Proof: In a principal ideal domain, every irreducible element is prime; and so due to the Lemma 2 it is sufficient to show that every principal ideal domain is a factorization domain. Let D be a principal ideal domain and $a \in D$ be a nonzero and non unit element of D. We show that *a* is a product of irreducible elements. If possible, let *a* be not a product of irreducibles. Then *a* is not an irreducible

element, and so there are two non units $a_1, a_1' \in D$ such that $a = a_1 a_1'$ and at least one, say a_1 is not a product of irreducible element. Since a_1' is not a unit, we have $< a > \subsetneq < a_1 >$.

Again since a_1 is not a product of irreducibles, similarly we get $a_2 \in D$ such that $< a > \subsetneq < a_1 > \subsetneq < a_2 >$ and a_2 is not a product of irreducibles. We continue and get a strictly ascending infinite chain of ideals

$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq ...$

in D. This contradicts that D is a principal ideal domain. Thus a has an irreducible factorization. The converse of the above theorem is not true, in general. We know that Z[x] is not a principal ideal domain; in the following we show that Z[x] is a UFD. In fact, we prove a more general result that D[x] is a UFD whenever D is so.

Definition: Let D be a unique factorization domain and $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n$ be a nonzero polynomial on D. Then $\gcd(a_0, a_1, ..., a_n)$ is called content of $f(x)$.

This is denoted by $c(f)$.

Since gcd is not unique, in fact it is unique up to associates, it follows that $c(f)$ is unique up to associates.

Definition: Let D be a unique factorization domain. A nonzero polynomial $f(x) \in D[x]$ is called a primitive polynomial if $c(f)$ is unit.

If D is a unique factorization domain, and $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n \in D[x]$ be a nonzero polynomial. Since some a_i is nonzero the $\gcd(a_0, a_1, ..., a_n)$ exists in D, say $d = \gcd(a_0, a_1, ..., a_n)$. Then there are $a_i' \in D$ such that $a_i = d a_i'$ and $\gcd(a_0', a_1', ..., a_n') = 1$. Thus $f_1(x) = a_0' x^n + a_1' x^n + .. + a_n'$ is primitive and $f(x) = c(f) f_1(x)$

Lemma 3: Product of two primitive polynomials is primitive.

Proof: Let D be a unique factorization domain and $f(x) = a_0 x^m + a_1 x^{m-1} + ... + a_{m-1} x + a_m$ and $g(x) = b_0 x^n + b_1 x^{n-1} + ... + b_{n-1} x + b_n$ be two primitive polynomials over D. If possible, let $h(x) = f(x) g(x) = \sum_{i=0}^{m+n} c_i x^{n-i}$ be not primitive. Then $d = \gcd(c_0, c_1, ..., c_{m+n})$ is not a unit and so there is an irreducible element p in D such that $p \mid c_i \; \forall \, i$. Suppose k, l be the smallest nonnegative integers such that $p \nmid a_k$ and $p \nmid b_l$. Then $p \mid c_{k+l} = a_{k+l} b_0 + a_{k+l-1} b_1 + ... + a_{k+1} b_{l-1} + a_k b_l + a_{k-1} b_{l+1} + ... + a_0 b_{k+l}$ and $p \mid a_{k+l} b_0 + a_{k+l-1} b_1 + ... + a_{k+1} b_{l-1} + a_k b_l + a_{k-1} b_{l+1} + ... + a_0 b_{k+l}$

$\Rightarrow p \mid a_k \text{ or } p \mid b_l$. This contradicts the choice of *k* and *l*.

Lemma 4: Let R be a UFD and $f(x), g(x) \in R[x]$ be two primitive polynomials. Then f(x) and g(x) are associates in R[x] if and only if they are associates in Q(R)[x].

Proof: Let f(x) and g(x) be associates in Q(R)[x]. Since Q(R) is a field, so the units in Q(R)[x] are precisely the nonzero elements of Q(R). Hence there is a unit $w = ab^{-1} \in Q(R)$ such that $g(x) = ab^{-1} f(x)$ which implies that $bg(x) = af(x)$. It follows that $a = bu$ for some unit $u \in R$, since both $f(x)$ and $g(x)$ are primitive in $R[x]$. Therefore $g(x) = uf(x)$ and so $f(x)$ and $g(x)$ are associates in R[x].

Converse is trivial, since every unit in R[x] is a unit in Q(R)[x].

Lemma 5: Let R be a UFD and $f(x) \in R[x]$ be a non constant primitive polynomial. If $f(x)$ is irreducible over R then it is irreducible over $Q(R)$.

Proof: On the contrary, if possible, let $f(x)$ be reducible over $Q(R)$. Since $Q(R)$ is a field, so the units in $Q(R)[x]$ are precisely the nonzero elements of $Q(R)$. Hence there are two non constant polynomials $g(x), h(x) \in Q(R)[x]$ such that $f(x) = g(x)h(x)$. Let $g(x) = a_0 b_0^{-1} + a_1 b_1^{-1} x + ... + a_n b_n^{-1} x^n$. Then for $b = b_0 b_1 b_2 ... b_n \in R, bg(x) \in R[x]$. Denote $a = cont(b(g(x))$ in R. Then $bg(x) = ag^*(x)$ where $g^*(x) \in R[x]$ is a primitive polynomial. Similarly there are $c, d \in R$ such that $dh(x) = ah^*(x)$ where $h^*(x) \in R[x]$ is a primitive polynomial. Thus $bdf(x) = acg^*(x)h^*(x)$. Since product of two primitive polynomials is primitive, it follows that both $f(x)$ and $g^*(x)h^*(x)$ are primitive. Hence $ac = ubd$ for some unit $u \in R$, and $f(x) = ug^*(x)h^*(x)$ which shows that $f(x)$ is reducible over R, a contradiction. Therefore $f(x)$ is irreducible in $Q(R)[x]$.

Lemma 6: If R is a unique factorization domain, then the polynomial ring R[x] is also a unique factorization domain.

Proof: We first show that R[x] is a factorization domain. We apply induction on deg f(x), where $f(x)$ is a nonzero non unit element of R[x]. If deg f(x) = 0, then $f(x) \in R$ and it is a product of irreducibles, since R is a UFD. Let $\deg f(x) > 0$. Then $f(x) = c_f f^*(x)$ where $f^*(x) \in R[x]$ is a primitive polynomial. Since $c_f \in R$ so c_f is either unit or a product of irreducible elements in R. If $f^*(x)$ is irreducible, we are done. Otherwise, there are two nonzero non units $g(x), h(x) \in R[x]$ such that $f^*(x) = g(x)h(x)$. Since $f^*(x)$ is primitive, so neither $g(x)$ nor $h(x)$ is a constant. Hence $\deg g(x) < \deg f^*(x) = \deg f(x)$ and $\deg h(x) < \deg f^*(x) = \deg f(x)$. Then both $g(x)$ and $h(x)$ are

products of irreducible elements in R[x], by induction hypothesis. Therefore, $f(x) = a_1 a_2 ... a_r p_1(x) p_2(x) ... p_n(x)$ where $a_1, a_2, ..., a_r \in R$ and $p_1(x), p_2(x), ..., p_n(x) \in R[x]$ are irreducible elements.

To prove the uniqueness of the factorization, assume that

$$f(x) = a_1 a_2 ... a_r p_1(x) p_2(x) ... p_m(x) = b_1 b_2 ... b_s q_1(x) q_2(x) ... q_n(x)$$

Where $a_1, a_2, ..., a_r, b_1, b_2, ..., b_s \in R$ and $p_1(x), p_2(x), ..., p_m(x), q_1(x), q_2(x), ..., q_n(x) \in R[x]$ are irreducible elements. Since $a_1 a_2 ... a_r = b_1 b_2 ... b_s = c_f$, so it follows that

$$p_1(x) p_2(x) ... p_m(x) = u q_1(x) q_2(x) ... q_n(x)$$

for some unit $u \in R$. Since $Q[R]$ is a field, so $Q(R)[x]$ is a UFD. Also the irreducible polynomials $p_1(x), p_2(x), ..., p_m(x), q_1(x), q_2(x), ..., q_n(x) \in R[x]$ are primitive, which implies that they are also irreducible in $Q(R)[x]$. Hence it follows that $m = n$ and there is a permutation $\sigma \in S_n$ such that $p_i(x)$ is an associate of $q_{\sigma(i)}(x)$ in $Q(R)[x]$ and so $p_i(x)$ is an associate of $q_{\sigma(i)}(x)$ in $R[x]$, by Lemma 4. Therefore the factorization f(x) in R[x] is unique.

This result shows that Z[x] is a unique factorization domain. Similar result is not true for principal ideal domain or Euclidean domain; e.g. Z is a principal ideal domain but Z[x] is not.

Unlike to the PID, Bezout's identity does not hold in UFD. For example, consider the UFD Z[x]. Then $\gcd(x+2, x+4) = 1$, but there are no $f(x), g(x) \in Z[x]$ such that

$$1 = (x+2) f(x) + (x+4) g(x)$$

otherwise $1 = 2a_0 + 4b_0$

In most of the deductions regarding divisibility in Z, we prefer to use B_ezout's identity, hardly we use the Fundamental Theorem of Arithmetic. Here we show that the Fundamental Theorem of Arithmetic can also be used in these deductions.

Example 7: Let D be a UFD and a, b, c be there non zero elements of D such that $a \mid bc$ and $\gcd(a, b) = 1$. We show that $a \mid c$. If a or b is a unit, the result follows trivially. Assume that neither a nor b is a unit. Let $a = a_1^{n_1} a_2^{n_2} ... a_r^{n_r}$ and $b = b_1^{m_1} b_2^{m_2} ... b_s^{m_s}$ where a_i and b_j are irreducible elements and $1 \le n_i, m_j$ for every $i = 1, 2, ..., r$ and $j = 1, 2, ..., s$. Since $\gcd(a, b) = 1$, so no a_i is an associate of any b_j. If c is a unit then $bc = aq, q \in D$ implies that $b = aqc^{-1}$. This contradicts that D is a UFD, since no a_i is an associate of any b_j. Thus c is a non unit. Let $c = c_1^{l_1} c_2^{l_2} ... c_t^{l_t}$ be an irreducible factorization of c.

Then $bc = aq$ implies that $b_1^{m_1} b_2^{m_2} ... b_s^{m_s} c_1^{l_1} c_2^{l_2} ... c_t^{l_t} = a_1^{n_1} a_2^{n_2} ... a_r^{n_r} q$. Since no a_i is an associate of any b_j, so every a_i is an associate to some c_k and $n_i \le l_k$. Hence $a \mid c$.

Check your progress

Problem 1: What are the ideals of the set $I_5 = \{0,1,2,3,4\}$?

Problem 2: Check out the principal ideal in the ring (R) of integer generated subgroup while it is not a maximal subgroup.

12.9 *SUMMARY*

In this unit, we have learned about the important relation between two rings name as isomorphic relation. If two ring are isomorphic to each other then we can unfold the information about the unknown ring on the basis of known ring. In this unit we have also learned about the ideals of the ring. On the basis of ideals we have further learned about the principal ideal domain. The other important topics of this unit are Euclidean domain and unique factorization domain. The overall summarization of this units are as follows:

- Every field has no proper ideal.
- Each integral domain can be imbedded in a field.
- In a unique factorization domain, every irreducible element is prime.
- Every principal ideal domain (PID) is unique factorization domain (UID).
- Arbitrary intersection of ideals of ring is again an ideal of the ring.
- Each field has no proper ideal.
- Commutative ring with unity is a field if it has no proper ideals
- Every Euclidean domain is a PID.

12.10 *GLOSSARY*

- $R \cong R'$: Denotes two rings R, R' are isomorphism to each other.
- **UFD:** Unique factorization domain.
- **PID:** Principal ideal domain.
- **ED:** Euclidean domain.

12.11 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.

- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5^{th} Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

12.12 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3^{rd} Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2^{nd} edition), Pearson, 2014.

12.13 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that any ring R without a unity element may be imbedded in a ring that contains a unity element.

2. Prove that each integral domain can be imbedded in a field?

3. In a unique factorization domain, every irreducible element is prime.

4. Prove that every principal ideal domain (PID) is unique factorization domain (UID).

5. If a is an element in a commutative ring R with unity, then prove that the set $S = \{ra | r \in R\}$ is a principal ideal of R generated by the element a *i.e.,* $S = (a)$.

Short Answer Type Question:

6. Prove that intersection of two ideal of a ring is again a ideal of the ring.

7. Prove that arbitrary intersection of ideals of ring is again an ideal of the ring.

8. Prove that each field has no proper ideal

9. Prove that a commutative ring with unity is a field if it has no proper ideals.

10. To find the principal ideal in the ring (R) of integer generated by 7.

11. Prove that product of two primitive polynomials is primitive.

12. Let a and b be two nonzero elements in a unique factorization domain D. Then prove that $\gcd(a, b)$ exists in D.

Fill in the blanks:

13. In a UFD, every irreducible element is …….

14. Every PID is ……..

15. Product of two primitive polynomials is …….

16. Every Euclidean domain is a ……

17. If every ideal of integral domain is principal ideal then an integral domain is called …..

12.14 *ANSWERS*

Answer of self cheque question:

1. $\{0\}$ and F itself **2.** $< 7 >= \{...,-14,-7,0,7,14,...\}$

Answer of terminal question:

13. Prime **14.** UFD **15.** Primitive **16.** PID **17.** PID

Unit-13: POLYNOMIAL RINGS AND IRREDUCIBILITY CRITERIA, EINESTEIN'S CRITERIA OF IRREDUCIBILITY

CONTENT:

13.1 *INTRODUCTION*

In this unit we give some results to test irreducibility of polynomials over a field, specially over the field Q of all rational numbers. If K is a subfield of F, then every polynomial $p(x)$ over K can also be considered as a polynomial over F. It follows that if $p(x)$ is irreducible over F then it is so over K, but the converse is not true. For example, $x^2 - 3$ is irreducible over Q but reducible over R

Eisenstein's criteria in mathematics provides a necessary condition for a polynomial with integer coefficients to be irreducible over the rational numbers, that is, not factorizable into the product of non-constant polynomials with rational coefficients. This condition does not apply to all polynomials with integer coefficients that are irreducible over the rational numbers, but it does allow irreducibility to be shown with minimum effort in certain crucial examples. It can be used immediately

or after the original polynomial has been transformed. This criteria is named after Gotthold Eisenstein. It was known as the Schönemann-Eisenstein theorem in the early twentieth century since Theodor Schönemann was the first to publish it.

