Semester - II

		L	T	P	C
17MMU203	**GROUP THEORY I**	**6**	**2**	**0**	**6**

Scope: On successful completion of course the learners gain about the groups and its properties.

Objectives: To enable the students to learn and gain knowledge about groups, cyclic groups, sub groups and abelian groups.

UNIT I

Symmetries of a square, Dihedral groups, definition and examples of groups including permutation groups and quaternion groups (illustration through matrices), elementary properties of groups.

UNIT II

Subgroups and examples of subgroups, centralizer, normalizer, center of a group, product of two subgroups.

UNIT III

Properties of cyclic groups, classification of subgroups of cyclic groups. Cycle notation for permutations, properties of permutations, even and odd permutations, alternating group, properties of cosets, Lagrange's theorem and consequences including Fermat's Little theorem.

UNIT IV

External direct product of a finite number of groups, normal subgroups, factor groups, Cauchy's theorem for finite abelian groups.

UNIT V

Abelian groups, finitely generated abelian group, divisible and reduced groups, Torsion group,

SUGGESTED READINGS

TEXT BOOK

1. Fraleigh.J. B., (2004). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.

REFERENCES

1. Artin .M., (2008). Algebra, Prentice-Hall of India, New Delhi.
2. Joseph A. Gallian., (2006). Contemporary Abstract Algebra, Fourth Edition, Narosa Publishing House, New Delhi.
3. Herstein. I. N., (2010). Topics in Algebra, Second Edition, Wiley and sons Pvt Ltd, Singapore.
4. Joseph J. Rotman, (2001). An Introduction to the Theory of Groups, Fourth Edition, Springer

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Coimbatore – 641 021.

LECTURE PLAN

DEPARTMENT OF MATHEMATICS

STAFF NAME: Dr. K.KALIDASS SUBJECT NAME: GROUP THEORY I
SUB.CODE:17MMU302 SEMESTER: III
CLASS: II B. Sc. MATHEMATICS

S. No	Lecture Duration Hour	Topics To Be Covered	Support Materials
UNIT-I			
1	1	Introduction	R2: Ch 1, 29
2	1	Symmetries of a square	R2: Ch 1, 29-30
3	1	Theorems on Dihedral groups	R2: Ch 1, 31-32
4	1	Definition of group	R2: Ch 2, 40
5	1	**Tutorial**	
6	1	Examples of groups	R2: Ch 2, 41
7	1	**Tutorial**	
8	1	Examples of groups	R2: Ch 2, 41-42
9	1	Examples of groups	R2: Ch 2, 43
10	1	Permutation groups	T: Ch 2, 75-78
11	1	Quaternion groups	R2: Ch 2, 45
12	1	Elementary properties of groups.	R2: Ch 2, 46-47
13	1	**Tutorial**	
14	1	Elementary properties of groups.	R2: Ch 2, 48
15	1	**Tutorial**	
16	1	Elementary properties of groups.	R2: Ch 2, 49
17	1	Elementary properties of groups.	R2: Ch 2, 49-50
18	1	Recapitulation and discussion of possible questions	
Total number of hours planed for unit I 18 hours			
. UNIT-II			
1	1	Subgroups	R1: Ch 2, 44-48
2	1	examples of subgroups	R2: Ch 3, 57-58
3	1	**Tutorial**	
4	1	examples of subgroups	R2: Ch 3, 58
5	1	**Tutorial**	
6	1	examples of subgroups	R2: Ch 3, 59-60

7	1	examples of subgroups	R2: Ch 3, 61
8	1	Theorems on centralizer	R2: Ch 3, 62
9	1	Problems on centralizer	R2: Ch 3, 62
10	1	Problems on centralizer	R2: Ch 3, 62-63
11	1	**Tutorial**	
12	1	Theorems on normalizer	R2: Ch 3, 64
13	1	**Tutorial**	
14	1	Problems on normalizer	R2: Ch 3, 64-65
15	1	Theorems on center of a group	R2: Ch 3, 66
16	1	Problems on center of a group	R2: Ch 3, 67
17	1	Theorems on product of groups	R2: Ch 3, 68
18	1	Problems on product of groups	R2: Ch 3, 69-70
19	1	**Tutorial**	
20	1	Recapitulation and discussion of possible questions	
Total number of hours planed for unit II 20 hours			
UNIT-III			
1	1	**Introduction to cyclic groups**	R2, Ch 4,71
2	1	Theorems on cyclic groups	R2, Ch 4,71-72
3	1	Theorems on f cyclic groups	R2, Ch 4,73
4	1	Properties of cyclic groups	R2, Ch 4,74
5	1	classification of subgroups	R2, Ch 4,74-75
6	1	classification of subgroups	R2, Ch 4,76-78
7	1	**Tutorial**	
8	1	Cycle notation for permutations	R2, Ch 5, 90
9	1	**Tutorial**	
10	1	Properties of permutations	R3, Ch 2, 64-66
11	1	Even and odd permutations	R2, Ch 5, 93
12	1	alternating group	R2, Ch 5, 94-95
13	1	properties of cosets	R2, Ch 5, 96
14	1	Lagrange's theorem	R2, Ch 5, 97
15	1	**Tutorial**	
16	1	Fermat's Little theorem	R2, Ch 5, 98
17	1	**Tutorial**	
18	1	Recapitulation and discussion of possible questions	
Total number of hours planed for unit III 18 hours			
UNIT-IV			
1	1	External direct product	R2, Ch 8, 149
2	1	Theorems on external direct product	R2, Ch 8, 150-151
3	1	Problems on external direct product	R2, Ch 8, 152
4	1	Theorems on normal subgroups	R2, Ch 9, 171
5	1	**Tutorial**	
6	1	Theorems on normal subgroups	R2, Ch 9, 172

7	1	**Tutorial**	
8	1	Theorems on normal subgroups	R2, Ch 9, 172-173
9	1	Theorems on factor groups	R2, Ch 9, 173
10	1	Theorems on factor groups	R2, Ch 9, 174
11	1	Theorems on factor groups	R2, Ch 9, 175
12	1	Cauchy's theorem	R2, Ch 9, 175
13	1	**Tutorial**	
14	1	Finite abelian groups	R2, Ch 11, 210
15	1	**Tutorial**	
16	1	Theorems on finite abelian groups	R2, Ch 11, 210-211
17	1	Theorems on finite abelian groups	R2, Ch 11, 211
18	1	Recapitulation and discussion of possible questions	
Total number of hours planed for unit IV 9 hours			
UNIT-V			
1	1	Theorems on finite abelian groups	R2, Ch 11, 211
2	1	Theorems on finite abelian groups	R2, Ch 11, 211-212
3	1	**Tutorial**	
4	1	Theorems on finite abelian groups	R4, Ch 5, 249
5	1	**Tutorial**	
6	1	finitely generated abelian group	R2, Ch 11, 214
7	1	Theorems on finitely generated abelian group	R2, Ch 11, 214-215
8	1	Theorems on finitely generated abelian group	R2, Ch 11, 214-215
9	1	divisible and reduced groups	R2, Ch 11, 215
10	1	Theorems on divisible and reduced groups	R2, Ch 11, 216
11	1	**Tutorial**	
12	1	Theorems on divisible and reduced groups	R2, Ch 11, 216
13	1	**Tutorial**	
14	1	Theorems on divisible and reduced groups	R2, Ch 11, 216-217
15	1	Theorems on divisible and reduced groups	R2, Ch 11, 217
16	1	Torsion group	R2, Ch 11, 218
17	1	Recapitulation and discussion of possible questions	
18	1	Discusion of ESE qns	
19	1	Discusion of ESE qns/ **Tutorial**	
20	1	Discusion of ESE qns	
21	1	Discusion of ESE qns/ **Tutorial**	
22	1	Discusion of ESE qns	
Total number of hours planed for unit V 22 Hours			

Unit	Hours(L+T)
I	18(14+4)
II	20(15+5)
III	18(14+4)
IV	18(14+4)
V	22(16+6)
Total	96(73+23)

SUGGESTED READINGS

TEXT BOOK

1. Fraleigh.J. B., (2004). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.

REFERENCES

1. Artin .M., (2008). Algebra, Prentice-Hall of India, New Delhi.
2. Joseph A. Gallian., (2006). Contemporary Abstract Algebra, Fourth Edition, Narosa Publishing House, New Delhi.
3. Herstein. I. N., (2010). Topics in Algebra, Second Edition, Wiley and sons Pvt Ltd, Singapore.
4. Joseph J. Rotman, (2001). An Introduction to the Theory of Groups, Fourth Edition, Springer

UNIT-I

SYLLABUS

Symmetries of a square, Dihedral groups, definition and examples of groups including permutation groups and quaternion groups (illustration through matrices), elementary properties of groups

Introduction to set theory

The algebra of sets defines the properties and laws of sets, the set-theoretic operations of union, intersection, and complementation and the relations of set equality and set inclusion. It also provides systematic procedures for evaluating expressions, and performing calculations, involving these operations and relations.

Preliminary notations:

Set theory:

1. A set is any well defined class or collection of objects.
2. A set 'A' is said to be a subset of s. if every element in A is an element of s. if aεA=aεs.
3. A set is said to be a finite if it consists of a specific number of different elements, otherwise it is called as an infinite set.
4. Two sets A and B are said to be equal if and only if every element of A is an element of B, and also every element of B is an element of A.

   If the two sets A and B are equal then we write it as A=B.

   If the two sets A and B are not equal then we write it as A≠B.
5. A set which contains no element is called as null set or an empty set.
6. A set consisting of a single element is called singleton set.
7. Given a set S we use the notations as,

   $A=\{a\varepsilon s/p(a)\}$ means that A is the set of all the elements in s for which the property p holds
8. The union of the two sets A and B is denoted as AUB the set is $\{x/x\varepsilon A \text{ or } x\varepsilon B\}$.
9. The intersection of the two sets A and B is denoted as A∩B is the set $\{x/x\varepsilon A \text{ and } x\varepsilon B\}$.

10. The two sets A and B have no elements is then we say that A and B are disjoint or mutually exclusive.

Prepositions:

1. For any 3 sets A,B,C we have
   A∩(BUC)=(A∩B)U(A∩C)

   First we try to prove that

   (A∩B)U(A∩C)ς A∩(BUC)

   Now B ς BUC

   A∩B ς A∩(BUC)⟶ 1

   c ς BUC

   A∩C ς A∩(BUC)⟶ 2

   1 and 2 (A∩B)U(A∩C) ς A∩(BUC)⟶ 3

   Next we try to prove

   A∩(BUC) ς(A∩B)U(A∩C)

   xεA A∩(BUC)⟶ 4

   Let xεA and (xεB or xεC)

   xεA and xεB or xεA and xεC

   xε A∩B or xε A∩C

   xε(A∩B)U(A∩C)⟶ 5

   from 4 and 5 A∩(BUC) ς(A∩B)U(A∩C)⟶ 6

Definitions:

1. Given a set T we say that T serves as an index set for the family f.f=$\{A_\alpha\}$ of sets if for every $\alpha \varepsilon T$, there is a set of A_α is the family of F.The index set T can be any finite set or infinite.