Theodor Schönemann, commonly known as Schoenemann, was a German mathematician who produced numerous significant discoveries in number theory involving the theory of congruences, which are published in Crelle's journal volumes 17 to 40. Notably, he obtained Hensel's lemma before to Hensel, Scholz's reciprocity rule prior to Scholz, and Eisenstein's criteria prior to Eisenstein. He also investigated what are now known as finite fields (more general than those of prime order) in the form of integer polynomials modulo both a prime number and an irreducible polynomial (remaining irreducible modulo that prime number).

13.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the polynomial ring.
- Analyze about the division algorithm in terms of polynomials.
- Analyze about the irreducibility criteria of polynomials
- Analyze the Eisenstein's criteria for irreducibility over Q.

13.3 *INTRODUCTION OF POLYNOMIALS*

Let R be a commutative ring with unity 1. A polynomial over R is defined as an infinite sequence $(a_0, a_1, a_2, ...)$ such that all but finitely many a_i are 0, i.e. there is a nonnegative integer n (depending on the sequence $(a_0, a_1, a_2, ...)$ under consideration) such that $a_i = 0$ for all $i \geq n$; and the set of all polynomials on R is denoted by $R[x]$. Thus

$$R[x] = \{(a_0, a_1, a_2, ...) \mid a_i \in R \text{ and } a_i = 0 \text{ for all but finitely many } i\}$$

We now define addition and multiplication on $R[x]$ as follows:

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$$

and $(a_0, a_1, a_2, ...).(b_0, b_1, b_2, ...) = (c_0, c_1, c_2, ...),$

where $c_i = \sum_{r=0}^{i} a_r b_{i-r}$ for $i = 0, 1, 2, ...$

We leave it to the reader to verify that $(R[x],+,.)$ is a commutative ring with unity $(1,0,0,...)$. Also $(0,0,0,...)$ is the zero element of $R[x]$ and the additive inverse of $(a_0,a_1,a_2,...)$ is $(-a_0,-a_1,-a_2,...)$ The mapping

$$a \to (a,0,0,...)$$

is a monomorphism of the ring R into $R[x]$. Thus, R can be considered as a subring of R[x] and we no longer distinguish between a and $(a,0,0,...)$.

The particular element $(0,1,0,0,0...)$ is called the indeterminate over R and is usually denoted by x. Then according to the definitions of addition and multiplication in $R[x]$, we have

$$x^2 = (0,1,0,0,...)(0,1,0,0,...) = (0,1,0,0,...)$$

$$x^3 = (0,1,0,0,...)(0,1,0,0,...) = (0,0,0,1,0,...)$$

.

.

.

and then

$$a_1x = (a_1,0,0,0,...)(0,1,0,0,...) = (0,a_1,0,0,0,...)$$

$$a_2x^2 = (a_2,0,0,0,...)(0,0,1,0,...) = (0,0,a_2,0,0,...)$$

.

.

.

Thus we have

$$(a_0,a_1,a_2,...,a_n,0,...) = (a_0,0,0,...) + (0,a_1,0,0,...) + ... + (0,...,0,a_n,0,...)$$

$$= a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

The elements $a_0,a_1,a_2,...,a_n$ are called the coefficients of the polynomial $P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. If $a_n \neq 0$, then a_n is called the leading coefficient and if the leading coefficient $a_n = 1$, then $p(x)$ is called a monic polynomial. We define the zero element $(0,0,0,...)$ of the ring $R[x]$ as the zero polynomial, and it will be denoted by 0. Thus a polynomial $P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ is zero if and only if $a_0 = a_1 = a_2 = ... = a_n = 0$.

Example 1: Consider the polynomial ring $Z_6[x]$. Then $f(x) = [2]x^3$ and $g(x) = [3]x^2$ are two nonzero elements of $Z_6[x]$ but $f(x)g(x) = [0]$. This shows that $Z_6[x]$ is not an integral domain.

Now we characterize the rings R for which the associated polynomial ring R[x] is an integral domain.

Theorem 1: Let R be a commutative ring with unity 1. The $R[x]$ is an integral domain if and only if R is an integral domain.

Proof: First assume that R is an integral domain. Then $R[x]$ is a commutative ring with 1. Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$ be two nonzero polynomials in $R[x]$. Then, we may consider $a_n \neq 0$ and $b_m \neq 0$ and so $a_nb_m \neq 0$, since R is an integral domain. Then the polynomial $f(x)g(x) = c_0 + c_1x + c_2x^2 + ... + c_{n+m}x^{n+m}$ is such that $c_{n+m} = a_nb_m \neq 0$. This implies that $f(x)g(x) \neq 0$. Thus, $R[x]$ is an integral domain.

The converse follows directly.

In fact, even if R is a field then also $R[x]$ is not a field, for x has no multiplicative inverse.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ be a nonzero polynomial in $R[x]$. If $a_n \neq 0$ then a_n is called the leading coefficient of $p(x)$; and n is called the degree of $p(x)$. It is denoted by $\deg f(x)$. In this case, a_n is called the leading coefficient of $f(x)$. If the leading coefficient is 1, then $f(x)$ is called a monic polynomial.

We do not define degree of the zero polynomial.

Example 2: Consider the polynomial ring $Z_6[x]$. Then $f(x) = [2]x^3 + x + [1]$ and $g(x) = [3]x^2 + [2]$ are two nonzero polynomials of degree 3 and 2, respectively. Now $f(x)g(x) = x^3 + [3]x^2 + [2]x + [2]$ shows that $f(x)g(x) < \deg f(x) + \deg g(x)$

In general, we have the following inequality.

Theorem 2: Let be a commutative ring with unity and $f(x), g(x)$ be two nonzero polynomials in $R[x]$

1. If $f(x)g(x) \neq 0$, then $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$. Equality holds if R is an integral domain.
2. If $f(x) + g(x) \neq 0,$, then $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$

Proof 1: If $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^n$, then $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + a_nb_mx^{n+m}$. If $f(x)g(x) \neq 0$, then at least one of the coefficients of $f(x)g(x)$ is nonzero. Suppose $a_nb_m \neq 0$, then $\deg(f(x)g(x)) = n + m = \deg f(x) + \deg g(x)$. If $a_nb_m = 0$ (which can hold if R has zero divisors), then $\deg(f(x)g(x)) < n + m = \deg f(x) + \deg g(x)$.

2: If $\deg f(x) > \deg g(x)$, then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_m)x^m + ... + a_nx^n$ shows that the leading coefficient of $f(x) + g(x)$ is $a_n \neq 0$ and so $\deg(f(x) + g(x)) = n = \max\{\deg f(x), \deg g(x)\}$. If $\deg f(x) = \deg g(x)$, then

$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+...+(a_n+b_n)x^n$ shows that either $f(x)+g(x)=0$ or $\deg(f(x)+g(x))\le n=\max\{\deg f(x),\deg g(x)\}$ $(=or<accordingly\ a_n+b_n\neq 0\ or=0)$

Now we characterize the units in a polynomial ring $R[x]$.

Theorem 3: Let R be a commutative ring with 1. Then $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n\in R[x]$ is a unit if and only if a_0 is a unit and a_i is nilpotent in $R\,\forall\, i=1,2,...,n$

Proof: First assume that a_0 is a unit and $a_1,a_2,...,a_n$ an are nilpotents in R. Then $a_1x,a_2x^2,...,a_nx^n$ are nilpotents and so $a_1x+a_2x^2+...+a_nx^n$ is a nilpotent in $R[x]$. Since a_0 is a unit, so it follows that $a_0+a_1x+a_2x^2+...+a_nx^n$ is a unit.

We prove the converse by induction on the $\deg f(x)$. If $\deg f(x)=0$, then the result follows directly. Let us make our induction hypothesis that the result holds for every nonzero polynomial of degree less than n. Let $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ be a unit in $R[x]$. Then there is a polynomial $b_0+b_1x+b_2x^2+...+b_mx^m\in R[x]$ such that

$(a_0+a_1x+a_2x^2+...+a_nx^n)(b_0+b_1x+b_2x^2+...+b_mx^m=1$

This implies that

$$a_0b_0=1 \qquad (1)$$

$$a_0b_1+a_1b_0=0 \qquad (2)$$

$$a_0b_2+a_1b_1a_2b_0=0 \qquad (3)$$

.

.

.

$$a_{n-2}b_m+a_{n-1}b_{m-1}+a_nb_{m-2}=0 \qquad (4)$$

$$a_{n-1}b_m+a_nb_{m-1}=0 \qquad (5)$$

$$a_nb_m=0 \qquad (6)$$

We multiply a_n to both sides of (5) and get

$$a_n{}^2b_{m-1}=0$$

Again multiplying $a_n{}^2$ to both sides of (4), we get

$$a_n{}^3b_{m-2}=0$$

Proceeding similarly we get $a_n^{m+1}b_0 = 0$. Since, by (1), b_0 is a unit, so $a_n^{m+1} = 0$. Thus $a_n = 0$ is a nilpotent and so is $a_n x^n = 0$. Then it follows that $g(x) = f(x) - a_n x^n = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$ is a unit, since $f(x)$ is a unit. Since $\deg g(x) < n$, so a_0 is a unit and $a_1, a_2, ..., a_{n-1}$ are nilpotents in R, by the induction hypothesis. Thus the result follows.

13.4 *DIVISION ALGORITHM*

In the ring Z of all integers, for any two nonzero integers m and n, we have unique integers q and r such that $n = mq + r$, where $0 \le r \le |m|$. The usual process, we do for computing q and r, is known as long division (Division Algorithm).

Let us define divisibility first. Let $f(x)$ and $g(x)$ be two nonzero polynomials in $R[x]$. If there exists $q(x) \in R[x]$ such that $f(x) = q(x)g(x)$, then we say that $g(x)$ divides $f(x)$ or that $g(x)$ is a factor of $f(x)$. It is denoted by $g(x) \mid f(x)$

Theorem 4 (Division Algorithm): Let R be a commutative ring with 1 and $f(x), g(x)$ be two nonzero polynomials in $R[x]$ such that the leading coefficient of $g(x)$ is a unit in R. Then there exist unique polynomials $q(x), r(x) \in R[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

Proof: We initially prove the existence of such polynomials $q(x)$ and $r(x)$. Note that $g(x)$ is a nonzero polynomial, since the leading coefficient is nonzero. If $g(x) \mid f(x)$, then there exists $q(x) \in R[x]$ s.t. $f(x) = g(x)q(x)$ which gives the desired presentation where $r(x) = 0$. If $g(x) \nmid f(x)$, then consider the set

$S = \{f(x) - q(x)g(x) \mid q(x) \in R[x]\}$.

Now, by the well-ordering principle, the set $N = \{\deg h(x) \mid h(x) \in S\}$ (since $g(x) \nmid f(x)$, so S does not contain the zero polynomial), we have a polynomial $r(x)$ having the least degree among all polynomials in S. Then there exists $q(x) \in R[x]$ such that $f(x) = g(x)q(x) + r(x)$. So it is sufficient to show that $\deg r(x) < \deg g(x)$. Let $g(x) = a_0 + a_1 x + ... + a_n x^n$ and $r(x) = b_0 + b_1 x + ... + b_m x^m$. Since a_n is a unit so a_n^{-1} exists in R. Suppose, on the contrary, $\deg r(x) \ge \deg g(x)$. Let we define

$$s(x) = r(x) - b_m a_n^{-1} x^{m-n} g(x).$$

Then $s(x) \neq 0$, otherwise $r(x) = b_m a_n^{-1} x^{m-n} g(x)$ and $f(x) = (q(x) + b_m a_n^{-1} x^{m-n}) g(x)$ which contradicts $g(x) \nmid f(x)$. Now $s(x) = f(x) - (q(x) + b_m a_n^{-1} x^{m-n}) g(x)$ shows that $s(x) \in S$ and then

$\deg s(x) < \deg r(x)$

contradicts the choice of $r(x)$ in S. Therefore $\deg r(x) < \deg g(x)$.

To prove the uniqueness of $q(x)$ and $r(x)$, assume that there are polynomials $q'(x), r'(x) \in R[x]$ such that

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x), r'(x) = 0$ or $\deg r'(x) < \deg g(x)$. Then

$$r(x) - r'(x) = (q'(x) - q(x))g(x).$$

If $r(x) - r'(x) \neq 0$ then $q'(x) - q(x) \neq 0$, and since the leading coefficient of $g(x)$ is a unit,

$\deg((q'(x) - q(x))g(x) = \deg(q'(x) - q(x)) + \deg g(x) \geq \deg g(x)$, that is

$\deg(r(x) - r'(x)) \geq \deg g(x),$

Which is impossible since $\deg r(x), \deg r'(x) < \deg g(x)$. Thus, $r(x) - r'(x) = 0$. Then

$0 = (q'(x) - q(x))g(x),$

$\Rightarrow q'(x) - q(x) = 0$, since the leading coefficient of $g(x)$ is a unit.

Thus $r(x) = r'(x)$ and $q'(x) = q(x)$

Definition: Let R be a commutative ring with 1 and $f(x), g(x)$ be two nonzero polynomials in $R[x]$ such that the leading coefficient of $g(x)$ is a unit in R. Then the unique polynomials $q(x), r(x) \in R[x]$ in the above Theorem, are called the quotient and remainder, respectively, after dividing $f(x)$ by $g(x)$.

Let R be a commutative ring with 1 and $f(a) = a_0 + a_1 a + ... + a_n x^n \in R[x]$. For all $a \in R$ we define

$f(a) = a_0 + a_1 a + ... + a_n a^n$

Definition: Let R be a commutative ring with 1 and $f(x) \in R[x]$ be two nonzero polynomials. If $r \in R$ is such that $f(r) = 0$, then r is called a root or zero of $f(x)$. A root r is said to be of multiplicity $m \geq 1$ if $f(x) = (x - r)^m g(x)$ where $g(x) \in R[x]$ is such that $g(r) \neq 0$.

Theorem 5 (Remainder theorem): Let R be a commutative ring with 1, $f(x) \in R[x]$ be a nonzero polynomial and $a \in R$. Then there exists unique $q(x) \in R[x]$ such that

$$f(x) = (x - a)q(x) + f(a)$$

Proof: Denote $g(x) = (x - a)$. Then the leading coefficient of $g(x)$ is 1, a unit in R, and so there are

unique $q(x), r(x) \in R[x]$ such that $f(x) = (x-a)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Now if $r(x) \neq 0$, then deg $r(x) < 1$ shows that $r(x) \in R$. Thus in either case $r(x) = b \in R,$, and we have $f(x) = (x-a)q(x) + b$. This implies that $f(a) = b$, and hence $f(x) = (x-a)q(x) + f(a)$.

Corollary 1(Factorization Theorem): Let R be a commutative ring with 1, $f(x) \in R[x]$ a non zero polynomial and $a \in R$. Then $x - a \mid f(x)$ if and only if a is a root of $f(x)$.

Thus a is a root of $f(x)$ if and only if $f(x) = (x-a)q(x)$ for some $q(x) \in R[x]$. This immediately

gives us the following result

Theorem 6: If R is an integral domain and $f(x)$ is a nonzero polynomial in $R[x]$ of degree n, then $f(x)$ has at most n roots in R counted according to multiplicity.

Proof: We will prove this theorem by induction on $\deg f(x) = n$. If $n = 0$, then $f(x)$ is a nonzero constant in R and hence has no roots. Let us assume $n > 0$. If $f(x)$ has no roots in R, the result holds. Suppose $f(x)$ has a root, say $a \in R$. Then $f(x) = (x-a) f_1(x)$. Since R is an integral domain, so $\deg f_1(x) = n - 1$. Then $f_1(x)$ has at most $n-1$ roots in R, by the induction hypothesis. Also, if $b \neq a$ is a root of $f(x)$ in R, then $f(b) = (b-a) f_1(b)$

$\Rightarrow f_1(b) = 0$

since R is an integral domain, that is, b is a root of $f_1(x)$. Therefore $f(x)$ has at most n roots in R.

Corollary 2: Let R be an integral domain and $f(x), g(x) \in R[x]$ such that $\deg f(x), \deg g(x) \leq n$. If $f(a) = g(a)$ for $n+1$ elements $a \in R$, then $f(x) = g(x)$

Proof: If, on the contrary, $f(x) \neq g(x)$, then $h(x) = f(x) - g(x)$ is a nonzero polynomial over R such that $\deg h(x) \leq n$ and $h(x)$ has at least $n+1$ roots in R. This theorem is the contradiction of theorem 6. Therefore $f(x) = g(x)$.

13.5 *ARITHMETIC OF POLYNOMIAL*

Theorem 7: Every ideal in $F[x]$ is principal ideal, where F is principal ideal.

Proof: Let I be an ideal of $F[x]$. If $I = \{0\}$, then $I = <0>$. Suppose $I \neq \{0\}$. By the well-ordering principle on the set $N = \{\deg f(x) \mid 0 \neq f(x) \in F[x]\}$ we have a polynomial, say $d(x) \in I$ with the least degree in I. Then $<d(x)> \subseteq I$. For the reverse inclusion, let $f(x) \in I$. By the Division Algorithm, there are $q(x), r(x) \in F[x]$ such that $f(x) = d(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg d(x)$. If $r(x) \neq 0$, then $r(x) = f(x) - d(x)q(x) \in I$ contradicts that $d(x)$ is a polynomial

of least degree in I. Hence $r(x) = 0, f(x) = d(x)q(x) \in < d(x) >$, and so $I \subseteq < d(x) >$. Thus $I = < d(x) >$. is a principal ideal.

Suppose $f(x), g(x) \in F[x]$ be two polynomials. A nonzero polynomial $d(x) \in F[x]$ is called a common divisor of $f(x)$ and $g(x)$ if $d(x) \mid f(x)$ and $d(x) \mid g(x)$. If $f(x)$ and $g(x)$ are not both zero, then the ideal $< f(x), g(x) >$ is a principal ideal and so there is $d(x) \in F[x]$ such that $< f(x), g(x) > = < d(x) >$ then $d(x) \mid f(x)$ and $d(x) \mid g(x)$. This shows that every divisor of $d(x)$ is a common divisor of $f(x)$ and $g(x)$. Thus common divisor of polynomials $f(x)$ and $g(x)$ exists in $F(x)$ and there may be several common divisors. To introduce a polynomial equivalent of the concept of the greatest common divisor (gcd) of two integers, the first difficulty is that there is no natural or standard partial ordering between polynomials that allows us to make our choice unique by considering the 'greatest' among all common divisors. If $d(x)$ and $d'(x)$ are two gcd of $f(x)$ and $g(x)$, then our experience in Z shows that $d(x) \mid d'(x)$ and $d'(x) \mid d(x)$

$\Rightarrow d'(x) = ad(x)$ for some $a \in F^*$

To get some degree of uniqueness, we need begin with the monic common divisors.

Definition: Let $f(x), g(x) \in F[x]$ be two polynomials not both zero. Then a polynomial $d(x) \in F[x]$ is called a greatest common divisor of $f(x), g(x)$ if $d(x)$ is a monic polynomial such that:

1. $d(x) \mid f(x)$ and $d(x) \mid g(x)$
2. $c(x) \mid f(x)$ and $c(x) \mid g(x) \Rightarrow c(x) \mid d(x)$

Now we have to show that the gcd of $f(x), g(x)$ exists in $F[x]$ uniquely.

Theorem 8: Let $f(x), g(x) \in F[x]$ be two polynomials not both zero. Then gcd of $f(x), g(x)$ exists in $F[x]$ and it is unique.

Moreover, if $d(x)$ is the gcd of $f(x), g(x)$, then there exist $u(x), v(x) \in F[x]$ such that $d(x) = f(x)u(x) + g(x)v(x)$

Proof: Consider $I = \{ f(x)r(x) + g(x)s(x) \mid r(x), s(x) \in F[x] \}$. Then I is the ideal $< f(x), g(x) >$ of $F[x]$ generated by $f(x)$ and $g(x)$. It is a nonzero ideal since either of $f(x)$ and $g(x)$ is nonzero. Since F is a field, every ideal of $F[x]$ is principal. Suppose $d_1(x) = a_0 + a_1 x + ... + a_n x^n \in F[x], a_n \neq 0$ is such that $I = < d_1(x) >$. Since F is a field, so that a_n^{-1} exists in F and $d(x) = a_n^{-1} d_1(x) \in F[x]$ is a monic polynomial such that $< d(x) > = < d_1(x) > = < f(x), g(x) >$. Then $f(x), g(x) \in < d(x) >$

$\Rightarrow d(x)$ d(x) is common divisor of the polynomials $f(x), g(x)$. Now $d(x) \in < f(x), g(x) >$

$$d(x) = f(x)u(x) + g(x)v(x)$$

for some $u(x), v(x) \in F[x]$. If $h(x) \in F[x]$ is a common divisor of $f(x), g(x)$, then $h(x) \mid f(x)u(x) + g(x)v(x) = d(x)$. Thus $d(x)$ is a greatest common divisor of $f(x), g(x)$.

To prove the uniqueness of gcd, consider a gcd $c(x) \in F[x]$ of $f(x), g(x)$. Then $c(x) \mid d(x)$ and $d(x) \mid c(x)$, and so $d(x) = ac(x)$ for some a $a \in F^*$. Since both $c(x)$ and $d(x)$ are monic, it follows that $c(x) = d(x)$

We denote the gcd of $f(x), g(x)$ by $\gcd(f(x), g(x))$.

Example 3: Consider two polynomials $f(x) = 2(x-1)(x-2)$ and $g(x) = 2(x-2)(x-3)$ over R. Then $d(x) = x-2$ is the monic common divisor of $f(x)$ and $g(x)$ of greatest degree. Thus $\gcd(f(x), g(x)) = x-2.$

Definition: Let $f(x)$ and $g(x)$ two polynomials in $F[x]$ not both zero. If $\gcd(f(x), g(x)) = 1$, then $f(x), g(x)$ are said to be relatively prime.

Theorem 9: Two polynomials $f(x), g(x) \in F[x]$ are relatively prime if and only if $1 = f(x)u(x) + g(x)v(x)$ for some $u(x), v(x) \in F[x]$.

Proof: Let $1 = f(x)u(x) + g(x)v(x)$, where $u(x), v(x) \in F[x]$. If $d(x) = \gcd(f(x), g(x))$, then

$\Rightarrow d(x) \mid f(x), d(x) \mid g(x)$

$\Rightarrow d(x) \mid 1$

Since $d(x)$ is monic, so it follows that $d(x) = 1$. Hence $f(x)$ and $g(x)$ are relatively prime.

Converse of this theorem will be follows from Theorem 8.

Corollary 3: Let K be a subfield of F and $f(x), g(x) \in K[x]$. Then $f(x)$ and $g(x)$ are relatively prime in $K[x]$ if and only if so in $F[x]$.

Proof: Let $f(x)$ and $g(x)$ be relatively prime in $K[x]$. Then $1 = f(x)u(x) + g(x)v(x)$ for some $u(x), v(x) \in K[x]$. Since $K[x] \subseteq F[x]$, it follows that $1 = \gcd(f(x), g(x))$ in $F[x]$, by Theorem 9.

Conversely, assume that $f(x)$ and $g(x)$ be relatively prime in $F[x]$. Then $1 = f(x)u(x) + g(x)v(x)$ for some $u(x), v(x) \in F[x]$. Let $d(x) = \gcd(f(x), g(x))$ in $K[x]$. Then $d(x) \mid f(x), d(x) \mid g(x)$ and $d(x) \mid f(x)u(x) + g(x)v(x)$ in $F[x]$. It follows that $d(x) \mid 1$, and since $d(x)$ is monic, so $d(x) = 1$. Thus $f(x)$ and $g(x)$ are relatively prime in $K[x]$.

Definition: Let F be a field. A nonconstant polynomial $f(x) \in F[x]$ of degree n is called irreducible over F if there is no factorization $f(x) = g(x)h(x)$ in $F[x]$ such that $\deg f(x) < n$ and $\deg g(x) < n$. In the other way $f(x)$ is said to be reducible.

Thus, a nonconstant polynomial $p(x)$ is irreducible *iff* it has only two monic divisors 1 and $a^{-1}p(x)$ where, a is leading coefficient of $p(x)$.

Theorem 10: Let F be a field and $f(x), p(x) \in F[x]$. If $p(x)$ is irreducible, then

$$\gcd(p(x), f(x)) = 1 \quad \text{if } p(x) \nmid f(x)$$
$$= a^{-1}p(x) \quad \text{if } p(x) \mid f(x)$$

Where, a is leading cofficient of $p(x)$.

Proof: Let $p(x) \nmid f(x)$. Since $p(x)$ is irreducible, so it has no monic divisors other than 1 and $a^{-1}p(x)$

Where, a is leading coefficient of $p(x)$. But $a^{-1}p(x)$ is not a divisor of $f(x)$, since $p(x) \nmid f(x)$.

Hence $\gcd(p(x), f(x)) = 1$

If $p(x) \mid f(x)$, then $a^{-1}p(x)$ is the monic common divisor of highest degree. It follows that $\gcd(p(x), f(x)) = a^{-1}p(x)$.

Theorem 11: Let F be a field and $p(x) \in F[x]$. Then $p(x)$ is irreducible *iff* for any $f(x), g(x) \in F[x], p(x) \mid f(x)g(x)$ implies either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Proof: Let $p(x) \mid f(x)g(x)$ and $p(x) \nmid f(x)$. Since $p(x)$ is irreducible, so $1 = \gcd(p(x), f(x))$. Then $1 = p(x)u(x) + f(x)v(x)$ for some $u(x), v(x) \in F[x]$. It follows that $g(x) = p(x)g(x)u(x) + f(x)g(x)v(x)$. Now $p(x) \mid f(x)g(x)$

$\Rightarrow p(x) \mid p(x)g(x)u(x) + f(x)g(x)v(x)$, i.e., $p(x) \mid g(x)$

Conversely, let $p(x) = f(x)g(x)$. Then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$. If $p(x) \mid f(x)$, then

$\deg p(x) \le \deg f(x) \le \deg f(x) + \deg g(x) \le \deg p(x)$

$\Rightarrow \deg p(x) = \deg g(x)$.

Similarly, if $p(x) \mid g(x)$, then $\deg p(x) = \deg g(x)$. Thus $p(x)$ is an irreducible polynomial.

The relevance of prime integers is undeniably demonstrated in the Fundamental Theorem of Arithmetic. A similar conclusion is obtained here, demonstrating that every nonconstant polynomial over a field may be represented as a combination of irreducible polynomials.

Theorem 12: Let F be a fied. Then every non constant polynomial $f(x) \in F[x]$ can be written uniquely as a product of a nonzero constant and monic irreducible polynomials in $F[x]$ up to the order of the irreducible factors.

Proof: We initially prove that, the existence of such factorization by using the mathematical induction on $n = \deg f(x)$. If $n = 1$ then $f(x) = ax + b; a \neq 0$. Since F is a field, so $a^{-1}1$ exists in F and

$x + a^{-1}b$ is a monic irreducible polynomial in $F[x]$. Then $f(x) = a(x + a^{-1}b)$ shows that we are done for $n = 1$. Let $f(x)$ be a polynomial of degree $n > 1$ and leading coefficient a. If $f(x)$ is irreducible, then $f(x) = a(a^{-1}f(x))$ is a desired factorization. If $f(x)$ is reducible then $f(x) = g(x)h(x) \in F[x]$ in F[x] with $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$. By the induction hypothesis, $g(x) = bp_1(x)p_2(x)...p_r(x), h(x) = cq_1(x)q_2(x)...q_s(x)$ and $f(x) = bcp_1(x)p_2(x)...p_r(x)q_1(x)q_2(x)...q_s(x)$ where $b, c \in F$ and $p_i(x), q_i(x)$ are monic irreducible polynomials in $F[x]$.