2. By the union of sets A_α where α is in T, we mean the set
$\{x/x\varepsilon A_\alpha$ for atleast one α in T$\}$ we denote it by U A_α $\alpha \varepsilon T$.

3. By the intersection of he sets A_α where α is in T we mean that the set
$\{ x/x\varepsilon A_\alpha$ for every $\alpha \varepsilon T \}$ we denote it by $\cap$ $\alpha \varepsilon T$ A_α.

4. The sets A_α are mutually disjoint if $\alpha \neq \beta$ $A_\alpha \cap A_\beta$ is the null set.

5. Given the two sets A and B then the difdferenc set A-B is the set $\{x\varepsilon A/x\varepsilon B\}$ then B is a subset of A in this case we call A-B is the complement of B in A.

6. Let A and B be any two given sets then their Cartesian product A*B is defined as the set of all ordered pairs(a,b) where $a\varepsilon A$ and $b\varepsilon B$.

Note:

i) $(a_1,b_1)=(a_2,b_2)$ iff $a_1=a_2$ and $b_1=b_2$ given any index set T we can define the Cartesian product of the sets A_α as α varies over T.

ii) If the set A is a finite set having elements then the set A*A is also a finite set but has n^2 elements.

iii) The set of all elements (a,a) is A*A is called the diaponal of A*A.

Definition:

The binary relation ~ on A is said to be a equivalence relation if for all a,b,c is A.

i) a~a reflexing

ii) a~b=b~a symmetry
iii) a~b and b~c=a~c transistivity

Example:

Let s be the set of all integers given a,bεs defines a~b if a-b is even integer.

Solution:

i) since 0=a-a is even a~a

ii) if a~b then a-b is even –(b-a) is also even=b~a.

iii)if a~b then a-b is even and b~c then (b-c) is even.

a-c=(a-b)+(b-c) is also even=a~c.

The given relation is equivalence relation.

Definition:

If A is a set and if ~ is an equivalence relation on A then the equivalence class of aεA is the set {xεA/a~x} we write it as cl(a).

Fundamental theorem on equivalence relation:

Theorem 1.1.1

The distinct equivalence classes of an equivalence relation A provide us with a decomposition of A as a union of mutually disjoint subsets. Conversely given a decomposition of A as union of mutually disjoint, non empty subsets we can define an equivalence relation on A for which these subsets are the distinct equivalence classes.

Proof:

Let the equivalence relation on A be denoted by '~' since for any aεA, a~a.

A must be in cl(a).

Hence the union of the cl(a) is all of A we now try to prove that given two equivalence classes they are either equal or disjoint.

Now we suppose that cl(a) and cl(b) are not disjoint then f an element.

$x \varepsilon cl(a) \cap cl(b)$

Since $x \varepsilon cl(a)$ $a \sim x$

Since $x \varepsilon cl(b)$ $b \sim x$

But by the symmetry of relation we have $x \sim b$.

$a \sim x$ and $x \sim b = a \sim b \longrightarrow$ 1

Now we suppose that $y \varepsilon cl(b)$

$b \sim y \longrightarrow$ 2

1 and 2 $a \sim y = y \varepsilon cl(a)$.

Every element in cl(b) is in cl(a) $cl(b) \varsubsetneq cl(a) \longrightarrow$ 3

In a similar way we can prove that

$Cl(a) \varsubsetneq cl(b) \longrightarrow$ 4

3 and 4 cl(a)=cl(b)

Thus we have shown that the distinct cl(a) are either they are equal or disjoint.

Let us suppose that $A = uA_\alpha$ where A_α mutually disjoint non empty set[α is in the some index set]. Given an element a is A is exactly in one A_α.

We define for $a,b \varepsilon A, a \sim b$ if a and b are in the same A_α.

We now prove that this is an equivalence relations on a and that the distinct equivalence classes on the A_α.|.

Now a and a are in the same A_α. $a \sim a$.

Now assume that $a \sim b$, then by definition a and b are in the same A_α.

$b \sim a$ hence if $a \sim b = b \sim a$ then it follows that a and b are in the same A_α.

B and c are in the same A_β.

Now suppose that $A_\alpha \neq A_\beta$ since $b \varepsilon A_\beta . = A_\alpha \cap A_\beta \neq 0$

Which is a contradiction. Since A_α and A_β. Are distinct $A_\alpha=A_\beta$. Hence a and c are in the same A_α.

a~c thus a~b and b~c=a~c. thus the relation defined above satisfies reflexity symmetry and transitivity. Hence the above relation is an equivalence relation.

Lat aεA let A_α be the unique no of the partition such that aε A_α then by definition of ~ we get cl(a)= A_α.

Thus distinct equivalence classes are A_α.

State And Prove Demorgan's Theorem:

Statement:

For a subset c of s let $c^|$ denotes the complement of c in s. for any two subsets A,B of s we have,

i) $(A\cap B)^{|'}=A^| \cup B^|$ ii) $(AUB)^|= A^| \cap B^|$

Proof:

i)let $x\varepsilon(A\cap B)^|$ ⟶ 1

$x\not\varepsilon(A\cap B)$

$x\varepsilon A$ and $x\not\varepsilon B$

$x\varepsilon A^|$ and $x\varepsilon B^|$

$x\varepsilon A^| \cup B^|$ ⟶ 2

from 1 and 2 we get $(A\cap B^|)\varsigma A^| \cup B^|$ ⟶ 3

now let $x\varepsilon A^| \cup B^|$ ⟶ 4

$x\varepsilon A^|$ or $x\varepsilon B^|$

$x\varepsilon A$ or $x\not\varepsilon B$

$x\not\varepsilon(A\cap B)$

$x\not\varepsilon(A\cap B)^|$ ⟶ 5

from 4 and 5we get $(A^{|} \cup B^{|}) \varsigma (A \cap B)^{|} \longrightarrow 6$

from 3 and 6 we get $(A \cap B)^{|} = (A^{|} \cup B^{|})$

ii)$(AUB)^{|} = A^{|} \cap B^{|}$

let $x \varepsilon (AUB)^{|} \longrightarrow 1$

$x \text{ɛ} (AUB)$

$x \text{ɛ} A$ and $x \text{ɛ} B$

$x \varepsilon A^{|}$ and $x \varepsilon B^{|}$

$x \varepsilon A^{|} \cap B^{|} \longrightarrow 2$

from 1 and 2 we get $(AUB)^{|} \varsigma A^{|} \cap B^{|} \longrightarrow 3$

now let $x \varepsilon A^{|} \cap B^{|} \longrightarrow 4$

$x \varepsilon A^{|}$ and $x \varepsilon B^{|}$

$x \text{ɛ} A$ and $x \text{ɛ} B$

$x \text{ɛ} AUB$

$x \varepsilon (AUB)^{|} \longrightarrow 5$

from 4 and 5 we get $A^{|} \cap B^{|} \varsigma (AUB)^{|} \longrightarrow 6$

from 3 and 6 we get $(AUB)^{|} = A^{|} \cap B^{|}$.

Problem:

1. If A is a finite set having n elements then prove that A has exactly 2^n distinct subsets.

Solution:

Given that A is a finite set with n elements

Thus A contains obviously the empty set also that it contains the following subsets.

nc_1=number of 1 element subsets.

nc_2=number of 2 element subsets.

nc_n=number of n element subsets.

The total number of subsets=$nc_0+nc_1+nc_2+\ldots\ldots+nc_n$

$=1+nc_1+nc_2+\ldots\ldots\ldots+1$

From binomial theorem we know that

$(1+x)^n=1+nx+\frac{n(n-1)}{2!}x^2+\ldots\ldots\ldots..+x^n$

When x=1 we have,

$2^n=1+n+\frac{n(n-1)}{2!}+\ldots\ldots\ldots\ldots+1$

From these both we have the total no of subsets=2^n.

Introduction to Mappings

In mathematics, the term mapping, usually shortened to map, refers to either

A function, often with some sort of special structure, or

A morphism in category theory, which generalizes the idea of a function**.**

Mappings:

A mapping from a set S is a rule that associates with each element s in s a unique element t in T.

Note:

In the above case way that t is the unique of s under the mapping.

Definition:

If S and T are non empty sets then a mapping from s to T is a subset of M of s*t such that for every sεS there is a unique tεT such that the ordered pairs(s, t) is in M.

Note:

Let σ be a mapping from S to T we denote this by σ : ST or T=Sσ.

Examples:

1. Let S be any set. Define i:S $\Longrightarrow$S by s=si for any sets sεs. This mapping I is called the identity mapping.

2. Let S and T be any two sets and let t_0 be an element of T. define ψ:S $\Longrightarrow$T by an $\psi(s)=t_0$ for every sεs then ψ is a mapping.

3. Let S and T be any two sets. Define τ by $(a, b)\tau = a$ for any $(a, b)\varepsilon S*T$. this τ is called as the projection of S*T on S. in a similarity we can define the projection of S * T on T.

Note: .

Let S be any set we construct a new set s^*, the set whose elements are the subsets of S then we call S^* the set of subsets of S.

Example:

1. If $S=\{x_1, x_2\}$

Then $s^*= \{\{\}, \{x_1\}, \{x_2\}, S\}$

2.Given a mapping τ: T, we define for tεT, the inverse of t w.r.to τ to be the

set $\{s\varepsilon S/t=ST\}$.

Definition:

1.The mapping τ of S into T is said to be onto T if given tεT, F an element sεS such that t=st.
2. The mapping τ of s into T is said to be a one to one mapping. If whenever $s_1 \neq s_2$ then $s_1\tau \neq s_2\tau$.
3. The two mappings σ and τ of s into T are said to be equal is $s\sigma=s\tau$ for every sεs.
4. If σ:S $\Longrightarrow$ T and τ:T $\Longrightarrow$ U then the composition (or product) of τ andσ is the mapping $\sigma_0\tau$: S $\Longrightarrow$ U.
5. Defined by $s(\sigma_0\tau) =(s\sigma)\tau$ fro every s ε S
=tτ for every tεT
=u for every uεU.

Example:

Let $S = \{x_1, x_2, x_3\}$ and T=S.