Now, to prove the uniqueness of the factorization, let us suppose

$ap_1(x)p_2(x)...p_m(x) = bq_1(x)q_2(x)...q_n(x)$

where $a, b \in F$ and $p_i(x), q_i(x)$ are monic irreducible polynomials in $F[x]$. Since all $p_i(x), q_i(x)$ are monic, so $a = b$. Then $p_1(x)p_2(x)...p_m(x) = q_1(x)q_2(x)...q_n(x)$

$\Rightarrow q_1(x) \mid p_1(x)p_2(x)...p_m(x)$

Since $q_1(x)$ is irreducible, so either of $p_1(x)p_2(x)...p_m(x)$ is divisible by $q_1(x)$, say $q_1(x) \mid p_1(x)$. It follows that $p_1(x) = q_1(x)$, since both $p_1(x)$ and $q_1(x)$ are monic and irreducible

$\Rightarrow p_2(x)...p_m(x) = q_2(x)...q_n(x)$ (By the cancellation property)

Continuing cancelation of irreducible factors, we get $p_{n+1}(x)p_2(x)...p_m(x) = 1$ if $m > n$ or $q_{m+1}(x)q_2(x)...q_n(x) = 1$ if $n > m$, which is a contradiction, since every irreducible polynomial is non constant. Thus $m = n$ and after reindexing, $p_i(x) = q_i(x)$.

13.6 *IRREDUCIBILITY OF POLYNOMIAL*

There is a simple characterization on irreducibility of polynomials of degree 2 or 3.

Theorem 13: Let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Then $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.

Proof: First suppose that $\deg f(x) = 3$ and $f(x)$ has a root in F, say a. Then $x - a$ divides $f(x)$ in $F[x]$ and so $f(x) = (x - a)q(x)$ for some $q(x) \in F[x]$. Thus $f(x)$ is reducible over F.

Conversely suppose that $f(x)$ is reducible over F. Then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ with $\deg g(x) \geq 1$ and $\deg h(x) \geq 1$. Now $\deg(g(x)h(x)) = 3$ shows that either $\deg g(x) = 1$ and $\deg h(x) = 2$ or $\deg g(x) = 2$ and $\deg h(x) = 1$. If $\deg g(x) = 1$, then $g(x) = ax + b$ for some

$a,b \in F, a \neq 0$. Now $-a^{-1}b \in F$ shows tha $g(-a^{-1}b) = 0$ shows that $f(-a^{-1}b) = 0$ has a root in F. If $h(x) = 1$, then similarly $f(x)$ has a root in F.

A similar argument can be used for the case when $\deg f(x) = 2$.

Example 4: Consider $f(x) = x^2 + x + [1] \in Z_2[x]$. Then $f([0]) = [0]^2 + [0] + [1] \neq [0]$ and $f([1]) = [1]^2 + [1] + [1] \neq [0]$ shows that $f(x)$ has no roots in Z_2. Also $\deg f(x) = 2$. Thus, by theorem 13, $f(x)$ is irreducible over Z_2.

Example 5: Consider $f(x) = (x^2 + 1)(x^2 + 2) \in Q[x]$. Then $f(x)$ has no root in Q, still it is reducible over Q. Thus the above result does not hold for polynomials of degree more than 3.

Theorem 13 is an appropriate criteria for assessing polynomial irreducibility over finite fields. Because the nonexistence of roots in an infinite field is difficult to verify, it does not operate well over an infinite field. Now we demonstrate a lovely strategy for checking the nonexistence of roots of a polynomial over Q in a finite number of steps. We'll start with a well-known lemma known as Gauss's Lemma.

If $f(x) = a_0 + a_1 x + ... + a_n x^n \in Z[x]$, then for any $m \in N$ denote $\overline{f}(x) = [a_0] + [a_1]x + ... + [a_n]x^n \in Z_m[x]$. Since $\psi : Z \to Z_m$ defined by $\psi(a) = [a]$ is a ring homomorphism, so it follows that $\psi^* : Z[x] = Z_m[x]$ given by $\psi^*(f(x)) = \overline{f}(x)$ is a ring homomorphism.

Lemma 1: Let $f(x) \in Z[x]$. If $f(x) = G(x)H(x)$ over Q where $\deg G(x), \deg H(x) < \deg f(x)$ then there are $g(x), h(x) \in Z[x]$ with $\deg G(x) = \deg g(x)$ and $\deg H(x) = \deg h(x)$ s.t. $f(x) = g(x)h(x)$.

Proof: Let $n_1, n_2 \in Z$ be such that $n_1 G(x), n_2 H(x) \in Z[x]$. Consider $g_1(x) = n_1(x)G(x), h_1(x) = n_2 H(x)$ and $n = n_1 n_2$. Then

$$nf(x) = n_1 G(x) n_2 H(x) = g_1 h_1(x)$$

If p is a prime divisor of n, then the identity $nf(x) = g_1(x)h_1(x)$ becomes $\overline{g_1(x)h_1(x)} = 0$ in $Z_p[x]$. Since $Z_p[x]$ is an integral domain, so at least one of $\overline{g_1(x)}$ and $\overline{h_1(x)}$ say is 0. Hence p divides all the coefficients of $\overline{g_1(x)}$, that is, $\overline{g_1(x)} = pg_2(x)$ for some $g_2(x) \in Z[x]$. If $n = pm$, then

$$pmf(x) = pg_2(x)h_1(x)$$

$\Rightarrow mf(x) = g_2(x)h_1(x)$. Note that $\deg g_2(x) = \deg g_1(x) = \deg G(x)$ and $\deg h_1(x) = \deg H(x)$.

Continuing cancelation of prime factors of n, we reach our desired factorization $f(x) = g(x)h(x)$ in $Z[x]$.

Theorem 14: Let $f(x) = a_0 + a_1x + ... + a_nx^n \in Z[x]$ be a polynomial of degree $n > 1$. If there exists a prime p such that $\overline{f(x)} = [a_0] + [a_1]x + ... + [a_n]x^n$ is of degree n and irreducible over Z_p, then $f(x)$ is irreducible over Q.

Proof: Suppose that p is a prime such that $\deg \overline{f(x)}$ is n and $\overline{f(x)}$ is irreducible over Z_p. If possible, let $f(x)$ be reducible over Q. Then there exist polynomials $g(x) = b_0 + b_1x + ... + b_kx^k$ and

$h(x) = c_0 + c_1x + ... + c_lx^l$ in $Z[x]$, $0 < k, l < n$ such that $f(x) = g(x)h(x)$. Then $n = k + l$. Since degree of $\overline{f}(x) = ([b_0] + [b_1]x + ... + [b_k]x^k)([c_0] + [c_1]x + ... + [c_l]x^l)$ is $n = k + l$, it follows that $[b_k][c_l] \neq [0]$ in Z_p, and hence $[b_k] \neq [0]$ and $[c_l] \neq [0]$. Consequently, $\overline{g}(x)$ and $\overline{h}(x)$ are nonconstant polynomials in $Z_p[x]$. $\Rightarrow \overline{g}(x)$ and $\overline{h}(x)$ are non units, since the nonzero elements

of Zp are the only units of $Z_p[x]$. Hence $\overline{f}(x)$ is reducible over Z_p, a contradiction. Thus $f(x)$ is irreducible over Q.

Example 6: Suppose the polynomial $f(x) = 7x^3 + 8x + 2$ over Q. Then in $Z_3[x]$, $\overline{f}(x) = x^3 + [2]x + [2]$. Now $\overline{f}([0]) = [2]$, $\overline{f}([1]) = [2]$ and $\overline{f}([2]) = [2]$ shows that $\overline{f}(x)$ has no root in $Z_3[x]$. Thus $\overline{f}(x)$ is irreducible over Z_3 and hence $f(x)$ is irreducible over Q.

13.7 *EISENSTEIN'S CRITERIA FOR IRREDUCIBLITY*

Now we will learn about the famous Eisenstein's criterion for irreducibility of polynomials over Q.

Theorem 15: Eisenstein's irreducibility criterion (EIC) Let $f(x) = a_0 + a_1x + ... + a_nx^n \in Z[x]$. If there is a prime integer p such that $p \mid a_i$ for all $i < n$, $p \nmid a_n$ and $p^2 \nmid a_n$, then $f(x)$ is irreducible over Q.

Proof: Assume, on the contrary, that $f(x)$ is reducible over Q. Then by Gauss's lemma

$f(x) = (b_0 + b_1x + ... + b_kx^k)(c_0 + c_1x + ... + c_mx^m)$

in $Z[x]$ where $k, m < n$. Let $g(x) = b_0 + b_1x + ... + b_kx^k$ and $h(x) = c_0 + c_1x + ... + c_mx^m$. Then we have $\overline{f(x)} = \overline{g(x)h(x)}$ in $Z_p[x]$. Since $p \nmid a_n$, so $[a_n]$ is a unit in Z_p. Then $p \mid a_i$ for all $i < n$ implies $\overline{f(x)} = ux^n$. Because irreducible polynomial factorization over a field is unique, so we have and $\overline{g(x)} = ux^k$ and $\overline{h(x)} = vx^m$ where u and v are units in Z_p. Thus $[b_0] = [0] = [c_0]$ in Z_p,

$\Rightarrow p \mid b_0$ and $p \mid c_0$. Then $p^2 \mid b_0c_0 = a_0$, a contradiction. Hence $f(x)$ is irreducible in $Q[x]$.

Example 7: Let $f(x) = x^5 + 12x^4 + 9x^2 + 6$. Then $3 \mid 6, 3 \mid 9, 3 \mid 12, 3 \nmid 1, 3^2 \nmid 6$ shows that $f(x)$ is irreducible over Q, by Eisenstein's criterion.

Corollary 4: For every prime integer p, the p*-th* cyclotomic polynomial

$$\phi_p(x) = 1 + x + ... + x^{p-1}$$

is irreducible over Q.

Proof: Note that $\phi_p(x) = \dfrac{x^p - 1}{x - 1}$ which implies

$$\phi_p(x+1) = x^{p-1} + x^{p-2} + ... + p$$

Since p is prime, we have $p \mid \forall i, 0 < i < p$. Hence $\phi_p(x+1)$ is irreducible in $Q[x]$, by

Eisenstein's criterion and it follows that $\phi_p(x)$ is irreducible over Q.

Irreducible polynomials are commonly utilised in abstract algebra applications such as coding theory, Galois theory, and so on. We show how to employ irreducible polynomials to build finite fields of non-prime order. First, we show the following fact, which is essential for building finite fields.

Theorem 16: Let F be a field and $p(x)$ be a nonzero polynomial over F. Then the following conditions are equivalent:

(*i*) $p(x)$ is irreducible;

(*ii*) $F[x] / < p(x) >$ is an integral domain;

(*iii*) $F[x] / < p(x) >$ is a field.

Proof: $(i) \Rightarrow (iii)$: $F[x]/<p(x)>$ is a commutative ring with unity, since $F[x]$ is so. Consider a nonzero element $F[x]+<p(x)>$ of $F[x]/<p(x)>$. Then $f(x) \notin <p(x)>$ and so $p(x) \nmid f(x)$ in $F[x]$. Since $p(x)$ is irreducible, so $1 = \gcd(p(x), f(x))$. Then $u(x)f(x)+v(x)p(x)=1$, for some

$u(x), v(x) \in F[x]$

$\Rightarrow (u(x)+<p(x)>)(f(x)+<p(x)>) = 1+<p(x)>$. Thus

$f(x)+<p(x)>$ is a unit in $F[x]/<p(x)>$ and hence $F[x]/<p(x)>$ is a field.

$(iii) \Rightarrow (ii)$: Follows trivially.

$(ii) \Rightarrow (i)$ (ii)): $F[x]/<p(x)>$ is an integral domain and so contains at least two elements. Thus $F[x] \neq <p(x)>$ and so $p(x)$ is a non constant. Suppose that $p(x) = f(x)g(x)$, for some $f(x), g(x) \in F[x]$. Then $f(x), g(x) \in <p(x)>$

$\Rightarrow (f(x)+<p(x)>)(g(x)+<p(x)>) = 0+<p(x)>$.

Since $F[x]/<p(x)>$ contains no zero divisor, it follows that $f(x)+<p(x)> = 0+<p(x)>$ or

$g(x)+<p(x)> = 0+<p(x)>$, equivalently $f(x) \in <p(x)> or\ g(x) \in <p(x)>$. If $f(x) \in <p(x)>$ then there is $q(x) \in <p(x)>$ such that $f(x) = p(x)q(x)$. Hence $p(x) = f(x)g(x) = p(x)q(x)g(x)$ and so $\deg g(x) = 0$. Thus $g(x)$ is a unit. Similarly, if $g(x) \in <p(x)>$, then $f(x)$ is a unit. Thus $p(x)$ is irreducible over F.

Example 8: Consider the irreducible polynomial $f(x) = x^2 + x + [1] \in Z_2[x]$. Then it follows that $F = Z_2[x]/<x^2 + x + [1]> = \{f(x)+<x^2 + x + [1]> \mid f(x) \in Z_2[x]\}$ is a field. We show that this is a field of four elements. Now the Division Algorithm implies that for every $f(x) \in Z_2[x]$ there are unique polynomials $q(x), r(x) \in Z_2[x]$ such that

$f(x) = (x^2 + x + [1])q(x) + r(x)$

where $r(x) = 0$ r(x) = 0 or $\deg r(x) < \deg(x^2 + x + [1]) = 2$. Then $r(x) = [a]x + [b]$ for some $[a], [b] \in Z_2$. Now $f(x) - ([a]x + [b]) = (x^2 + x + [1])q(x) \in <x^2 + x + [1]>$

$\Rightarrow F = Z_2[x]/<x^2 + x + [1]>$

$= \{f(x)+<x^2 + x + [1]> \mid f(x) \in Z_2[x]\}$

$= \{([a]x + [b]) + < x^2 + x + [1] > | [a], [b] \in Z_2\}$

$= \{0 + < x^2 + x + [1] >, [1] + < x^2 + x + [1] >, x + < x^2 + x + [1] >, x + [1] + < x^2 + x + [1] >\}$.

Thus F is a field of four elements.

Check your progress

Problem 1: Check the polynomial $f(x) = 1 + x + x^2 + x^3 + x^4$ is irreducible over Q?

Problem 2: Check the polynomial $f(x) = x^5 + 15x^4 + 10x^2 + 5$ is irreducible over Q?

13.8 *SUMMARY*

In this unit, we have learned about the important definition of polynomial ring, irreducible polynomial and important concept of Eisenstein's criteria of irreducibility of a polynomial over Q. The overall summarization of this units are as follows:

- If F is a field then every ideal in $F[x]$ is principal ideal.
- $R[x]$ is an integral domain if and only if R is an integral domain.
- Two polynomials in $F[x]$, $f(x)$ and $g(x)$ not both zero are said to be relatively prime if $\gcd(f(x), g(x)) = 1$.
- A nonconstant polynomial $p(x)$ is irreducible *iff* it has only two monic divisors 1 and $a^{-1}p(x)$ where, a is leading coefficient of $p(x)$.
- Eisenstein's irreducibility criterion: Let $f(x) = a_0 + a_1x + ... + a_nx^n \in Z[x]$. If there is a prime integer p such that $p \mid a_i$ for all $i < n$, $p \nmid a_n$ and $p^2 \nmid a_n$, then $f(x)$ is irreducible over Q.

13.9 *GLOSSARY*

- **GCD:** Greatest common divisor
- **EIC:** Eisenstein's irreducibility criterion
- **Eisenstein's irreducibility criterion:** Let $f(x) = a_0 + a_1x + ... + a_nx^n \in Z[x]$. If there is a prime integer p such that $p \mid a_i$ for all $i < n$, $p \nmid a_n$ and $p^2 \nmid a_n$, then $f(x)$ is irreducible over Q.

13.10 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.

- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

13.11 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

13.12 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. State and prove the Eisenstein's criteria for irreduciblity over Q.

2. If F be a field and $p(x) \in F[x]$. Then prove that $p(x)$ is irreducible *iff* for any $f(x), g(x) \in F[x], p(x) \mid f(x)g(x)$ implies either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

3. Prove that, if K be a subfield of F and $f(x), g(x) \in F[x]$. Then $f(x), g(x)$ are relative prime in $K[x]$ *iff* so in $F[x]$.

4. If F be a field and $p(x) \in F[x]$. Then prove that $p(x)$ is irreducible iff $f(x), g(x) \in F[x], p(x) \mid f(x)g(x)$ implies that either $p(x) \mid f(x)$ or $p(x) \mid g(x)$

5. Prove that each non constant polynomial $f(x) \in F[x]$ can be expressed uniquely as a product of a nonzero constant and monic irreducible polynomials in $F[x]$ up to the order of the irreducible factors.

6. Prove that every ideal in $F[x]$ is principal ideal, where F is field.

Short Answer Type Question:

7. Show that the polynomial $f(x) = x^5 + 15x^4 + 10x^2 + 5$ is irreducible over Q.

8. Prove that p *-th* cyclotomic polynomial $\phi_p(x) = 1 + x + ... + x^{p-1}$ is irreducible over Q.

9. Prove that two polynomials $f(x), g(x) \in F[x]$ are relatively prime if and only if $1 = f(x)u(x) + g(x)v(x)$ for some $u(x), v(x) \in F[x]$.

10. Find the gcd of the polynomials $f(x) = 2(x-1)(x-2)$ and $g(x) = 2(x-2)(x-3)$.

11. If D is an integral domain and $f(x) \neq 0$ is a polynomial in $D[x]$ of degree n, then prove that $f(x)$ has at most n roots in D counted according to multiplicity.

12. Prove that in a commutative ring R with unity, $D = f(x) \in R[x]$ and $a \in R$ then $x - a \mid f(x)$ *iff* a is root of $f(x)$.

Fill in the blanks:

13. If F is a field then every ideal in $F[x]$ is …….

14. A non constant polynomial $p(x)$ is irreducible *iff* it has only two monic divisors $a^{-1}p(x)$ and …….

15. Two polynomials $f(x), g(x)$ are said to be relative prime if $\gcd(f(x), g(x)) =$ ……

13.13 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes

Answer of terminal question:

9. $(x-2)$ **13.** Principal ideal **14.** 1 **15.** 1

Unit-14: FIELD EXTENSION, GALOIS GROUPS AND GALOIS EXTENSION

CONTENT:

14.1 *INTRODUCTION*

A field extension in mathematics, specifically algebra, is a pair of fields $K \subseteq L$ where the operations of K are L operations confined to K. In this instance, K is a subfield of L and L is an extension field of K. For instance, under the conventional definitions of addition and multiplication, the real numbers are a subfield of the complex numbers, which are an extension field of the real numbers.

The Galois group of a certain kind of field extension is a particular group connected to the field extension in mathematics's branch of abstract algebra known as Galois theory. Galois theory is the study of field extensions and how they relate to the polynomials that give birth to them via Galois groups. It is named after Évariste Galois who made the initial discovery of field extensions.

In algebraic number theory, the study of polynomial roots via Galois theory, and algebraic geometry, field extensions play a key role.

14.2 *OBJECTIVES*

After reading this unit learners will be able to

- Memorized about the extension of fields.
- Analyze about the minimal polynomial in terms of field extension.
- Analyze about the Galois group of polynomial over a field F .

14.3 *EXTENSION OF FIELDS*

As we know that complex numbers are generally ordered pair of real numbers i.e., $C \subseteq R \times R$, and so, in its strict sense $R \not\subseteq C$. Still R is considered as a subfield of C. We can identifying each real number a with the complex number $(a,0)$.

So, what is the justification in doing this?

In the sense of isomorphism. Let we define a mapping $f : R \to C$, for all $a \in R$ s.t.,

$$f(a) = (a,0)$$

Then f is a monomorphism and $R \cong f(R) = \{(a,0) \mid a \in R\}$ which is a subfield of C.

Definition: Let F and K be two fields. F is called an extension or a field extension of K if there is a monomorphism

$$f : K \to F$$

It is denoted by F / K

Since, K is a field and we also know that a field has no ideal other than $\{0\}$ and F itself, every homomorphism $f : K \to F$ is either a zero homomorphism or a one-to-one homomorphism. Thus F is a field extension of K *iff* there is a nonzero homomorphism $f : K \to F$.

Example 1: The mapping $f : R \to C$ defined by for all $a \in R$,

$$f(a) = (a, 0)$$

is a monomorphism. Thus C is a field extension of R.

Similarly, R is a field extension of Q. There are more several field extensions of Q. Now we give some examples.

Example 2: Consider $p(x) = x^2 + 1$ on R. Since $p(x)$ is irreducible over R, $F = R[x] / < x^2 + 1 >$ is a field. Also we have $F = \{ f(x) + < x^2 + 1 > \mid f(x) \in R[x] \}$. Since R is a field, by the division algorithm $f(x) = (x^2 + 1)q(x) + (a + bx)$, where $a, b \in R$. Then $f(x) - (a + bx) = (x^2 + 1)q(x) \in < x^2 + 1 >$ implies that $f(x) + < x^2 + 1 > = a + bx + < x^2 + 1 >$. Thus

$$F = \{a + bx + < x^2 + 1 > | \ a, b \in R\}$$

Define a mapping $f : R \to F$ by: for all $a \in R$,

$$f(a) = a + < x^2 + 1 >$$

Then f is a homomorphism. Now for $a, b \in R$,

$f(a) = f(b) \Rightarrow a + < x^2 + 1 >= b + < x^2 + 1 >$

$\Rightarrow a - b \in < x^2 + 1 >$

$\Rightarrow a - b = (x^2 + 1)q(x)$

for some $q(x) \in R[x]$. If $a - b \neq 0$ then $a - b \in R$

$\Rightarrow \deg(a - b) = 0$, and $q(x)$ is nonzero.

Then $\deg((x^2 + 1)q(x)) = \deg(x^2 + 1) + \deg q(x) \geq 2$ leads to a contradiction. Thus $a = b$ and so f is a monomorphism. Hence F is an extension of R.

Also note that $\sigma : F \to C$ defined by:

$$\sigma(a + bx + < x^2 + 1 >) = a + ib$$

for every $a + bx + < x^2 + 1 > \in F$ is an isomorphism. Thus $F \cong C$.

Example 3: Let $F = Q[x] / < x^2 - 2 >$. Since $x^2 - 2$ is irreducible over Q, F is a field. Also, by the Division Algorithm on $Q[x]$, we have

$$F = \{a + bx + < x^2 - 2 > | \ a, b \in Q\}$$

Define a mapping $f : Q \to Q[x] / < x^2 - 2 >$ by $\forall a \in Q$

$$f(a) = a + < x^2 - 2 >$$

Then f is a homomorphism. Since Q is a field, so f is either a zero homomorphism or a monomorphism. Now $f(1) = 1 + < x^2 - 2 > \neq 0$ implies that f is a nonzero homomorphism. Thus f is a monomorphism. Hence F is an extension of Q.

Also note that $\sigma : F \to Q(\sqrt{2})$ defined by

$$\sigma(a + bx + < x^2 - 2 >) = a + b\sqrt{2}$$

for every $a + bx + < x^2 - 2 > \in F$ is an isomorphism. Thus $F \cong Q(\sqrt{2})$.

Example 4: Give examples of two fields which are not an extension of a field.

1. Q has no proper subfield.

Let K be a subfield of Q. Then $1 \in K$, and so $-1 \in K$. This shows that for all nonzero $a \in Z$,

$$a = 1 + 1 + ... + 1 (a \ times), if \ a > 0$$

$$= (-1) + (-1) + ... + (-1)(-a \ times), if \ a < 0$$

and hence $a \in K$. Thus $Z \subseteq K$ which shows that $Q = Q(Z) \subseteq K$.

2. Z_p has no proper subfield

If $K \subseteq Z_p$ is a subfield of Z_p, then $[1] \in K$

$\Rightarrow [a] = [1] + [1] + ... + [1]$ $(a \ times) \in K$

for every $[a] \in Z_p$. Thus $K = Z_p$

Definition: A field K is called a prime field if it has no proper subfield.

In other words, such domains cannot be thought of as extensions of other disciplines. Q and Z_p are prime fields for any prime integer p. We will now demonstrate that any prime field is isomorphic to any of these fields.

Theorem 1: Every field F is either an extension of Q or an extension of Z_p, for some prime p.

Proof: Define a mapping $f : Z \to F$

s.t., $f(n) = n1, \ n \in Z$

Then f is a homomorphism. Now either $char \, F = 0$ or $char \, F = p$ for some prime integer p.

Assume that $charF = p$. Then, $p1 = 0$

$\Rightarrow p \in \ker f$

$\Rightarrow \ker f \neq \phi$

Hence, $\ker f = mZ$ for some $m > 0$

Again $\text{Im} \, f$ being a subring of F with the same unity, $char \, \text{Im} \, f = char \, F = p$. Then $\text{Im} \, f \cong Z / \ker f \cong Z_m$ shows that $m = char \, \text{Im} \, f = p$. Thus $\text{Im} \, f \cong Z_p$, and hence F has a subfield which is isomorphic to Z_p.

Now assume that $char \, F = 0$. In this case, $\ker f = \{0\}$, and so f is one-to-one. Now we shall show that this f induces an one-to-one homomorphism

$$\psi : Q \to F$$

s.t., $\psi\left(\frac{a}{b}\right) = f(a) f(b)^{-1}$, where $\frac{a}{b} \in Q$ [Since f is 1-1, $f(b) \neq 0 \forall b \neq 0$]

Let $\frac{a}{b}, \frac{c}{d} \in Q$. Then $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow f(ad) = f(bc) \Leftrightarrow f(a) f(d) = f(b) f(c) \Leftrightarrow f(a) f(b)^{-1}$

$= f(c) f(d)^{-1} \Leftrightarrow \psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right)$

$\Rightarrow \psi$ is one-one and as well as defined.

Now $\psi\left(\frac{a}{b}+\frac{c}{d}\right)=\psi\left(\frac{ad+bc}{bd}\right)=f(ad+bc)f(bd)^{-1}=(f(a)f(d)+f(b)f(c))f(b)^{-1}f(d)^{-1}$

$=f(a)f(b)^{-1}+f(c)f(d)^{-1}=\psi\left(\frac{a}{b}\right)+\psi\left(\frac{c}{d}\right)$ and $\psi\left(\frac{a}{b}\frac{c}{d}\right)=\psi\left(\frac{ac}{bd}\right)=f(ac)f(bd)^{-1}$

$=f(a)f(c)f(b)^{-1}f(d)^{-1}=f(a)f(b)^{-1}f(d)^{-1}=f(a)f(b)^{-1}f(c)f(d)^{-1}=\psi\left(\frac{a}{b}\right)\psi\left(\frac{c}{d}\right)$.

Thus F has a subfield which is isomorphic to Q.

Corollary 1: Let F be a prime field.

1. If $char\, F=0$, then $F\cong Q$.

2. If $char\, F=p$, then $F\cong Z_p$.

Let F/K be a field extension. Then there is a monomorphism $\sigma: K\to F$, and so K is isomorphic to $\sigma(K)$, a subfield of F. Also, if K is a subfield of F, then the inclusion mapping $f: K\to F$ is a monomorphism. Hence F is an extension of K. Thus it is of no harm to identify K and its isomorphic image $\sigma(K)$ is an extension F.

Let F/K be a field extension. As we know that arbitrary intersection of subfields of F is a subfield of F, given any $c_1,c_2,...,c_n\in F$ there is the smallest subfield that contains $K\cup\{c_1,c_2,...,c_n\}$. This is called the subfield of F generated by $c_1,c_2,...,c_n$ over K and is denoted by $K(c_1,c_2,...,c_n)$. For $c\in F, K(c)$ is of our special interest.

Definition: A field extension F/K is called a simple extension if there is $c\in F$ such that $F=K(c)$.