Let σ : S$\Longrightarrow$S be defined by $x_1\sigma = x_2$, $x_2\sigma = x_3$, $x_3\sigma = x$ and τ : S$\Longrightarrow$S be defined by

$x_1\tau = x_1$, $x_2\tau = x_3$, $x_3\tau = x_2$

thus $x_1(\sigma_0\tau)=(x_1\sigma)\tau$

$= x_2\tau = =x_3$

$X_2(\sigma_0\tau)=(x_2\sigma)\tau$

$= x_3\tau = = x_2$

$X_3(\sigma_0\tau)=(x_3\sigma)\tau$

$= x_1\tau = = x_1$

$x_1(\tau_0\sigma)=(x_1\tau)\sigma$

$= x_2\sigma = = x_2$

$X_2(\tau_0\sigma)=(x_2\tau)\sigma$

$= x_3\sigma = = x_1$

$X_3(\tau_0\sigma)=(x_3\tau)\sigma$

$= x_2\sigma = = x_3$

So from above resets we conclude that is general $\sigma_0\tau \neq \tau_0\sigma$.

Lemma 1.2.1: Associative law:

If σ: S $\Longrightarrow$t, τ : T $\Longrightarrow$U and u: U $\Longrightarrow$V then

$(\sigma_0\tau)_0\mu = \sigma_0(\tau_0\mu)$

Proof:

We know that $\sigma_0\tau$ makes sense and takes S into U.

Thus $(\sigma_0\tau)_0\mu$ also makes sense and takes S into V.

Now let us prove for any sεS,

$S[(\sigma_0\tau)_0\mu]=s[\sigma_0(\tau_0\mu)]$

l.h.s $=s[(\sigma_0\tau)_0\mu]$

$=s(\sigma_0\tau)\mu$

$=((s\sigma)\tau)\mu$
$=s\sigma(\tau_0\mu)$

$= s[\sigma_0(\tau_0\mu)]$=r.h.s.= associative property.

Lemma 1.2.2:

Let σ:S$\Longrightarrow$ T and τ:T$\Longrightarrow$ U then

i) $\sigma_0\tau$ is onto if each of σ and τ is onto.

ii) $\sigma_0\tau$ is one to one if each of σ and τ is one to one.

Proof:

Since τ: T $\Longrightarrow$U is onto for a given uεU , F a tεT such that

$t\tau=u \longrightarrow 1$

since σ:S $\Longrightarrow$ T is onto

for given tεT F a sεS such that

$s\sigma=t \longrightarrow 2$

now $s(\sigma_0\tau)=(s\sigma)\tau$

$=t\tau$ by 2

=u by 1

Thus for every uεU F a sεS such that $s(\sigma_0\tau)=u$

Then by definition $\sigma_0\tau$ is onto

Let $s_1, s_2 \varepsilon s$ and $s_1 \neq s_2$

Since σ is one to one $s_1\sigma \neq s_2\sigma$

$s_1\sigma \& s_2\sigma$ are distinct elements in T.

since τ is one to one $s_1\tau \neq s_2\tau$

$= s_1(\sigma_0\tau)=(s_1\sigma)\tau \neq (s_2\sigma)\tau=s_2(\sigma_0\tau)$

$= s_1(\sigma_0\tau) \neq s_2(\sigma_0\tau)$

$=(\sigma_0\tau)$ is one to one by definition.

Note:

The converse of above lemma is false.

i) If$(\sigma_0\tau)$ is onto then σ and τ is need not be onto.

ii) $\sigma_0\tau$ is one to one if each of σ and τ is need not be one to one.

Definition:

Let σ:S T if σ is both one to one and on to then we say the mapping σ is one to one correspondence between S and T.

Lemma 1.2.3:

Statement:

The mapping σ: S $\Longrightarrow$ T is one to one correspondence between S and T iff there exists a mapping μ:T $\Longrightarrow$ S such that $\sigma_0\mu$ and $\mu_0\sigma$ are the identity mappings on S and T respectively.

Proof:

First let us assume that the mapping σ: S $\Longrightarrow$ T is a one to one correspondence between S and T.
Since σ is onto, for given tεT, F an element sεS such that sσ=t ⟶ 1
Since σ is one to one this s in must be unique now we define the mapping
σ^{-1}:T $\Longrightarrow$ S by s= t σ^{-1} iff t=sσ the mapping σ^{-1} is the inverse of σ.
Let $\sigma_0\ \sigma^{-1}$: s $\Longrightarrow$ S

Now for any sεS, s $(\sigma_0\ \sigma^{-1}) = (s\sigma)\ \sigma^{-1}$
$=t\ \sigma^{-1}$ by 1
= s
=si
$\sigma_0\ \sigma^{-1}$ is the identity mapping on s.
if we take $\mu= \sigma^{-1}$ then
$\sigma_0\mu$ is the identity mapping on s.
Now $\sigma^{-1}{}_0\sigma$: T $\Longrightarrow$ T then for any tεT.
$t(\sigma^{-1}{}_0\sigma)=(\ t\sigma^{-1})\sigma$
=sσ
=t
=ti

$\sigma^{-1}{}_0\sigma$ is the identity mapping on T.

Conversely if σ: S $\Longrightarrow$ T is such that F a mapping on μ: T $\Longrightarrow$ S with the property that $\sigma_0\mu$ and $\mu_0\sigma$ are the identity mapping on S and T respectively. Then we have to show that σ is a one to one correspondence between S and T. we have to show σ is both one to one and onto.

Let tεT then t=ti

$=t(\mu_0\sigma)=(t\mu)\sigma$

Now $t\mu$ is an element of S. so t is the image under σ of the element $t\mu$ in s. for a given $t\varepsilon T$ F a $t\mu\varepsilon S$ such that $(t\mu)\ \sigma=t$ by definition σ is onto.

Let $s_1, s_2\ \varepsilon\ S$ assume that $s_1\sigma=s_2\sigma$

Now consider $s_1=s_1(\sigma_0\mu)$

$=(s_1\sigma)\ \mu$

$=(s_2\sigma)\ \mu$

$=s_2\ (\sigma_0\mu)$

$=s_2\ (\sigma_0\mu$ is the identity on s)

Whenever $s_1\sigma=s_2\sigma=s_1=s_2$

Then by definition σ is one to one.

Definition:

A binary operation 0 on a non empty set A is a mapping which associates each pair (a, b) of elements of A an uniquely defined element $C\varepsilon A$ thus 0 is a mapping of product of the set A*A to A symbolically a map 0: A*A $\Longrightarrow$ A is called a binary operation on the set A.

Example:
Addition and multiplication on binary operation on N.
If S is non empty set then A(s) is the set of all one to one mappings of s onto itself.
Theorem: 1.2.1:
If σ, τ, μ are elements of A(S) then i) $\sigma_0\tau$ is in A(S)
ii) $(\sigma_0\tau)\ 0\mu=\sigma_0\ (\tau_0\mu)$
iii) F an element I the identity map in A(S) such that $\sigma_0 i=i_0\sigma$
iv)F an element $\sigma^{-1}\varepsilon A(S)$ such that $\sigma_0\sigma^{-1}=\sigma^{-1}0\sigma = i$
Proof:

1.Lemma 1.2.2

2.Lemma 1.2.1

3.Clearly the identity map 'i' is both one to and on to $i\varepsilon A(S)$ let $s\varepsilon S$

Now consider $s(\sigma_0 i)=(s\sigma)i$

$=s\sigma$ ¥ $s\varepsilon S=\sigma_0 i=\sigma$

Lemma 1.2.3(write the first part only).

Lemma: 1.2.4:

If s has more than two elements we can find two elements $\sigma*\tau$ in A(S) such that $\sigma_0\tau \neq \tau_0\sigma$.

Proof:

Let us assume that S has more than two elements let x_1, x_2, and x3 be three distinct elements in s.

Now we define σ: S$\Longrightarrow$S

By $x_1\sigma=x_2$

$X_2\sigma=x_3$

$X_3\sigma=x_1$

$S\sigma=s$ for only $s\varepsilon S$ different from x_1, x_2, x_3

Define τ: S$\Longrightarrow$S

By $x_2\tau=x_3$

$x_3\tau=x_2$

and $s\tau=s$ for any $s\varepsilon S$ different from x_2, and x3 clearly both σ and τ are one to one and on to and hence in A(S)

now $x_1(\sigma_0\tau)=(x_1\sigma)\tau$

$=x_2\tau$

$=x_3 \longrightarrow 1$

And $x_1(\tau_0\sigma)=(x_1\tau)\sigma$

$=x_1\sigma$

$=x_2 \longrightarrow 2$

Comparing 1 and 2 we observe that $\sigma_0\tau \neq \tau_0\sigma$.

Problem1:

If the set S has n elements then prove that A(S) has n! Elements.

Solution:

When $S=\{x_1, x_2, x_3...x_n\}$

Any one to one mapping on S onto itself is given by specifying the image of each elements.

The image of x_1 can be chosen is different ways. Since the image of x_2 is different from image of x_1 it can be chosen in n – 1 different ways and so on. Hence the total no of one to one mapping of s onto itself is n(n-1)(n-2)……3.2.1=n!.

Problem2:

If f: A$\Longrightarrow$B is a map and E_1, E_2 are any two subsets of A then show that

i) $f(E_1 \cup E_2)=f(E_1) \cup f(E_2)$

ii) $f(E_1 \cap E_2) \subseteq f(E_1) \cap f(E_2)$

Solution:

i) Let $b \in f(E_1 \cup E_2)$

$b=f(a)$ for some $a \in E_1 \cup E_2 \longrightarrow 1$

$b=f(a)$ for some $a \in E_1$ or $a \in E_2$

$b=f(a)$ and $f(a) \in f(E_1)$ or $f(a) \in f(E_2)$

$b=f(a)$ and $f(a) \in f(E_1) \cup f(E_2) \longrightarrow 2$

from 1 and 2 we get $f(E_1 \cup E_2) \subseteq f(E_1) \cup f(E_2) \longrightarrow 3$

now let $b' \in f(E_1) \cup f(E_2) \longrightarrow 4$

$b' \in f(E_1)$ or $b' \in f(E_2)$

$b'=f(a')$ for some $a' \in E_1$ or E_2

$b'=f(a')$ for some $a' \in (E_1 \cup E_2)$

$b'=f(a')$ for some $f(a') \in f(E_1 \cup E_2) \longrightarrow 5$

from 4 and 5 we get $f(E_1) \cup f(E_2) \subseteq f(E_1 \cup E_2) \longrightarrow 6$

from 3 and 6 we get $f(E_1 \cup E_2)= f(E_1) \cup f(E_2)$

ii) Let $b \in f(E_1 \cap E_2) \longrightarrow 7$

$b \in f(a)$ for some $a \in E_1 \cap E_2$

$b=f(a)$ for some $a\varepsilon E_1$ and $a\varepsilon E_2$

$b=f(a)$ and $f(a)\varepsilon f(E_1)$ and $f(a)\varepsilon f(E_2)$

$b=f(a)$ and $f(a)\varepsilon f(E_1)\cap f(E_2)$ ⟶ 8

from 7 and 8 we get $f(E_1\cap E_2)\varsigma f(E_1)\cap f(E_2)$

Introduction to Group Theory

In mathematics, a **group** is a set of elements together with an operation that combines any two of its elements to form a third element satisfying four conditions called the group axioms, namely closure, associativity, identity and invertibility. One of the most familiar examples of a group is the set of integers together with the addition operation; the addition of any two integers forms another integer. The abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

Group theory:

Definition of a group:

A non empty set G is called a group if in G there is defined a binary operation called a product and denoted by '.' Such that

i) For a, bεG $a.b\varepsilon G^{-1}$(closure property)

ii) a,b,cεG a.(b.c)=(a.b).c(associative property)

iii) F an element eεG such that a.e=e.a ¥ aεG e is called the identity of the element in G.

iv) For every aεG F an element $a^{-1}\varepsilon G$ such that $a.a^{-1}=a^{-1}.a=e$ eixtence of inverse.