Now let us look after the explicit form of the elements of $K(c)$. Now $c,c^2,...\in K(c)$

$\Rightarrow K(c)$ contains the elements of the form $k_0+k_1c+...+k_nc^n$. Thus for any $f(x)\in K[x]$, $f(c)\in K(c)$, i.e., $K[c]=\{f(c)\mid f(x)\in K[x]\}\subseteq K(c)$. Since $K[c]$ is an integral domain, the field of quotients $Q(K[c])$ of $K[c]$ exists, and if follows from the fact $K[c]$ is the smallest subfield that contains $K\cup\{c_1,c_2,...,c_n\}$ that $K[c]=Q(K[c])$. Thus we have:

$$K(c)=\left\{f(c)g(c)^{-1}\mid f(x),g(x)\in K[x],g(c)\neq 0\right\}$$

Example 5: Consider $Q(\sqrt{2})=\left\{\frac{f(\sqrt{2})}{g(\sqrt{2})}\middle| f(x),g(x)\in Q[x],g(\sqrt{2})\neq 0\right\}$. Let

$f(x)=a_0+a_1x+...+a_nx^n\in Q[x]$. Then

$f(\sqrt{2})=a_0+a_1\sqrt{2}+5a_2+2a_3\sqrt{2}...+a_n(\sqrt{2})^n$

$= (a_0 + 2a_2 + ...) + (a_1 + 2a_3 + ...)\sqrt{2}$

$= a + b\sqrt{2}$,where $= a, b \in Q$

Prove that if $\alpha \in Q(\sqrt{2})$, then

$$\alpha = \frac{f(\sqrt{2})}{g(\sqrt{2})}$$

$$= \frac{a + b\sqrt{2}}{c + d\sqrt{2}}$$

$= r + s\sqrt{2}$ for some $r, s \in Q$

Also $r + s\sqrt{2} \in Q(\sqrt{2}) \forall\, r, s \in Q$. Thus we have $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$.

We demonstrate in the example below how extensions produced by many parts might be straightforward extensions.

Example 6: Let us consider the extension $Q(\sqrt{3}, \sqrt{5})$ of Q. Then $\sqrt{3}, \sqrt{5} \in Q(\sqrt{3}, \sqrt{5})$

$\Rightarrow \sqrt{5} - \sqrt{3} \in Q(\sqrt{3}, \sqrt{5})$. Since $Q(\sqrt{5} - \sqrt{3})$ is the smallest field which contains Q and $\sqrt{5} - \sqrt{3}$, which follows that $\Rightarrow Q(\sqrt{5} - \sqrt{3}) \subseteq Q(\sqrt{3}, \sqrt{5})$.

Again, $\Rightarrow \sqrt{5} - \sqrt{3} \in Q(\sqrt{5} - \sqrt{3})$

$\Rightarrow \frac{1}{\sqrt{5} - \sqrt{3}} \in Q(\sqrt{5} - \sqrt{3})$ *i.e.*, $\frac{1}{2}(\sqrt{5} + \sqrt{3}) \in Q(\sqrt{5} - \sqrt{3})$

$\Rightarrow \sqrt{3} = \frac{1}{2}(\sqrt{5} + \sqrt{3}) - \frac{1}{2}(\sqrt{5} - \sqrt{3}) \in Q\left(\sqrt{5} - \sqrt{3}\right)$ and $\sqrt{5} = \frac{1}{2}(\sqrt{5} + \sqrt{3}) + \frac{1}{2}(\sqrt{5} - \sqrt{3}) \in Q\left(\sqrt{5} - \sqrt{3}\right)$

$\Rightarrow Q(\sqrt{3}, \sqrt{5}) \subseteq Q(\sqrt{5} - \sqrt{3})$.

Thus $Q(\sqrt{3}, \sqrt{5}) = Q(\sqrt{5} - \sqrt{3})$

Recall that C is a vector space over R of dimension 2 and $\{1, i\}$ is a basis of C over R. Also $Q(\sqrt{2})$ is a vector space over Q and $\{1, \sqrt{2}\}$ is a basis.

Let F / K be a field extension. Then the multiplication in F induces an external composition $K \times F \to F$. Then for all $c \in K$ and $\alpha, \beta \in F$, we have

(*i*) $(c + d)\alpha = c\alpha + d\alpha$, (right distributivity law of multiplication over addition in F)

(*ii*) $(cd)\alpha = c(d\alpha)$, (associativity of multiplication in F)

(*iii*) $c(\alpha + \beta) = c\alpha + c\beta$, (left distributivity law of multiplication over addition in F)

(*iv*) $1.\alpha = \alpha$,

which shows that F is a vector space over K.

Definition: Let F/K be a field extension. Then the dimension of F as a vector space over K is called the degree of the extension of F/K.

It is denoted by $[F:K]$.

Thus $[C:R] = 2$ and $[Q(\sqrt{2}):Q] = 2$

Example 7: Now we prove that $[F:K]=1$ *iff* $K=F$.

If $F=K$, then $\dim F=1$ as a vector space over K. Hence $[F:K]=1$.

Conversely, let $[F:K]=1$. Consider $c\in F$ and $c\neq 0$. Then $\{c\}$ is linearly independent and so a basis of F over K. Then there is $k\in K$ such that $1=kc$. This implies that $k\neq 0$ and $c=k^{-1}\in K$. Thus $F\subseteq K$ and hence $F=K$

Definition: A field extension F/K is called finite if $[F:K]$ is so, otherwise F/K is called an infinite extension.

If $[F:K]=2$, then F is called a quadratic extension of K.

Example 8: 1. $Q(\sqrt{2})/Q, C/R, Q(\sqrt[3]{2})/Q$ are finite extension of fields.

2. R/Q is an infinite extension.

3. $Q(\sqrt{2})/Q, C/R$ are quadratic extension.

4. $Q(\sqrt[3]{2})/Q$ is not a quadratic extension.

Following results are very important to find the degree of field extension and also known as tower rule.

Theorem 2: Let F/L and L/K be two finite extensions of fields. Then F/K is also a finite extension and $[F:K]=[F:L][L:K]$

Moreover, if $\{u_1,u_2,u_3,...,u_m\}$ is a basis of F/L and $\{v_1,v_2,v_3,...,v_n\}$ is a basis of L/K, then $B=\{u_iv_j \mid 1\le i\le m, 1\le j\le n\}$ is a basis of F/K.

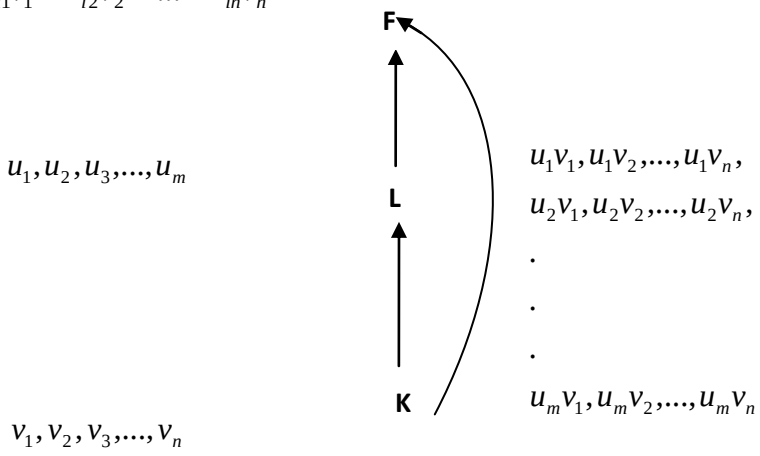
Proof: Suppose that $[F:L]=m$ = m and $[L:K]=n$. Consider bases $\{u_1,u_2,u_3,...,u_m\}$ of F over L and

$\{v_1,v_2,v_3,...,v_n\}$ of L over K. Then for any $a\in F$, there are $l_1,l_2,u_3,...,l_n\in L$ such that

$a=l_1u_1+l_2u_2+l_3u_3+...+l_mu_m$.

Since for each $l_i\in L$ there are $k_{i1},k_{i2},...,k_{in}\in K$ such that

$l_i = k_{i1}v_1 + k_{i2}v_2 + ... + k_{in}v_n$



Thus,

$$a = k_{11}u_1v_1 + k_{12}u_1v_2 + ... + k_{1n}u_1v_n$$
$$+ k_{21}u_2v_1 + k_{22}u_2v_2 + ... + k_{2n}u_2v_n +$$
$$.$$
$$.$$
$$.$$
$$+ k_{m1}u_mv_1 + k_{m2}u_mv_2 + ... + k_{mn}u_mv_n.$$

which shows that $B = \{u_iv_j \mid 1 \le i \le m, 1 \le j \le n\}$ generates F as a vector space over K. This is left for learners to checking that $B = \{u_iv_j \mid 1 \le i \le m, 1 \le j \le n\}$ is linearly independent. Thus $B = \{u_iv_j \mid 1 \le i \le m, 1 \le j \le n\}$ is a basis of F over K.

Note: Let F/K be a field extension of finite degree and L is an intermediate field. Then aforesaid theorem implies that L/K is finite extension and $[F:K] = [F:L][L:K]$

$\Rightarrow [L:K] \mid [F:K]$

Corollary 2: If F/K is a finite field extension and L is an intermediate field, then $[L:K] \mid [F:K]$.

There are several uses for the tower rule. We demonstrate its application to determine the degree of an extension in the further books. Let's now think about the case below.

Example 9: Let L and M be two intermediate fields of a field extension F/K. If $[L:K]$ is prime, then either $L \cap M = K$ or $L \subseteq M$

Denote $N = L \cap M$. Then $K \subseteq N \subseteq L$

$\Rightarrow N$ is an intermediate field of L/K, and

hence $[L:K] = [L:N][N:K]$. Since $[L:K]$ is prime, $[L:N] = 1 = 1$ or $[N:K] = 1$. Then $N = L$ or $N = K$, *i.e.*, $L \subseteq M$ or $L \cap M = K$.

14.4 *MINIMAL POLYNOMIAL*

In this unit we defined degree $[F:K]$ of a field extension F/K to be the dimension of F as a vector space over K. Though we have results ensuring existence of basis of every vector space, but there is no for finding a basis in general. In this unit we set the theory a step forward to find $[F:K]$. The degree of a simple extension $K(c)/K$ is finite if and only if c is a root of some nonconstant polynomial $f(x)$ over K. Here we discuss how to find a basis and dimension of such simple extensions $K(c)/K$.

Definition: Let F/K be a field extension. Then $c \in F$ is called an algebraic element over K, if there is a non constant polynomial $f(x) \in K[x]$ s.t. $f(c)=0$, *i.e.* if there exists $k_0, k_1, ..., k_n \in K$ not all $k_i = 0$ s.t.,

$$k_0 + k_1 c + ... + k_n c^n = 0$$

Otherwise c is called a transcendental element over K.

Example 10: 1, $\sqrt{2}$, $3\sqrt{5}$, i etc are algebraic over Q and e, π, e^e are transcendental over Q.

Definition: A complex number α is called an algebraic number if α is an algebraic element over Q that is, if there is a non constant polynomial $f(x)$ with rational coefficients such that

$$f(\alpha) = 0$$

Otherwise $\alpha \in C$ is called a transcendental number.

Let $\alpha \in F$ be an algebraic element over K. Now we show that uniqueness can be imposed to the polynomials $f(x) \in K[x]$ such that $f(\alpha)=0$ up to some restrictions.

Theorem 3: Let F/K be a field extension and $\alpha \in F$ be algebraic over K. Then there is a unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha)=0$

Proof: Since α is algebraic over K, there is a nonconstant polynomial $f(x) \in K[x]$ such that $f(\alpha)=0$.

$\Rightarrow P = \{f(x) \in K[x] \mid f(x)$ is nonconstant and $f(\alpha)=0\}$ is nonempty and hence

$N = \{\deg f(x) \mid f(x) \in P\}$ is a nonempty subset of N. By the well-ordering principle of natural numbers, N has the least element, say n and correspondingly a polynomial

$k_0 x^n + k_1 x^{n-1} + ... + k_{n-1} x + k_n \in K[x]$ of degree n in P. Then $k_0 \neq 0$ and hence $m(x) = k_0^{-1} f(x)$ becomes a monic polynomial of the least degree n such that $m(\alpha)=0$.

Suppose $p(x)$ is a monic polynomial of degree n and $p(\alpha)=0$. Since K is a field, there

are $q(x), r(x) \in K[x]$ such that $p(x) = m(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. If $\deg r(x) < \deg m(x)$, then $r(x)$ becomes a non constant polynomial such that $r(\alpha) = r(\alpha) - m(\alpha)q(\alpha) = 0$, which contradicts the choice of $m(x)$ as a polynomial of least degree such that $m(\alpha) = 0$. Thus $r(x) = 0$ and we have $p(x) = m(x)q(x)$ which implies that $\deg q(x) = 0$, i.e. $q(x) = k \in K$. Since both $p(x)$ and $m(x)$ are monic, $p(x) = km(x)$ implies that $k = 1$ and thus the uniqueness of $m(x)$ is established.

Definition: Let F / K be a field extension and $\alpha \in F$ algebraic over K. Then the unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$ is called the minimal polynomial of α over K.

If $n = \deg m(x)$, then α is called algebraic of degree n over K.

Example 11: Consider the extension R / Q. Then $x^2 - 3$ is the minimal polynomial of $\sqrt{3} \in R$ over Q. Thus $\sqrt{3}$ is algebraic of degree 2 over Q.

Example 12: Let F / K be a field extension and c be algebraic over K of degree 5. We show that $K(c) = K(c^2)$.

Let $m(x) = x^5 + k_4x^4 + k_3x^3 + k_2x^2 + k_1x + k_0$ be the minimal polynomial of c over K. Then c can not be a root of any polynomial of degree less than 5, and so $c^4 + k_3c^2 + k_1 \neq 0$. Then

$$c^5 + k_4c^4 + k_3c^3 + k_2c^2 + k_1c + k_0 = 0$$

$$\Rightarrow c = \frac{-k_0 - k_2c^2 - k_4c^4}{k_1 + k_3c^2 + c^4} \in K(c^2), \text{ and hence } K(c) = K(c^2)$$

Although the aforementioned evidence for the existence and uniqueness of the minimum polynomial $m(x)$ is inherent, it does not offer any guidance on how to go about locating the minimal polynomial. We now present evidence that irreducibility may serve as an effective comparable criteria for our practical goal.

Let's start by demonstrating the lemma that follows, which follows directly from the minimum polynomial's leastness in degree such that $m(\alpha) = 0$

Lemma 1: Let F / K be a field extension $\alpha \in F$ and algebraic over K. Then for every $f(x) \in K[x], f(\alpha) = 0 \Rightarrow m(x) \mid f(x)$

Proof: By the Division Algorithm, there are $q(x), r(x) \in K[x]$ such that $f(x) = m(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. If $\deg r(x) < \deg m(x)$, then $r(x)$ becomes a non constant polynomial such that $r(\alpha) = p(\alpha) - m(\alpha)q(\alpha) = 0$, which contradicts the choice of $m(x)$ as a

polynomial of least degree such that $m(\alpha)=0$. Thus $r(x)=0$ and we have

$f(x)=m(x)q(x)\Rightarrow m(x)\mid f(x)$.

If $f(x)$ is a nonconstant polynomial such that $f(\alpha)=0$, then the above lemma shows that some factor of $f(x)$ is the minimal polynomial of α. Thus if we have some irreducible polynomial $p(x)$ such

that $p(\alpha)=0$, then this must be the monic polynomial up to a unit multiple, that is $m(x)=up(x)$.

Since $K[x]$ is a UFD, there are irreducible polynomials $p_1(x), p_2(x),..., p_m(x)\in K[x]$ s.t.

$f(x)=p_1(x), p_2(x),..., p_m(x)$. Then $f(\alpha)=0$

$\Rightarrow p_1(\alpha)p_2(\alpha)...p_m(\alpha)=0$ and hence $p_i(\alpha)=0$ for some *i*. Thus we have an irreducible polynomial $p_i(x)$ having a root α. Now we show that irreducibility is enough to characterize minimal polynomials.

Theorem 4: Let F/K be a field extension and $\alpha\in F$ algebraic over K. Then $m(x)\in K[x]$ is the minimal polynomial of α over K *iff* it is a monic irreducible polynomial such that $m(\alpha)=0$.

Proof: First, let us assume that $m(x)\in K[x]$ is the minimal polynomial of α over K. Suppose

$m(x)=u(x)v(x), u(x), v(x)\in K[x]$. Then $m(\alpha)=0$

$\Rightarrow$ either $u(\alpha)=0$ or $v(\alpha)=0$. If $u(\alpha)=0$, then $\deg u(x)$ can never be less than $\deg m(x)$ and hence $\deg u(x)=\deg m(x)$.

$\Rightarrow \deg v(x)=0$ and hence $v(x)$ is a unit. Similarly $v(\alpha)=0$

$\Rightarrow u(x)$ is a unit. Thus $m(x)$ is irreducible.

Conversely, consider a monic and irreducible polynomial $p(x)\in K[x]$ such that $p(\alpha)=0$. Then $p(x)=m(x)q(x)$. Then the irreducibility of $p(x)$ implies that either $m(x)$ is a unit or $q(x)$ is a unit. Since $m(x)$ is non constant, it is not a unit. Thus $q(x)$ is a unit. Since both $p(x)$ and $m(x)$ are monic we have $q(x)=1$. Thus $p(x)=m(x)$.

Corollary 3: Let F/K be a field extension and $\alpha\in F$. Then α is algebraic over K if and only if $K[\alpha]=K(\alpha)$. Moreover in this case, $K[\alpha]=K(\alpha)\cong K[x]/<m(x)>$.

Proof: First assume that α is algebraic over K. Define $\psi: K[x]\to K[\alpha]$ by for every $f(x)\in K[x]$,

$$\psi(f(x))=f(\alpha)$$

Then ψ is an onto homomorphism. Now,

$\ker\psi=\{f(x)\in K[x]\mid f(\alpha)=0\}$

$=\{f(x)\in K[x]\mid m(x)\mid f(x)\}$

$=< m(x) >$

Now, by first isomorphism theorem, that $K[x]/< m(x) > \cong K[\alpha]$. Since $m(x)$ is irreducible, it follows that $K[x]/< m(x) >$ is a field forcing $K[\alpha]$ to be a field. Hence $K[\alpha] = K(\alpha)$.

Conversely, suppose that $K[\alpha] = K(\alpha)$. That $\alpha = 0$ is algebraic follows directly. Let $\alpha \neq 0$. Since $K(\alpha)$ is a field, $\alpha^{-1} \in K(\alpha) = K[\alpha]$ and hence $\alpha^{-1} = k_0 + k_1\alpha + ... + k_n\alpha^n$ *for some* $k_i \in K$, where, $k_i, i = 0,1,2,...,n$ not all k_i are zero. Then $k_n\alpha^{n+1} + k_{n-1}\alpha^n + ... + k_0\alpha - 1 = 0$ which shows that α is algebraic over K.

In the following we show that $K(c)$ is an infinite extension of K for every transcendental element c.

Corollary 4: Let F/K be a field extension and $c \in F$. Then c is transcendental over K if and only if $K[c] \subset_{\neq} K(c)$. In this case, $K[c] \cong K[x]$ and $K(c) \cong K(x)$.

Proof: First part of this result follows from the above corollary, since $K[c] \subseteq K(c)$. For the second part, consider the onto homomorphism $\psi : K[x] \to K[c]$ for every $f(x) \in K[x]$,

$$\psi(f(x)) = f(c)$$

Since c is transcendental over K, there is no nonzero polynomial $f(x) \in K[x]$ such that $f(c) = 0$

Thus $\ker\psi = \{0\}$ showing that ψ is one-to-one. Thus $K[x] \cong K[c]$

Since $K(x)$ and $K(c)$ are the quotient fields of $K[x]$ and $K[c]$ respectively, $\psi : K[x] \to K[c]$ induces an isomorphism $\psi' : K(x) \to K(c)$ defined by, for every $\frac{f(x)}{g(x)} \in K(x)$

$\psi'\left(\frac{f(x)}{g(x)}\right) = \frac{f(c)}{g(c)}$. Therefore $K(c) \cong K(x)$.

If $m(x)$ is a polynomial of degree n, then by division algorithm for polynomial over the field defined that $K[x]/< m(x) >$ is a n dimension vector space over the field K having basis

$\{1 + < m(x) >, x + < m(x) >, ..., x^{n-1} + < m(x) >\}$.

If $m(x)$ is irreducible over K, then

$F = K[x]/< m(x) >$ is a field and $c = x + < m(x) > \in F$ is a root of $m(x)$. Thus, by the Corollary 3, we have the results.

Theorem 5: Let F/K be a field extension, $c \in F$ be algebraic over K and $m(x)$ be the minimal polynomial of c over K. If $\deg m(x) = n$, then $\{1, c, c^2, ..., c^{n-1}\}$ is a basis of $K(c)$ over K. Thus

$$[K(c) : K] = \deg m(x).$$

Proof: Let $\alpha \in K(c)$. Since c is algebraic over K, $K(c) = K[c]$.

Which shows that $\alpha = f(c)$ for some $f(x) \in K[x]$. By division algorithm $\exists q(x), r(x) \in K[x]$, s.t.

$f(x) = m(x)q(x) + r(x)$

where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. In other case we will assume that

$r(x) = r_0 + r_1 x + ... + r_{n-1}x^{n-1}$, where $r_i \in K$. Then $m(c) = 0$

$\alpha = f(c) = r(c) = r_0 + r_1 c + ... + r_{n-1}c^{n-1}$

Thus, $\{1, c, c^2, ..., c^{n-1}\}$ generates $K(c)$ over K. By the definition of linearly independent if there are

$k_0 + k_1 c + ... + k_{n-1}c^{n-1} = 0$

Then $p(x) = k_0 + k_1 x + ... + k_{n-1}x^{n-1} \in K[x]$ will be non zero polynomial s.t. its degree will be less $\deg m(x)$

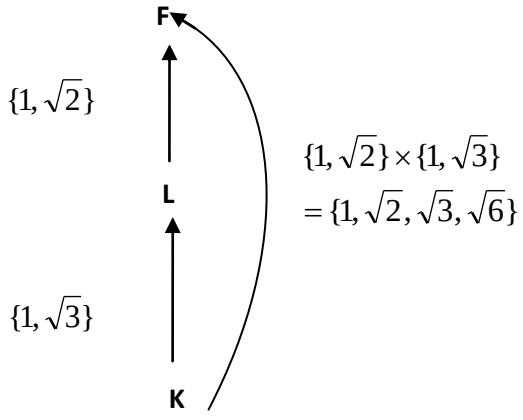
s.t. $p(c) = 0$ which is the contradict that $m(x)$ is minimal polynomial of c over K. Thus

$\{1, c, c^2, ..., c^{n-1}\}$ is a basis of $K(c)$ over the field K.

Example 13: Let us consider the extension $Q(\sqrt[3]{2})$ over Q. The minimal polynomial of $\sqrt[3]{2}$ over Q is given by $m(x) = x^3 - 2$. So $[Q(\sqrt[3]{2}) : Q] = 3$ and $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ is a basis of $Q(\sqrt[3]{2})$ over Q. Thus

$Q(\sqrt[3]{2}) = \{a + b\,2^{1/3} + c\,2^{2/3} \mid a, b, c \in Q\}$

Example 14: Consider $Q(\sqrt{2}, \sqrt{3})$ as $Q(\sqrt{3})(\sqrt{2})$. Since $x^2 - 2$ is irreducible over $Q(\sqrt{3})$, the minimal polynomial $\sqrt{2}$ over $Q(\sqrt{3})$ is $x^2 - 2$. Then $[Q(\sqrt{3})(\sqrt{2}) : Q(\sqrt{3})] = 2$ and $\{1, \sqrt{2}\}$ is basis of $Q(\sqrt{3})(\sqrt{2})$ over $Q(\sqrt{3})$. Also $[Q(\sqrt{2}, \sqrt{3}) : Q] = [Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{3})][Q(\sqrt{3}) : Q] = 4$



Since $\{1, \sqrt{2}\}$ is basis of $Q(\sqrt{3})(\sqrt{2})$ over $Q(\sqrt{3})$ and $\{1, \sqrt{3}\}$ is a basis of $Q(\sqrt{3})$ over Q, it follows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $Q(\sqrt{2}, \sqrt{3})$ over Q. Thus

$Q(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in Q\}$.

14.5 *GALOIS GROUP*

In this section we will discuss important definition of Galois group of polynomial over a field

Splitting Field: If $f(x) \in F[x]$, a finite extension E of F is said to be a splitting field over F for $f(x)$ if over E (i.e., in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear (first degree) factors.

The field F is called the base field or the initial field.

Theorem 6: There exist a splitting field for every $f(x) \in F[x]$.

Proof: Let n degree polynomial $f(x) \in F[x]$. Initially, we will prove that $\exists$ finite extension E of F of degree at most $n!$ in which $f(x)$ has n roots.

Let $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n, a_0 \neq 0.$

Let $\alpha_1, ..., \alpha_n$ be n root in E of $f(x)$. Then $f(x)$ can be factored as

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$$

As a product of first degree factors, $f(x)$ divides up fully across E in this manner. Thus, we can show that there is a finite extension of F called E that decomposes $f(x)$ into a linear product. As a result, there is a finite extension of F of minimum degree that shares this feature. Because no suitable subfield of this minimal extension can divide $f(x)$ as a product of linear factors, this minimal extension will operate as a splitting field for $f(x)$.

Another way

An extension E of a field F is said to be a splitting field of $f(x) \in F[x]$, if $f(x) \in E[x]$ is expressible as

$f(x) = a_0(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$, where $a_0 \in F, \alpha_1, \alpha_2, ..., \alpha_n \in E$ and $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$.

Note. *Uniqueness of splitting field*: This is to note that a polynomial's splitting field is distinct from isomorphism. Let E_1 and E_2 be two splitting field of $f(x) \in F[x]$ s.t.

$f(x) = a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ over E_1

and $f(x) = a(x-\beta_1)(x-\beta_2)...(x-\beta_n)$ over E_2

Here, fields $F(\alpha_1, \alpha_2, ..., \alpha_n)$ and $F(\beta_1, \beta_2, ..., \beta_n)$ are isomorphic by an isomorphism leaving every element of F fixed.

Normal extension: A finite extension K of a field F is name as a normal extension of F if the fixed field of $G(K, F)$ is F.

By the definition it is obvious that if any element of K which is not in F, then we must have some automorphism σ in $G(K,F)$ s.t., $\sigma(a) \neq a$

Definition (Galois group): Let $f(x)$ be polynomial in $F[x]$ and let K be its splitting field over F. The Galois group of $f(x)$ is the group $G(K,F)$ of all those automorphisms of K which leave every element of F is fixed.

Note: If K is an extension of a field F, then an automorphism of K which leaves every element of F fixed is also called an $F-$automorphism of K. If K is a normal extension of a field F of characteristic 0, then K is the splitting field of some polynomial $f(x)$ in $F[x]$. The group $G(K,F)$ of $F-$automorphism of K is also called the Galois group of K over F.

Theorem 7: The Galois group of a polynomial is isomorphic to a group of permutations of its roots.

Proof: Let the polynomial $f(x)$ over the field F and K be the splitting field of $f(x)$ over F. Then K is normal extension of F. Thus the Galois group $G(K,F)$ of $f(x)$ is of finite order n *i.e.*, $[K,F]=n$. Let n distinct element of $G(K,F)$ are $\sigma_1, \sigma_2, ..., \sigma_n$. Let us suppose that in K, $f(x)$ has m distinct roots. It can be possible that $f(x)$ has multiple roots. Assume that $S=\{\alpha_1, \alpha_2, ..., \alpha_m\}$ be the collection of m distinct root of $f(x)$ in K. Let P be the collection of all those permutation on S such that which are not in F i.e., P contain those element of S in which element of F is fixed (if any exist). If p_1, p_2 are two element of P then $p_1 p_2$ should also in P because $p_1 p_2$ will also leave each element of F fixed. So we can say that P is closed w.r.to product of two permutation. Thus P is subgroup of group of all permutation on S. Now we have to prove that group $G(K,F)$ is isomorphic to group P.

Let the permutation $\sigma \in G(K,F)$ and σ^* be the restriction of σ to S. As we know that if M is the extension of F and if $f(x) \in F[x]$ and if ϕ is an *automorphism* of M s.t. it leaving each element of F fixed then ϕ must take a root of $f(x)$ lying in M into a root of $f(x)$ in M. Using this theorem we can say that if a is any root of $f(x)$ in K, then $\sigma(a)$ is also a root of $f(x)$ in K.

Therefore $a \in S \Rightarrow \sigma(a) = \sigma^*(a) \in S$

$\Rightarrow \sigma^*$ is function from S to S.

Further σ^* is one-one because σ is one-one. As we know that S is finite set then,

σ^* is one-one $\Rightarrow \sigma^*$ is also a onto function.