The algebra structure of the group is given by (G,.).

Definition:

i) A group G is said to be an abelian group or commutative if for every a,bεG a.b=b.a

ii) A group which is not abelian is called a non abelian group.

iii) The order of a group G, denoted by o(G) is the no of elements in G.

iv) If G contains finite no of elements we say that G is a finite group otherwise it is called as an infinite group.

v) We know that if a set S contains 'n' elements then A(S) contains n! elements amd A(S) is a group. This group is called as the symmetric group of degree n denoted by s_n.

Some examples of groups.

Let G consists of the integers 0, ±1, ±2,…… where we means by a.b foe a,bεG the usually sum of integers that is a.b=a+b.

Solution:

Closure property:

Let a, b εG then a+bεG, since the sum of two integers is also an integer in G.

Associative property:

Let a,b,cεG then (a+b)+c=a+(b+c) since the associative property is true in the case of integers.

Existence of identity elements:

OεG, now a+o=a ¥aεG o is the additive identity element in G.

Existence of inverse element:

For any aεG we can find an element –a in G such that a+(-a)=0

-a acts as the inverse for a in G (G, +) is a group.

Examples:

1. The set of all 2*2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a,b,c,dεR is a group under matrix addition.
2. Q,R,C groups are all under usual addition.
3. Let G consists of real nos (1, -1) under the binary operation multiplication then G is an abelian group of order 2.
4. Since sum of two integers is commutative for any a,bεG a+b=b+a G is an abelian group. Also G contains infinite number of elements. G is an infinite abelian group to the binary operation addition.

Some preliminary lemmas:

Lemma 2.3.1:

If G is a group then

1. The identity element of G is unique.
2. Every aεG has an unique inverse in G.
3. Left and right cancellation laws hold

   a.b=a.c b=c

   b.a=c.a b=c

4. for every aεG $(a^{-1})^{-1}=a$

5. for all aεG $(a.b)^{-1}=b^{-1}.a^{-1}$

Proof:

If possible let there be two I denoted elements e, f in G.

Let aεG since e is the identity. Consider f as an ordinary elements in G. then by the definition,

a.e=e.a=a

f.e=e.f=f

since f is the identity consider e as an ordinary element in G. then by definition

a.f=f.a=a

e.f=f.e=e

we know that e.f=f and e.f=e f=e hence the identity element is unique.

2. let aεG

If possible let there be two inverses $a^{|}$ and $a^{||}$ for a in G. then by definition we know that $a.a^{|}=a^{|}.a=e$

$a.a^{||}=a^{||}.a=e$

Since e is the identity element we can wriye

$a^{|} = a^{|}.e$

$= a^{|}.(a.a^{|})$

$= (a^{|}.a).a^{||}$

$= e.a^{||}$

$= a^{||}$

$a^{|} = a^{||}$ hence every element in G has a unique inverse.

3.. let $a,b,c \varepsilon G$ let us suppose that $a.b=a.c$

Since $a \varepsilon G$ $a^{-1} \varepsilon G$

Now premultiplying by a^{-1} we get

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

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

$e.b=e.c$

$b=c$

left cancellation law is true.

Since $a \varepsilon G$ $a^{-1} \varepsilon G$ now post multiplying by a^{-1} we get

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

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

$b.e=c.e$

right cancellation law is true.

4. let $a \varepsilon G$ let a^{-1} be the inverse of a in G then $(a^{-1})^{-1}$ will be the inverse of a^{-1} in G.

Since G is a group we have

$a. a^{-1}= a^{-1}.a=e$ and $a^{-1}(a^{-1})^{-1}=(a^{-1})^{-1}. a^{-1}=e$

we have $a^{-1}.a= a^{-1}.(a^{-1})^{-1}$

using left cancellation law we have $a=(a^{-1})^{-1}$.

5.. let $a,b \varepsilon G$ let $a^{-1,} b^{-1}$ be the inverse of a and b in G.

Then a.b and $b^{-1}. a^{-1}$ exists in G by closure property

Now we consider

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

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

$=a.\ a^{-1}$

$=e$

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

Lemma 2.3.2:

Given a,b in the group G then the equations a.x=b and y.a=b have unique solutions for x and y in G.

Proof:

Given that $a,b \varepsilon G$

Since $a,b \varepsilon G$, $a^{-1} \varepsilon G$

$. x=a^{-1}.b \varepsilon G$

Now consider

$a.x=a.(a^{-1}.b)$

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

$=e.b$

$=b$

X satisfies the given equation and hence $x=a^{-1}.b$ is a solution.

To establish the uniqueness of the solution, let there be two solution x_1 and x_2 for the equation a.x=b

We have $a.x_1=a.x_2$

$x_1=x_2$

henc $x=a^{-1}.b$ is a unique solution for a.x=b. in a similar way we can prove that $y=b.a^{-1}$ is a unique solution for y.a=b.

Problem:

Show that the set G ={ a+b√2: a,b∈Q} is a group with respect to addition.

Solution:

Closure Property:

Let x,y be any two elements of G. Then x= a+b√2, y = c+d√2, where a,b,c,d ∈Q

Now x+y=(a+c)+(b+d) √2∈Q,

Thus x+y ∈G for every x,y ∈G.

Therefore G is closed with respect to addition.

Associativity:

The elements of G are all real numbers and the addition of real numbesr is associative.

Existence of identity:

We have 0+0√2 ∈G since 0∈Q.

If a+b√2 is any element of G, then (0+0√2)+(a+b√2) = a+b√2

0+0√2 is the identity.

Existence of inverse:

We have a+b $\sqrt{2} \in G \Rightarrow (-a) + (-b)\sqrt{2} \in G$ since a, b ∈ Q ⇒ - a, -b ∈ Q.

Now [(-a)+(-b)$\sqrt{2}$] + $[a + b\sqrt{}] = [(-a) + a] + [-b) + b]\sqrt{2} = 0 + 0\sqrt{2} =$ the left identity.

There for (-a) +(-b)$\sqrt{2}$ is the left inverse of a+b$\sqrt{2}$.

Hence G is a group with respect to addition.

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. i) Prove that $A\cap(B\cup C) = (A\cap B) \cup (A\cap C)$

ii) If a finite set S has n elements, then prove that the power set S has 2^n elements.

2. Write about the types of binary operations.

3. If G is a group ,then prove that
i)the identity element of G is unique
ii)every $a\in G$ has a unique inverse in G
iii)for every $a\in G$, $(a^{-1})^{-1} = a$
iv)for all $a,b\in G$, $(a.b)^{-1} = b^{-1}.a^{-1}$

4. If a,b are any two elements of a group G, then prove that the equations ax = b and ya = b have unique solutions in G.

5. Show that the set $G =\{ a+b\sqrt{2}: a,b\in Q\}$ is a group with respect to addition.

6. i) Prove that the inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order.
ii)Show that if every element of the group G is its own inverse , then G is abelian.

7. Let G be a group. Then prove that i) identity element of G is unique
ii) for any $a\in G$, the inverse of a is unique.

8. Prove that if G is an abelian group, then for all $a,b\in G$ and all integers n, $(a.b)^n=a^n.b^n$.

9. If G is a group, in which $(a.b)^i = a^ib^i$ for three consecutive integers i for all $a,b\in G$. Show that G is abelian.

10. If a.b.c are any elements of G, then prove that $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

UNIT-II

SYLLABUS

Subgroups and examples of subgroups, centralizer, normalizer, center of a group, product of two subgroups

Introduction to Subgroups

In algebra, given a group G under a binary operation $*$, a subset H of G is called a subgroup of G if H also forms a group under the operation $*$. More precisely, H is a subgroup of G if the restriction of $*$ to $H \times H$ is a group operation on H. This is usually represented notationally by $H \leq G$, read as "H is a subgroup of G".A proper subgroup of a group G is a subgroup H which is a proper subset of G (i.e. $H \neq G$). The trivial subgroup of any group is the subgroup {e} consisting of just the identity element. If H is a subgroup of G, then G is sometimes called an overgroup of H.The same definitions apply more generally when G is an arbitrary semigroup, but this article will only deal with subgroups of groups. The group G is sometimes denoted by the ordered pair (G, $*$), usually to emphasize the operation $*$ when G carries multiple algebraic or other structures.This article will write ab for $a * b$, as is usual.

Sub groups:

A non empty subset H of a group G is said to be a subgroup of G if under the product is G,H itself forms a group.

Note:

If H is a subgroup of G and K is a subgroup of H, K is a subgroup of G.

Lemma 2.1:

A non empty subset H of a group G is a subgroup of G itself:

i) $a, b \varepsilon H = ab \varepsilon H$
ii) $a \varepsilon H = a^{-1} \varepsilon H$

Proof:

First we assume that H is a subgroup of G then by definition H is a group under the same binary operation as in G.

$a, b \varepsilon H = ab \varepsilon H$ and

$a \varepsilon H = a^{-1} \varepsilon H$, ¥ a, b εH

conversely let us assume that,

$a, b \varepsilon H = ab \varepsilon H$ and

$a \varepsilon H = a^{-1} \varepsilon H$, ¥ a, b εH

now we prove that H is a subgroup of G. from the first result we observe that closure property is valid.

Since H is a non empty subset of G since the associative law is true in G, itmust be true to H also.

Associativity is true also.

From the second result we observe that inverse exists for every element of H.

Existence of inverse is true.

Once again the second result is a, $a^{-1}\varepsilon H$

$aa^{-1}\varsigma e\varepsilon H$

Existence of identity is true.

Hence H is a subgroup of G.

Note:

It is enough if we prove that if a, $b\varepsilon H$ then $ab^{-1}\varepsilon H$ where H is a subgroup of G.

Lemma 2.2:

If H is a non empty finite subset of a group G and H is closed under multiplication then H is a subgroup of G.

Proof:

By hypothesis $a,b\varepsilon H=ab\varepsilon H$

Let us now prove that $a\varepsilon H=a^{-1}\varepsilon H$

It is given that H is closed under multiplication

Let $a\varepsilon H$ then $a^2=a.a\varepsilon H$

Let $a^3=a^2.a\varepsilon H$……

H contains infinite no of elements a, a^2, a^3…… but H is given to be a finite subset of the group G. thus there must be repetitions, in this collection of elements.