$\Rightarrow \sigma^*$ is also a permutation on S.

Since σ leaves each element of F fixed, in similar way σ^* will also leave each element of F fixed.

$\Rightarrow \sigma^* \in P$.

Let us consider $\phi : G(K,F) \to P$

s.t. $\phi(\sigma) = \sigma^* \ \forall \sigma \in G(K,F)$

ϕ **is one-one:** Let us consider $\sigma_1, \sigma_2 \in G(K,F)$. Then

$\phi(\sigma_1) = \phi(\sigma_2)$

$\Rightarrow \sigma_1^* = \sigma_2^*$

$\Rightarrow \sigma_1^*(a) = \sigma_2^*(a) \ \forall a \in S$

$\Rightarrow \sigma_1(a) = \sigma_2(a) \ \forall a \in S$

Now $K = F(a_1, a_2, ..., a_m)$. Each element of K may therefore be obtained by performing a limited number of addition, subtraction, multiplication, and division operations on the components of F and on $(a_1, a_2, ..., a_m)$, but σ_1 and σ_2 are automorphisms of K. Each one maps every element of S the same way while leaving every element of F fixed.

ϕ **is onto:** Let $b \in P$ then b is a permutation on S while keeping fixed the S elements that are in F. Now consider there is an automorphism σ of K that maps each element of S in the same way as b maps it while leaving every element of F fixed. The automorphism σ of K will be fully determined since each element of K may be obtained by performing a limited number of addition, subtraction, multiplication, and division operations on the elements F and $(a_1, a_2, ..., a_m)$.

ϕ **preserve the composition:** Let $\sigma_1, \sigma_2 \in G(K,F)$ be arbitrary. Then

$\phi(\sigma_1\sigma_2) = (\sigma_1\sigma_2)^*$, the restriction of $\sigma_1\sigma_2$ to S. Since $\forall a \in S$, we have

$$(\sigma_1\sigma_2)^*(a) = (\sigma_1\sigma_2)(a)$$

$$= \sigma_1[\sigma_2(a)]$$

$$= \sigma_1[\sigma_2^*(a)]$$

$$= \sigma_1^*[\sigma_2^*(a)] = (\sigma_1^*\sigma_2^*)(a)$$

$\therefore (\sigma_1\sigma_2)^* = \sigma_1^*\sigma_2^*$

$\therefore \phi(\sigma_1\sigma_2) = \sigma_1^*\sigma_2^* = \phi(\sigma_1)\phi(\sigma_2)$

Thus ϕ is an isomorphic mapping. Hence $G(K,F) \cong P$.

Now we will discuss about **fundamental theorem of Galois group**.

Theorem 8: Let K be the normal extension in a field F with characteristic 0. Prove that there exist a one to one correspondence between set of subgroups of $G(K,F)$ and set of subfield of K. Further, show that if M is any subfield of K which contains F, then

(i) $[K:M]=O(G(K,M))$, and $[M:F]=index of\ G(K,M)\ in G(K,F)$

(ii) M is normal extension in F *iff* $G(K,M)$ is normal subgroup of $G(K,F)$

(iii) If M is a normal extension of F, then $G(M,F)$ is isomorphic to $G(K,F)/G(K,M)$

Proof: For any subfield M of K which contains F, consider $G(K,M)$ be the group of all automorphism of K which leave each element of M fixed. We have

$\sigma \in G(K,M) \Rightarrow \sigma$ leaves each element of M fixed

$\Rightarrow \sigma$ leaves each element of F fixed

Since $F \subseteq M$

$\Rightarrow \sigma \in G(K,F)$

Thus $G(K,M) \subseteq G(K,F)$

$\Rightarrow G(K,M)$ is subgroup of $G(K,F)$

So, for any subfield T of K who contains F we will found a subgroup $G(K,M)$ of $G(K,F)$. Now define a mapping ϕ between set of subfields of K which contains F into set of subgroup of $G(K,F)$ s.t.,

$\phi(M)=G(K,M)$ for each subfield M of K which contains F.

ϕ **is on-to:** Let $K_H=\{x\in K:\sigma(x)=x\forall\sigma\in H\}$ denote the fixed field of H, where H is any subgroup of $G(K,F)$. Then K_H is a subfield of K. Also

$\sigma \in H \Rightarrow \sigma \in G(K,F)$. Since H is subset of $G(K,F)$.

$\Rightarrow \sigma(a)=a\ \forall\ a\in F$.

Thus if $\sigma \in H$, then $\sigma(a)=a\ \forall\ a\in F$. Therefore $F\subseteq K_H$ and so K_H is a subfield of K containing F. Since we have $\phi(K_H)=G(K,K_H)$ [By definition]

[By the **Theorem:** If K is the finite extension of a field F with characteristic 0 and H is subgroup of $G(K,F)$. Let K_H be the fixed field of H. Then (i) $[K:K_H]=O(H)$ (ii) $H=G(K,K_H)$]

By using this theorem we can say that,

$\phi(K_H)=H$.

$\therefore \phi$ is onto.

ϕ **is one-one:** As we know that K is the normal extension with characteristic 0 of a field F.

$\Rightarrow K$ is the splitting field for some polynomial $f(x)\in F[x]$. If M is any subfield of K containing F then K will also the splitting field of $f(x)$ regarded as a polynomial over M. Then by using the theorem (K is the normal extension with characteristic zero of a field F *iff* K is the splitting field of some polynomial over F) K is normal extension of M. Thus according to the definition of normal extension the fixed field of $G(K,M)$ is M.

$\Rightarrow K_{G(K,M)}=M$

Let us consider two subfield of K are M_1, M_2 which contain F.

Then consider, $\phi(M_1)=\phi(M_2)$

$\Rightarrow G(K,M_1)=G(K,M_2)$ [By definition]

$\Rightarrow$ The fixed field of $G(K,M_1)=$ The fixed field of $G(K,M_2)$

$\Rightarrow K_{G(K,M_1)}=K_{G(K,M_2)}$

$\Rightarrow M_1=M_2$

$\Rightarrow \phi$ is one-one.

Thus we can say that ϕ gives the one to one correspondence. Now we have only to prove that (i), (ii) and (iii).

(i) If M is any subfield containing F, then as in previous part we have prove that K is normal extension of M. Therefore we have $O(G(K,M))=[K:M]$. Since K is normal extension of F, therefore

$O(G(K,F))=[K:F]$

$$= [K : M][M : F]$$

$$= O(G(K, M))[M : F]$$

$$\therefore [M : F] = \frac{O(G(K, F))}{O(G(K, M))} = index of\ G(K, M)\ in G(K, F).$$

(ii) Let M is subfield of K containing F. Then M is normal extension of F

$\Leftrightarrow \sigma(M) \subseteq M\ \forall\ \sigma \in G(K, F)$

i.e., $\Leftrightarrow \sigma(m) \in M\ \forall m \in M\ \ and\ \ \sigma \in G(K, F)$

i.e., $\Leftrightarrow \tau[\sigma(m)] = \sigma(m)\ \forall m \in M, \forall\ \sigma \in G(K, F)\ \ and\ \ \forall\ \tau \in G(K, M)$

[Note that $\tau \in G(K, M) \Leftrightarrow \tau(m) = m\ \forall\ m \in M$]

i.e., $\Leftrightarrow \sigma^{-1}[\tau[\sigma(m)]] = \sigma^{-1}[\sigma(m)] \forall m \in M, \forall\ \sigma \in G(K, F)\ and\ \forall\ \tau \in G(K, M)$

i.e., $\Leftrightarrow (\sigma^{-1}\tau\sigma)(m) = m\ \forall\ m \in M, \forall\ \sigma \in G(K, F)\ and\ \forall\ \tau \in G(K, M)$

i.e., $\Leftrightarrow \sigma^{-1}\tau\sigma \in G(K, M)\ \forall\ \sigma \in G(K, F)\ and\ \forall\ \tau \in G(K, M)$

[Note that $\sigma^{-1}\tau\sigma \in G(K, M) \Leftrightarrow (\sigma^{-1}\tau\sigma)(m) = m \forall m \in M$]

i.e., *iff* $G(K, M)$ is normal subgroup of $G(K, F)$ (By definition of normal subgroup)

(iii) If M is normal extension of F, then for any $\sigma \in G(K, F)$, we have

$$\sigma(M) \subseteq M$$

$\Rightarrow \sigma(t) \in M\ \forall\ m \in M$

Therefore σ induces an automorphism σ^* of M, defined as

$\sigma^*(m) = m\ \forall\ m \in M$

Since σ leaves each element of F fixed, therefore σ^* also leaves each element of F fixed.

$\Rightarrow \sigma^* \in G(M, F)$. If $\sigma_1, \sigma_2 \in G(K, F)$ then $m \in M$, we have

$(\sigma_1\sigma_2)^*(m) = (\sigma_1\sigma_2)m$

$$= \sigma_1[(\sigma_2 m)] = \sigma_1[(\sigma_2{}^* m)] = \sigma_1{}^*[(\sigma_2{}^* m)]$$

$$= (\sigma_1^* \sigma_2^*)(m)$$

$$\therefore (\sigma_1\sigma_2)^* = \sigma_1^* \sigma_2^*$$

So we conclude that the mapping $\psi : G(K,F) \to G(M,F)$ defined as $\psi(\sigma) = \sigma^* \; \forall \sigma \in G(K,F)$ is a homomorphism. The $\ker nel$ of this homomorphism consists all such element σ in $G(K,F)$ s.t. $\psi(\sigma) = \sigma^*$ is the identity of the group $G(M,F)$ and the identity of the group $G(M,F)$ is identity map on M. Therefore,

$$\ker nel(\psi) = \{\sigma \in G(K,F) \mid m = \sigma^*(m) = \sigma(m) \; \forall m \in M\}$$

But $\sigma(m) = m \; \forall m \in M \Leftrightarrow \sigma \in G(K,M)$. Therefore kernel of ψ is exactly $G(K,M)$. Now using fundamental theorem on homomorphism of groups, image of $G(K,F)$ in $G(M,F)$ under the mapping ψ is isomorphic to the quotient group $G(K,F)/G(K,M)$.

Now, $O(G(K,F)/G(K,M)) = \dfrac{O(G(K,F))}{O(G(K,M))}$

$$= index of \; G(K,M) \; in G(K,F)$$

$$= [M:F] \qquad \text{[By part (i) of theorem]}$$

$$= O(G(M,F)) \qquad [\, T \text{ is normal over } F \,]$$

Thus image of $G(K,F)$ in $G[M,F]$ is isomorphic to a group of order $O(G(M,F))$. Since image of $G(K,F)$ in $G[M,F]$ is a subgroup of $G[M,F]$, therefore it is all of $G[M,F]$. Hence $G(K,F)/G(K,M) \cong G(M,F)$.

Check your progress

Problem 1: Check that $B = \{u_i v_j \mid 1 \le i \le m, 1 \le j \le n\}$ is linearly independent?

Problem 2: Check that Q and Z_p has proper subfield or not?

14.6 *SUMMARY*

In this unit, we have learned about the important concept of extension of field, minimal polynomial over a field of extension field and important group name as Galois group of a polynomial over a field. The overall summarization of this units are as follows:

- R is a field extension of Q.
- Q, Z_p has no proper subfield.
- Each field F is either an extension of Q or an extension of Z_p.
- If F is prime field and if char(F) = 0 then $F \cong Q$ and if char(F) = p then $F \cong Z_p$.
- R/Q is an infinite extension.
- C/R finite extension of field and quadratic extension.
- For every $f(x) \in F[x]$ there exist a splitting field.
- The Galois group of a polynomial is isomorphic to a group of permutations of its roots.

14.7 *GLOSSARY*

- F/K**:** F is called field extension of K
- $[F:K]$**:** Denote degree of the extension of F/K 'or' the dimension of F as a vector space over K
- $G(K,F)$**:** Called the Galois group of all those automorphisms of K which leave every element of F is fixed.

14.8 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

14.9 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

14.10 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that every field F is either an extension of Q or an extension of Z_p, for some prime p.

2. Let F/K be a field extension and $\alpha \in F$ be algebraic over K. Then prove that there is a unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$.

3. If F/K be a field extension $\alpha \in F$ and algebraic over K. Then prove that for every $f(x) \in K[x], f(\alpha) = 0 \Rightarrow m(x) \mid f(x)$

4. Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then prove that $m(x) \in K[x]$ is the minimal polynomial of α over K *iff* it is a monic irreducible polynomial such that $m(\alpha) = 0$.

5. If F/K be a field extension, $c \in F$ be algebraic over K and $m(x)$ be the minimal polynomial of c over K. If $\deg m(x) = n$, then prove that $\{1, c, c^2, ..., c^{n-1}\}$ is a basis of $K(c)$ over K. Thus

$$[K(c) : K] = \deg m(x).$$

6. Prove that the Galois group of a polynomial is isomorphic to a group of permutations of its roots.

7. State and prove the fundamental theorem of Galois group.

Short Answer Type Question:

8. Let F/K be a field extension and $\alpha \in F$. Then prove that α is algebraic over K if and only if $K[\alpha] = K(\alpha)$. Moreover in this case, $K[\alpha] = K(\alpha) \cong K[x]/ < m(x) >$.

9. Prove that for every $f(x) \in F[x]$ there exist a splitting field.

10. Prove that $[F : K] = 1$ *iff* $K = F$.

11. Prove that if L and M be two intermediate fields of a field extension F/K. If $[L : K]$ is prime, then either $L \cap M = K$ or $L \subseteq M$

12. If F/K be a field extension and c be algebraic over K of degree 5. Then prove that $K(c) = K(c^2)$.

13. Define the following.

(*i*) Field extension

(*ii*) Normal extension

(*iii*) Galois group

Fill in the blanks:

14. Q has …….. proper subfield

15. Z_p has ……..…… proper subfield

16. A field K is called a prime field if it has no proper ……..……..

14.11 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes

Answer of terminal question:

14. No **15.** No **16.** Subfield

Teen Pani Bypass Road, Transport Nagar
Uttarakhand Open University, Haldwani, Nainital-263139
Phone No. 05946-261122, 261123
Toll free No. 18001804025
Fax No. 05946-264232,
E-mail:info@uou.ac.in
Website: https://www.uou.ac.in/