For some integers r, s with r>s>0 $a^r=a^s$

Let $a^{r-s} = a^0 =e$

But $a^{r-s}\varepsilon H$ since r-s>0 by definition of H

Let $e\varepsilon H$

Now consider $a^{r-s}=e$

$(a^{r-s})a^{-1}a=e$

$a^{r-s-1}=a^{-1}$ but $a^{r-s-1}\varepsilon H$

but $a^{-1}\varepsilon H$ where $a\varepsilon H$.

We have $a,b\varepsilon H=ab\varepsilon H$ and $a\varepsilon H=a^{-1}\varepsilon H$ where H is subgroup of G.

Examples:

1. Let G be the group of integers under addition H the subset consisting of all the multiplies of 5. Then H is a subgroup of G.

2. Let G be the group of all real nos under addition and H be the set of all integers then H is a subgroup of G.

3. Let G be the group of all non zero complex numbers a+ib(a, b real not both zero) under multiplication and let $H=\{a+ib\varepsilon G/a^2+b^2=1\}$ then H is a subgroup of G.

4. Let G be any group $a\varepsilon G$ let $(a)=\{a^i/i=0,+-1,\ldots\ldots\}$ then a is a subgroup of G. it is called as cyclic subgroup generated by a.

5. Let G be the group of all 2*2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with the condition $ad-bc\neq 0$ under multiplication. Let H= $\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \varepsilon G/ad \neq 0\}$ H is called subgroup of G.

Definition:

Let G be a group H a subgroup of G also let $a,b\varepsilon G$ then we say that a is concurrent to bmodH, written as $a \equiv b \bmod H$ if $ab^{1}\varepsilon H$

Lemma 2. 3:

The relation $a \equiv b \bmod H$ is an equivalence relation.

Proof:

Let a, b, c ε H

It is given that H is a subgroup of G eεH aa ^{1}=eεH

Then by definition a ≡ a mod H

Reflexitivity is true.

Now we assume that a ≡ b mod H

Then by definition ab $^{-1}$εH

(ab $^{-1}$) $^{-1}$εH

(b $^{-1}$) $^{-1}$a $^{-1}$εH ba $^{-1}$εH

Let b ≡ a mod H symmetry is true.

Now we assume that a ≡ b mod H and b ≡ c mod H. then by definition

ab $^{-1}$εH and bc $^{-1}$εH

Since H is a subgroup closure property is true ab $^{-1}$bc $^{-1}$ ac $^{-1}$εH

Then by definition a ≡ c mod H.

Transition is true. Then the relation is an equivalence relation.

Definition:

if H is a subgroup of G and aεG, then H_a={h_a/hεH} is called a right coset of H in G. ah={ah/hεH} is called left coset of H in G.

Lemma 2.4:

For all aεG H_a={xεG/a ≡ x mod H}.

Proof:

Let [a]= {xεG/a ≡ x mod H}.

Then it is enough if we prove that H_a=[a]

First we try to prove that H_aς[a]

Let xεH_a then x=Ha for some hεH

Post multiplying by a $^{-1}$ we get,

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

$(xa^{-1}\varepsilon h)$

$(xa^{-1})^{-1}\varepsilon H$

$(a^{-1})^{-1}x^{-1}\varepsilon H$

$ax^{-1}\varepsilon H$

$a \equiv x \bmod H \quad x \equiv a \bmod H$

$x \varepsilon [a]$

hence $H_a \varsubsetneq [a]$

to prove that $[a] \varsubsetneq H_a$

let $x\varepsilon[a]$ then by definition $a \equiv x \bmod H$

$ax^{-1}\varepsilon H$

$(ax^{-1})^{-1}\varepsilon H$

$xa^{-1}\varepsilon H$

So $xa^{-1}=n$ for $n\varepsilon H$

Post multiplying by 'a' we get

$xa^{-1}a=h_a$

$xe=h_a$

$x=h_a$

but $ha\varepsilon H_a$

$x\varepsilon H_a$

$[a] \varsubsetneq H_a$

From $H_a=[a]$ hence the proof.

Result:

Prove that any two right coset of H in G are either identical or have no element is common.

Proof:

We know that $H_a=[a]$ is an equivalence class of a in G. then by a theorem 1.1.1 these equivalence classes yields a decomposition of g into disjoint subsets. Thus any two right coset H in G are either identical or have no element in common.

Let us consider two right coset H_a and H_b of H in G where a, b εG.

Assume that H_a and H_b have an element C in common.

$C\varepsilon H_a \cap H_b$

$C\varepsilon H_a$ and $C\varepsilon H_a$ and H_b

$C=h_1a$ and $c=h_2b$ for some $h_1, h_2\varepsilon H$ $h_1a=h_2b$

Pre multiplying both sides by h_1^{-1} we get

$h_1^{-1}h_1a= h_1^{-1}h_1b$

$a=h_3b$ where $h_3=h_1^{-1}h_2$

$H_a=Hh_3b$

$=H_b$

$H_a=H_b$

Any two right coset of H in G are either identical or have no element is common.

Lemma 2.4.5:

There is a one to one correspondence between any two right cosets of H in G.

Proof:

Let G be a group and H a subgroup of G. let a, b εG

Let H_a and H_b be two right cosets of H in G

Define Φ: $H_a \longrightarrow H_b$

By $\Phi(h_a)=h_b$ ¥ $h\varepsilon H \longrightarrow$ 1

Let us prove that the mapping Φ is one to one and onto let $h_1, h_2 \varepsilon H$

Then h_1a and $h_2a \varepsilon H_a$

Now $\Phi(h_1a)=\Phi(h_2a)$

Let $h_1b=h_2b$

Let $h_1=h_2$

Post multiplying we get $h_1a=h_2a$

Φ is one to one by its definition

Let $h_b \varepsilon H_b$ then $h \varepsilon H$

. $h_a \varepsilon H_a$

But we have the mapping $\Phi(h_a)=h_b$

For every element $h_b \varepsilon H_b$ F an element $h_a \varepsilon H_a$ such that $\Phi(h_a)=h_b$

Thus Φ is a one to one correspondence.

Theorem 2.1:

Lagrange's theorem:

Statement:

If G is a finite group and H is a subgroup of G, then o(H) is a division of o(G).

Proof:

Since $H_a=[a]$ any two right coset being

i) Equivalence classes are either disjoint or identical.
ii) Also the union of the distinct right coset in G.
iii) Let there be K distinct right coset. Since there is an one to one correspondence between any two right cosets, all the right cosets have the same no of elements.
But H=He is a right coset and has o(H) elements. So the K distinct right cosets each having o(H) elements fill out g.

So K.o(H)=o(G)
o(H) is a divisor of o(G)
Hence the theorem.

Note:

let G be aa finite group.

H be a subgroup of G we know that o(H) is a divisor of o(G).

o(H)/o(G)

o(G)=K.o(H) where K is the no of distinct right cosets of H in G.

K=o(G)/o(H)

Problem:

Given an example of an infinite subgroup of an infinite group whose index infinite.

Solution:

Let G=z

Let H=2z

i^H_G=number of distinct right cosets of H in G=2.

Definition:

Let G be a group and aεG. The order or period of a is the least positive integer m such that a^m=e. it is denoted by o(a)

o(a)=m

.$a^{o(a)}$=e

If no such integer exists then a is of infinite order.

Example:

G={1,-1,I,-i} here 1 is the multiplicative identity.

e=1 $(-1)^2$=1 i^4=1 i^8=1 i^{12}=1 $(-i)^4$=1 $(-i)^8$=1 $(-i)^{12}$=1

0(-1)=2 0(i)=4 0(-i)=4

Corollary's for lagrange's theorem:

Corollary 1:

if G is a finite group and aεG then o(a)/o(G).

Proof:

Let us produce the subgroup of G whose order is 0(a). consider the cyclic subgroup generated by a.

(a)={e,a,a^2,……..}

Now $a^{o(a)}$=e(by def)

The subgroup has atmost 0(a) number of elements.

If it has less than 0(a) number of elements then $a^i=a^j$ for some integers I and j where $o\leq i\leq j\leq o(a)$ j-i>0 a^{j-i}=e but o<j-i<o(a).

We have an integer j-i<0(a) for which a^{j-i}=e contradicting the definition of o(a).

The cyclic group a has exactly o(a) number of elements then by lagrange's theorem o(a)/o(G)

Corollary 2:

If G is a finite group and aεG then $a^{o(G)}$=e

By corollary 1 we have o(a)/o(G)

o(G)/o(a)=k where K is some positive integer

o(G)=k.o(a)

Now $a^{o(g)}=a^{k.o(a)}$

$(a^{o(a)})^k=e^k$=e

Hence $a^{o(G)}$=e

Definition:

If a and b are relatively prime, we can find integers m and n such that ma+nb=1.

Corollary 3:

Euler's theorem:

If n is a positive integer and 'a' is a integer which is relatively prime to n then $a^{\Phi(n)} \equiv 1 \mod n$ where Φ(n) is the number of positive integer less than n and relatively prime to n.

Proof:

Let G={[x]/x is an integer less than n and relatively prime to n}.

We know that G is a group w.r.to multiplication of reside classes as the composition also now o(G)=Φ(n)

If 'a' is a positive integer relatively prime to n then [a]εG

. $[a]^{o(G)}$=identity=[1]

i.e., [a][a].....[a]=1

i.e.,$a^{\Phi(n)}=1$

i.e.,$a^{\Phi(n)}=1 \mod n$

hence the corollary.

Corollary 4:

Fermat's theorem:

Statement:

If p is a prime number and a is any integer then ap=a mod p.

Proof:

let G be the set of non zero residue classes of integers module p. if p is a prime number then w.r.to multiplication of residue classes. A is a group of order p-1. The identity elements of this group is [1].

Now suppose a is an integer

Case 1:

p is an divisor of a.

p/a

p/a^b

p/a^p-a

a^p=a mod p

case ii) p is not a divisor of a.

in this case [a]≠o [a]εG

now $a^{o(G)}$=[1] by corollary 2

a^{p-1}=[1]

p/a^{p-1}-1

p/a^p-a

a^p≡a mod p hence the corollary.

Definition:

In a group G and e are said to be trivial subgroup of G and the remaining subgroups are called non trivial subgroup of G.

Corollary 5:

If G is a finite group whose order is a prime number then G is a cyclic group or prove that finite group of prime order is cyclic.

Proof:

Let G be a finite group.

Let o(G)=p where p is a prime number

G has no non trivial subgroupsH

If H is a non trivial subgroup of G then by lagranges theorem o(H)/o(G)=p

Since p is prime its divisors are 1 and p.

o(H)=1 or o(H)=p

If o(H)=1 then since ?H is subgroup of G we must have h=G

G has no non trivial subgroup H let us assume that a≠eεG and H=(a), then H is a cyclic subgroup generated by (a) but H≠{e} since a≠e.
H=G(G has no non trivial subgroup)
G is a cyclic group generated by (a).

A counting principle:

Let H and K be any two sungroups of a group G. define HK={xεG/x=hk,hεH,kεK} HK is a non empty subset of G. but HK need not be a subgroup of G.

Example:

Let $G=s_3=\{e, \Phi, \psi, \psi^2, \Phi\psi, \psi\Phi\}$

$O(s_3)=6$ let $H=\{e, \Phi\}$ and $K=\{e, \Phi\psi\}$ H and K are subgroups of G. sine they are closed and inverse of Φ and $\Phi\psi$ are themselves respectively.

Now $HK=\{e,\Phi\Phi\psi,\Phi^2\psi\}$ $(\Phi^2=e)$

HK consists of 4 elements and 4*6 by lagranges theorem HK is not a subgroup.

Lemma 2.5:

HK is a subgroup of G iff HK=KH.

Proof:

First let us suppose that HK=KH now we try to prove that HK is a subgroup of G since eεHK, HK is a non empty subset of G. since HK=KH we have $h_1k_1=k_2h_2$

$H_1,h_2\varepsilon H$ $k_1, k_2\varepsilon K$

Here it need not be $h_1=h_2$ and $k_1=k_2$

Let $x_1y\varepsilon HK$

Then $x=h_1k_1$ $y=h_2k_2$ $h_1h_2\varepsilon H$ $k_1k_2\varepsilon K$

Now consider $xy=(h_1k_1)(h_2k_2)$

$=h_1(k_1h_2)k_2=h_1(h_3k_3)k_2=(h_1h_3)(k_3k_2)\varepsilon HK$

HK ic closed.

Let xεHK

Then x=hk for some hεH kεK

Now $x^{-1}=(hk)^{-1}$

$=k^{-1}h^{-1}\varepsilon KH=HK$

$X^{-1}\varepsilon HK$ whenever xεHK

Then by a lemma HK is a subgroup of G.

Conversely let us assume that HK is a subgroup of G. then we prove that HK=Kh

Let $h\varepsilon H_1$ kεK then khεKH

Let $h\varepsilon H_1$ kεK then khεKH

Since H and k are subgroup of G.

$h\varepsilon H=h^{-1}\varepsilon H$

$k\varepsilon K=k^{-1}\varepsilon K$

$h^{-1}k^{-1}\varepsilon HK$

$(h^{-1}k^{-1})^{-1}\varepsilon HK$

$(k^{-1})^{-1}(h^{-1})^{-1}\varepsilon HK$

khεHK

KHεHK

Now let xεHK

Then $x^{-1}\varepsilon HK$

x^{-1}=hk where hεH , kεK

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

$x=k^{-1}h^{-1}\varepsilon KH=HK\varsigma KH$

HK=KH

Hence HK is a subgroup of iff HK=KH

Corollary:

If H and K are subgroups of an abelian group G then Hk is a subgroup of G.

Proof:

Hk is a non empty subset of g since G is aabelian and H, K are subgroups of G we have hk=kh ¥ kεK, hεH
HK=Kh
Then by the above lemma HK is a sub group of G.

Theorem 2.2:

If H and K are are finite subgroups of G of orders o(H) and o(K) respectively then $o(HK)=\frac{o(H).o(K)}{o(H\cap K)}$

Proof:

Case i) let $H\cap K=\{E\}$ $o(H\cap K)=1$

In this acse it is enough to prove that o(HK)=o(H).o(K)

The elements of HK are h_1k_1, h_2k_2,h_3k_3……

Where h_1, h_2 ,h_3…….εH and k_1, k_2, k_3,…….εk

This list contains o(H).o(K) no of elements.

Claim:

Each product in this list is distinct $h_1k_1\neq h_2k_2$ whenever $h_1\neq h_2$ if possible let us assume that $h_1k_1=h_2k_2$ whenever $h_1\neq h_2$.

Per multiplying by h_2^{-1} and post multiplying by k_1^{-1} on both sides we get

$h_2^{-1}h_1k_1k_1^{-1}= h_2^{-1}h_2k_2k_1^{-1}$

$h_2^{-1}h_1= k_2k_1^{-1}$

but $h_2^{-1}h_1\varepsilon H$ and $k_2k_1^{-1}\varepsilon K$

$h_2^{-1}h_1\varepsilon H\cap K=\{e\}= h_2^{-1}h_1=e$ $h_2=h_1$

a contradiction to our assumption H is a subgroup. Thus our assumption is wrong. Hence each product in this list is distinct all the elements in this list of HK are distinct having o(H).o(K) number of elements. Thus in this case H∩K={e}

we have o(HK)= $\frac{o(H).o(K)}{o(H\cap K)}$

case ii) H∩K≠{e}

we shall know show that the list of elements of HK contains repetitions elements, repeating exactly o(H∩K) times.

Let $h_1 \varepsilon H\cap K$

Then $hk=(hh_1)(h_1^{-1}) \longrightarrow 1$

Where $hh_1 \varepsilon H$ and $h_1^{-1} k \varepsilon K$ thus hk is duplicated in the product atleast o(H∩K) times however if $hk=h^{-1}k^{-1}$

Then $h^{-1}hk(k^1)^{-1}=h^{-1}h^1k^1(k^1)^{-1}$

$K(k^1)^{-1}=h^{-1}h^1=u$ (say)

$u \varepsilon H\cap K$

$h^1=hu \quad k^1=u^{-1}k$

thus all duplications are taken into consideration in equation 1.

Hk appears in the list of HK exactly o(H∩K) times.

Thus the number of distinct elements in HK is the total no of elements in the list HK.

O(H).o(K) divided by the no of times a given element appears namely o(H∩K)

o(HK)= $\frac{o(H).o(K)}{o(H\cap K)}$.

Definition:

Cyclic group:

A group G is called a cyclic group if for some $a \varepsilon G$, every element $x \varepsilon G$ is of the form a^m where m is the some integer. The element a is called a generator of G.

Normal subgroups and Quotient groups.

Definition:

Let G be a group. A sub group N of G is said to be a normal subgroup of G, if for every gεG and nεN, gng $^{-1}$εN.

Equivalently if gNg $^{-1}$={gng $^{-1}$/nεN} then N is a normal subgroup of G. then gNg $^{-1}$ς ¥ gεG.

Lemma 2.6:

N is a normal subgroup of G iff gNg $^{-1}$=N ¥ gεG.

Proof:

If gNg $^{-1}$=N for every gεG, certainly gNg $^{-1}$ςN so by definition N is normal in G.

Now let us assume that N is normal in G. then by definition if gεG, gNg $^{-1}$ςN

Now gNg $^{-1}$= gN(g ¯1) ¯1ςN ¥ g $^{-1}$εG

Now since gNg $^{-1}$ςN, N=g(g $^{-1}$Ng)g $^{-1}$ς gNg $^{-1}$ςN

Now we get, gNg $^{-1}$=N ¥ gεG hence the lemma.

Lemma 2.7:

The subgroup N of G is a normal subgroup of G iff every left coset of N is G is a right coset of N in G.

Proof:

Let us assume that N is a normal subgroup of G then by a lemma 2.6 gNg $^{-1}$=N ¥ gεG.

Post multiplying both sides by g we get gNg $^{-1}$g=Ng

i.e., gN=Ng

every left coset of N in G is a right coset of N in G. conversely let N be a subgroup of G. every left coset of N in G is also a right coset of N in G. let g be any element of G. then gN=Ng for some gεG.

Since eεN, ge=gεgN=Ng

gεNg

also g=egεNg i.e.,gεNg

$gN=Ng$

post multiplying both sides by g^{-1} we get

$gNg^{-1}=Ngg^{-1}$

$gNg^{-1}=N$

then by a lemma 2.6 N is a normal subgroup of G.

Note:

If H is a subgroup of G then HH=H or $H^2=H$.

Proof:

Now $HH=\{h_1h_2/h_1h_2 \varepsilon H\} \varsubsetneq H$

$HH \varsubsetneq H$

$HH \in He \in H$

$HH \in H$

$HH=H$ or $H^2=H$

Lemma 2.6.3:

A subgroup N of G is a normal subgroup of G iff the product of the two right cosets of N in G is a right coset of N in G.

Proof:

First we assume that N is a normal subgroup of G. let a, $b \varepsilon G$ and consider the two right cosets Na and Nb.

Now NaNb=N(aN)b

=(NN)ab

=Nab

=Nc where $c=ab \varepsilon G$

Hence the product of any two right cosets of N in G is again a right cosets of N in G.

Conversely let us assume that the product of any two right cosets of N in G is again a right coset of N in G.

We have to prove that N is a normal in G. by hypothesis NaNb=Nc for some cεG

First we try to prove that NaNb=Nab

To prove that Nc=Nab

Now ab=eaeb=NaNb=Nc

abεNc

now ab=eabεNab

abεNab

but we know that any two right cosets are either distinct or identical.

Now we get Nab=Nc

Hence we have let a=g, b=g^{-1}

Then we have $NgNg^{-1}=Ngg^{-1}$

$NgNg^{-1}=N$ ¥ gεG

Now gNg^{-1}ε gNg^{-1}¥nεN

$gNg^{-1}=e$ gNg^{-1}ε$NgNg^{-1}=N$

gNg^{-1}εN ¥ gεG and nεN

then by definition N is a normal subgroup of G.

Hence the lemma.

SYLOWS THEOREM:

Statement:

Suppose G is a group of finite order and p is a prime number. If p^m/o(G) and p^{m+1} is not a divisor of o(G), then G has a subgroup of order p^m.

Proof:

We shall prove that the theorem by induction on o(G).

The theorem is true if o(G)=1

if o(G)=1 then $p^o/o(G)$ and $p^|*o(G)$ and G has a subgroup G itself of order p*{e}

let us assume the theorem is true for groups of order less than that of G.

let $o(G)=p^m.n$ where p is not a divisor of n. if m=0, then the theorem is p={e} obviously true.

If m=1 the theorem is true by cauchys theorem.

So let m>1 then G is a group of composite order and so G must posses a subgroup H such that H≠G

If p is not a divisor of o(G)/o(H), then $p^m/o(H)$ because $o(G)=p^m.n=o(H).o(G)/o(H)$ also p^{mh} cannot be a divisor of o(H) because p^{mh} will be a divisor of o(G) of while o(H) is divisor.

Further o(H)<o(G) by our induction hypothesis, the theorem is true for H.

H is a subgroup of order p^m and this will also be a subgroup of G. so let us assume that for every subgroup H of G where H≠G,

P is a divisor of o(G)/o(H)

Consider the class equation,

O(G)=o(z)+∑aεz o(G)/o(N(a))

Since aεz N(a)≠G,

According to our assumption p is a divisor of ∑aεz o(G)/o(N(a))also p/o(G)

We conclude that p is a divisor of o(z).

Then by cauchys theorem z has an element b of order p.

Hence z is the center of G. also N={b} is a cyclic subgroup of z of order p.

Since bεz N is a normal subgroup of G of order p.

Now consider the quotient group $G^|=G/N$

Then $o(G^|)=o(G^|)/o(N)=p^mn/p=p^{m-1}$

$O(G^|)<o(G)$

By our induction hypothesis $G^{|}$ has a subgroup $s^{|}$ of order p^{m-1}

We know that

Φ: G $\Longrightarrow$ G/N defined as $\Phi(x)=Nx¥x\varepsilon G$ is a homomorphism of G onto G/N with kernel N.

Let $S=\{x\varepsilon G/\Phi(x)\varepsilon S^1\}$

Then S is a subgroup of G and $S^1 \approx S/N$

$O(S^1)=o(S^*)/o(N)$

$O(s)=o(s^1).o(N)=p^{m-1}.p=p^m$

S is a subgroup of order p^m

Hence the theorem.

CAUCHY'S THEOREM:

Statement:

Suppose G is finite abelian group and p/o(G) i.e., p is a divisor of o(G) where p is a prime number. Then there is an element $a\neq e\varepsilon G$. Such that $a^p=e$.

Proof:

Let us prove that this theorem by the method of this induction on the order of G.

Assume that the theorem is true for abelian groups of order is less that G.

The theorem is vacuously true for groups of order one.

If G has no proper subgroups then G must be of prime order because every group of composite order possesses proper subgroups.

But p is prime and p/o(G)=o(G) must be p. also we know that every group of prime order is cyclic each element $a\neq e$of G will be a generatorof G.

G has p-1 element as $a\neq e$ such that $a^p=a^{o(G)}=e$.

If G has a proper subgroup H $H\neq\{e\}$ and $H\neq G$ and if p/o(H) then by our induction hypothesis the theorem is true for H and also H is abelian group with $o(H)<o(G)$.

F an element $b\varepsilon H$ and $b\neq e$ show that $b^p=e$.

Let us assume that p is not a divisor of o(H). since G is a abelian . H is a normal subgroup of G and so G/H is a quotient group.

Since G is a abelian G/H is also abelian.

Since $o(G/H)<o(G)$ since $o(H)>1$ since p/o(G) and p is not a divisor of o(H).

P is a divisor of o(G)/o(H). hence by our induction hypothesis the theorem is true for the group G/H.

Since H is the identity element of G/H F an element C in G such that $H_c\neq H$ is G/H.

So that $(H_c)^p=H$

With quotient group G/H, $o(H_c)=p$

$(H_c)^p=H$

$H_c{}^p=H=C^p\varepsilon H$

By corollary of lagranges theorem we have $(C^p)^{o(H)}=e$

$(C^{o(H)})^p=e$

$d^p=e$

let us prove that this $d\neq e$.

if we assume that d=e, then consider that

$(H_c)^{o(H)}=H_c{}^{o(H)}$

$=H_d$

$=H_e$

$=H$

$(H_c)^{o(H)}=H$ is the identity of G/H.

But $o(H_c)=p$ as $H_c=G/H$

p/o(H) which is a contradiction our assumption d=e is wrong

d≠e

=dp=e

d≠e show that d^p=e

hence the induction theorem is proved.

CAUCHY THEOREM :

Statement:

If p is a prime number and p/o(G) then G has an element of order p.

Proof:

It is given that let G be a group and let aεG is the order of a is the least +ve integer m show that a^m=e

1. P is a prime number.
2. p/o(G).

we shall prove this theorem by the method of induction on o(G).

Hence we may assume this theorem is true for all subgroups of G such that

o(T)<o(G) ⟶ 1

if possible let W≠G be a subgroup of G. hence from equ1 p/o(W). then F an element b_1≠eεW show that b_1p=e. hence the theorem.

In this case let us assume that let p is not a divisor of any proper subgroup of G.

Let aȼz(A) ⟶ 3

N(a)≠G ⟶ 4

And also let us assume that p is not a divisor of o(N(a)).

p ╳ $_o$(N(a)) ⟶ 5

we write the class equation as

o(G)=o(z(G))+∑aȼz(G) o(G)/o(N(a)) ⟶ 6

we have p/o(G) ⟶ 7 from the hypothesis of the theorem we have

p ╳ o(N(a)) ⟶ 8 from the equ5

p ∕ ∑a∉z(a) o(G)/o(N(a)) ⟶ 9

then equ6 can be written as

p ∕ (o(G)-∑a∉z(a) o(G)/o(N(a)))=o(z(G)) ⟶ 10

from 7 and 9 we have p ∕ o(G)- ∑aεz(a) o(G)/o(N(a)) ⟶ 11

p/o(z(G)) ⟶ 12

but in this case we have p is not a divisor of any proper subgroup

from 11 and 12 the only possibility is z(G)=G

G is abelian.

The remaining problem of this theorem will be true by use of cauchys theorem for abelian groups.

Cauchys theorem for abelian group is suppose G is a finite abelian group and p is divide o(G) where p is prime then F an element a≠e show that a^p=e.

SYLOWS THEOREM FOR ABELIAN GROUP:

STATEMENT:

If G is an abelian group of order o(p) and if p is a prime number show that pα/o(G) then G has a subgroup of order pα.

Proof:

If α=0 then the subgroup satisfies the conclusion of the result so let us suppose that α≠0 then p/o(G).

Then by cauchys theorem for abelian group there is an element a≠eεG, a^p=e

Let S={xεG/xp^n=e for some integer n} we have ep^n;e<s.

GεS and a≠e s=e s is non empty

We claim that S is a subset of G. if possible let w≠G be a subgroup of G hence p/o(W) then F an element b_1≠eεW show that b_1^p=e hence the theorem in this case is let us assume that p is not a divisor of the order of any proper subgroup of G.

Let aεz(G) ⟶ 3

N(a)≠G ⟶ 4

P ╳ N(A) ⟶ 5

We write the class equation as,

O(G)=o(z(G))+∑aεz(G)o(G)/o(N(G)) ⟶ 6

We have p/o(G) from the hypothesis of the theorem

P ╳ o(N(a)) from equ 5

p/ aεz(G)o(G)/o(N(G)) ⟶ 9

then 6 can be written as

o(G)- aεz(G)o(G)/o(N(G)) =0(Z(a)) ⟶ 10

from 7 and 9 we have

p/o(G)-∑aεx(G) o(G)/o(N(a))=p/o(z(G)) ⟶ 11

if H is a non empty finite subset of a group G and H is closed under multiplication then H is a subgroup of G, it is enough if we verify that H is closed.

Let x,y εS.

x^{pn}=e yp^m=e for some integers.

Now $(xy)^{p\ n+m}=x^{p\ m+n}$

$=xp^n.p^m$ yp^np^m

$=(xp^n)p^m.(yp^m)p^n$

=e.e=e

$(xy)^{pn+m}$=e for some integer n+m

xyεs s is closed.

S is a subgroup of G. we next claim that $o(s)=p^{\beta}$

With β as an integer $o<\beta<\alpha$.

FOR IF f A PRIME NUMNER Q SHOW THAT Q/0(S),$q\neq p$ then by cauchys theorem for abelian group there is an element $c\varepsilon s$, $e\neq e$, show that $c^{q}=e$ since $c\varepsilon s$, $c^{pn}=e$ for some integer n.

Now p^{n} and q are respectively prime.

We can find integers λ, μ show that $\lambda q+\mu p^{n}=1$

$C=c^{|}=c\ \lambda q+\mu p^{n}=c^{\lambda q}.c\ \mu p^{n}$

$=(c^{q}).(c^{pn})^{\mu}$

$=e^{\lambda}.e^{\mu}=e$

C=e this is a contradiction to the fact that $c\neq e$. there is no prime number $q/o(s)$ and $q\neq 0$ $o(s)=p^{\beta}$ for some β show that $0<\beta<\alpha$. by cauchys theorem $o(S)/o(G)$. $\beta\leq\alpha$. Let us assume that $\beta<\alpha$. Let us consider the abelian group G/s
G is abelian G/S is also abelian.
Now $o(G/s)=o(G)/o(S)$ s is a normal subgroup of an abelian group is normal. And $\beta<\alpha=p/o(G/S)$. there is an element $s_x(x\varepsilon G)$ is G/S, $s_x\neq S$ such that $(S_x)^{pn}=S$ from some integer $n>0$. But $S=(S_x)^{pn}=s_xp^{n}=x^{pn}\varepsilon s$. $e=(x^{pn})^{o(s)}=(x^{pn})^{p\beta}=x^{pn+\beta}$ $x\varepsilon s$
$s_x=s$ which is a contradiction to the fact that $s_x\neq s$ $\beta<\alpha$ is impossible. the only possibility is

$\beta=\alpha$. $O(s)=p^{\alpha}$.

S is the required subgroup of order p^{α}.

Hence the theorem.

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. Let H be a subgroup of G. Then prove that

   i) the identity element of H is the same as that of G

   ii) for each $a\in H$ the inverse of a in H is the same as the inverse of a in G.

2. State and prove Lagrange's theorem.

3. A non-empty subset H of a group G is a subgroup of G iff
   i) $a \in H, b \in H \Rightarrow ab \in H$
   ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

4. State and prove Fermat theorem.

5. If H and K are finite subgroups of G of orders O(H) and O(K), then prove that
   $O(HK) = \frac{O(H)O(K)}{O(H \cap K)}$.

6. Prove that A subgroup H of a group G is a normal subgroup of G if and only if the product of two right coset of H in G is a right coset of H in G.

7. State and prove Euler's theorem.

8. i) Prove that N is a normal subgroup of G if and only if $gNg^{-1} = N$ for all $g \in G$.
   ii) Prove that a subgroup of cyclic group is cyclic.

9. Prove that the subgroup N of G is a normal subgroup of G iff every left coset of N in G is a right coset of N in G.

10. Let G be a group , N be a normal subgroup of G and G/N denote the collection of all right cosets of N in G. Then prove that G/N is a group under the operation defined by $(Na)(Nb) = Nab$, for all $Na, Nb \in G/N$.

UNIT-III
SYLLABUS

Properties of cyclic groups, classification of subgroups of cyclic groups. Cycle notation for permutations, properties of permutations, even and odd permutations, alternating group,

Introduction to Homomorphism

A homomorphism is a map that preserves selected structure between two algebraic structures, with the structure to be preserved being given by the naming of the homomorphism.

- A semigroup homomorphism is a map that preserves an associative binary operation.
- A monoid homomorphism is a semigroup homomorphism that maps the identity element to the identity of the codomain.
- A group homomorphism is a homomorphism that preserves the group structure. It may equivalently be defined as a semigroup homomorphism between groups.
- A ring homomorphism is a homomorphism that preserves the ring structure. Whether the multiplicative identity is to be preserved depends upon the definition of *ring* in use.
- A linear map is a homomorphism that preserves the vector space structure, namely the abelian group structure and scalar multiplication. The scalar type must further be specified to specify the homomorphism, e.g. every **R**-linear map is a **Z**-linear map, but not vice versa.
- An algebra homomorphism is a homomorphism that preserves the algebra structure.
- A functor is a homomorphism between two categories.

Homomorphism's :

Definition:

A homomorphism is a mapping from one algebraic system to a like algebraic system which pressures structure.

A mapping Φ from a group G into a group $\overline{G}$ is said to be a homomorphism for all $a,b \varepsilon G$ $\Phi(ab)=\Phi(a).\Phi(b)$.

Example:

Let $\Phi:\overline{G} \Longrightarrow \overline{G}$ also let $G = G$ and $\Phi(x)=e \forall x \varepsilon G$

Then Φ is a homomorphism.

Proof:

Let $x,y \varepsilon G$ is defined by let $G = \overline{G}$ and $\Phi(x)=e ¥ x \varepsilon G$

$\Phi(x)=e \quad \Phi(y)=e$

Since $x,y \varepsilon G$ we have $xy \varepsilon G$

$\Phi(xy)=e$

Moreover $\Phi(x).\Phi(y)=e.e$

$=e$

Now we have $\Phi(xy)= \Phi(x).\Phi(y)$

Φ is homomorphism.

Lemma 3.1:

Suppose G is a group, N a normal subgroup of G define the mapping Φ from G to G/N by $\Phi(x)=N_x$ for all $x \varepsilon G$. Then Φ is a homomorphism of G onto G/N.

Proof:

Let $x,y \varepsilon G$

Then $\Phi(x)=N_x$ and $\Phi(y)=N_y$ where ¥ $x,y \varepsilon G$

Since $x,y \varepsilon G, xy \varepsilon G$

$\Phi(xy)=N_{xy}$

$=N_x.N_y$

$=\Phi(x).\Phi(y)$

Then by definition Φ is a homomorphism of G into G/N let $y \varepsilon G/N$ then $Y=N_x$ where $x \varepsilon G$ and $\Phi(x)=N_x=Y$

Foe every $Y \varepsilon G/N$, F an element of x in G such that $\Phi(x)=Y$.

Then by definition Φ is onto.

Hence Φ is a homomorphism of G onto G/N.

Note:

Φ is called the canonical homomorphism of G, onto G/N.

Definition:

Let Φ be a homomorphism of G into $\overline{G}$ then the kernel of Φ is denoted by $K\Phi$ is defined as $k\Phi=\{x\varepsilon G/\Phi(x)=\overline{e}\}$ where e is the identity element of $\overline{G}$.

Lemma 3.2:

If Φ is a homomorphism of G onto $\overline{G}$ then

i) $\Phi(\overline{e})=e$, the unit element of $\overline{G}$

ii) $\Phi(x^{-1})=[\Phi(x)]^{-1}$ ¥ $x\varepsilon G$

Proof:

i) Let $x\varepsilon G$ then $\Phi(x)\varepsilon\overline{G}$

Consider $\Phi(x)\ \overline{e}=\Phi(x)$

$=\Phi(xe)$

$=\Phi(x).\Phi(e)$

$=\Phi(e)$

ii) Now $e=\Phi(\overline{e})$

$=\Phi(xx^{-1})$ ¥$x\varepsilon G$

$=\Phi(x).\Phi(x^{-1})$

$=[\Phi(x)]^{-1}=\Phi(x^{-1})$

Hence the lemma

Note:

The above lemma shows that e is the kernel of any homomorphism.

The kernel k is always a non empty subset of G.

Lemma 3.3:

If Φ is a homomorphism of G into $\overline{G}$ with kernel k_1 then k is a normal subgroup of G. (or) the kernel of a homomorphism is a normal subgroup.

Proof:

By the previous lemma we have $e\varepsilon k$

K is a non empty subset of G.

Let $x_1 y\varepsilon k$ then by definition $\Phi(x)=\overline{e}$ and $\Phi(y)=\overline{e}$

Now consider $\Phi(xy)=\Phi(x).\Phi(y)$

$=\overline{e}\ .\ \overline{e}$

$=\overline{e}$

xyεk whenever x,yΦk

Let xεk then by definition $\Phi(x)=\overline{e}$

Now consider $\Phi(x^{-1})=[\Phi(x)]^{-1}$

$=(\overline{e})^{-1}$

$=\overline{e}$

X^{-1}εk whenever xεk

K is a subgroup of G

Let aεG and xεk then by definition $\Phi(x)=\overline{e}$

Now consider $\Phi(axa^{-1})=\Phi(a)\Phi(x)\Phi(a^{-1})$

$=\Phi(a)\overline{e}\Phi(a^{-1})$

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

$=\Phi(aa^{-1})$

$=\Phi(e)$

$=\overline{e}$

axa^{-1}εk ¥xεk and aεG

K is normal subgroup of G.

Lemma 3.4:

If Φ is a homomorphism of G onto $\overline{G}$ with lernel k then the set of all inverse images of $\overline{g}\,\overline{G}$ under Φ in G is given by k_x, where x is any particular inverse image of $\overline{g}$.

If $\overline{g}$ ε $\overline{G}$ then we say that an element xεG is an inverse image of $\overline{g}$ under Φ_1

If $\Phi(x)=\overline{g}$

If $\overline{g}=\overline{e}$ then the set of all inverse images of $\overline{g}$ is k.

Let $\overline{g}\neq\overline{e}$ if kεK and $y=kx\neq kx$ then $\Phi(k)=\overline{e}$

Now consider

$\Phi(y)=\Phi(kx)=\Phi(k).\Phi(x)$

$=\overline{e}\Phi(x)$

$=\Phi(x)$

$=\overline{g}$ by definition

Y=kx is also an inverse image of g thus all the elements is kx are mapped into g whenever $\Phi(x)=\overline{g}$

Even if any othr element z in G is the inverse image of $\overline{g}$ and $\overline{G}$. we can shw that $z\varepsilon kx$

Now $\Phi(z)=\overline{g}$ but $\Phi(x)=\overline{g}$

$\Phi(z)=\Phi(x)$

$\Phi(z)[\Phi(x)]^{-1}=\overline{e}$

$\Phi(z)\Phi(x^{-1})=\overline{e}$

$\Phi(zx^{-1})=\overline{e}$

$zx^{-1}\varepsilon k \quad z\varepsilon kx$

Kx contains exactly all the inverse images of $\overline{g}$ whenever x is a single such inverse image Hence the lemma.

Note:

If k={e} then by lemma 2.7.4 $\overline{g}\varepsilon G$ has exactly one inverse image. Φ is a one to one mapping.

Definition:

Isomorphism:

A homomorphism Φ from a group G into a group $\overline{G}$ is said to be an isomorphism if Φ is one to one.

Definition:

Two groups G, G^* are said to be isomorphic if there is an homomorphism of G onto G^*. in this case we write $G\approx G^*$

We have the following three facts

i) $G\approx G^*$

ii) $G\approx G^*= G^*\approx G$

iii) $G\approx G^{*=}G^*\approx G^{**}=G\approx G^{**}$

Hence the relation of isomorphic is the set of all groups is an equivalent relation.

Corollary:

A homomorphism Φ of G into G with the kernel k is an isomorphism of G into G iff k={e}.

Proof:

Let us first assume that Φ is an isomorphic of G into G

Then by definition Φ is one to one

Let aεk Φ(a)=e where e is the identity element of G.

=Φ(e)

Φ(a)=Φ(e)

A=e Φ is one to one.

K={e}

inversly assume that k={e} now it is enough to show that Φ is one to one let x,yεG then Φ(x), $\Phi(y)\varepsilon\overline{G}$

now Φ(x)=Φ(y)

post multiplying on both sides we get $[\Phi(y)]^{-1}$ then we have

$\Phi(x)[\Phi(y)]^{-1}=\Phi(y)[\Phi(y)]^{-1}$

$\Phi(x).\Phi(y^{-1})=\overline{e}$

$\Phi(xy^{-1})=\overline{e}$

$xy^{-1}\varepsilon k=e$

$xy^{-1}=e$

x=y

there Φ is one to one and hence Φ is isomorphic.

Theorem 3.1:

Fundamental theorem on homomorphism of groups.

Let Φ be a homomorphism of G onto $\overline{G}$ with kernel k then $G/k\approx\overline{G}$

(or)

Every homomorphic image of G is isomorphic to some quotient group of G.

Proof:

Let us define $\psi: G/k \longrightarrow \overline{G}$ by

$\Psi(ka)=\Phi(a) \longrightarrow$ 1 where ka is any element of G/k and aεG.

Let us first prove that the mapping to show that ka=kb ψ(ka)=ψ(kb)¥ka,kbεG/k

A, bεG

Now we assume that ka=kb

Now a¥ka=kb

Aεkb

a=kb where kεk ⟶ 2

now ψ(ka)=Φ(a) by equ 1

=Φ(kb) by equ 2

=Φ(k)Φ(b)

=Φ(b)

=¥ψ(kb) by equ 1

Ψ(ka)=ψ(kb) whenever ka=kb

Ψ is called well defined.

Let ka, kb εG/k where a, bεG

Now ψ(ka, kb)=ψ(kab)

=Φ(ab)

=Φ(a)Φ(b)

=ψ(ka).ψ(kb)

Ψ is homomorphism

Given that Φ is onto for every $\overline{g}\varepsilon\overline{G}$ F a gεG such that $\Phi(g)=\overline{g}$

$\Psi(kg)=\overline{g}$

For every $\overline{g}$ ε $\overline{G}$ kgεG/k such that $\psi(kg)=\overline{g}$

Then by definition ψ is onto

Let us show that ψ is one to one by showing that the kernel of ψ namely kψ consists of only one element k which is the identity element of G/k.

By definition kψ={kaεG/k/ψ(ka)=$\overline{e}$}

={kaεG/k/Φ(a)=$\overline{e}$ }

={k}

Then by previous corollary ψ is one to one then by definition G/k≈$\overline{G}$.

Note:

From theorem 2.7.1 we note that the groups G/k form homomporphic images of the given group G where k is normal in G. but by lemma 2.7.1 for any normal subgroup N of G, G/N is a homomorphic images of G. thus there is a one to one correspondence between homomorphc images of G and normal subgroup of G. to get all homomorphic images of G we can find all normal subgroups of G and construct all groups G/N. the set of all such constructed groups gves all homomorphic images of G.

Definition:

A group is said to be simple if it has no non trivial normal subgroups. If it has non trivial homomorphic images.

Lemma 3.5:

Let Φ be a homomorphism of G onto $\overline{G}$ with kernel k. For H a subgroup of G. let H be defined by H={xεG/Φ(x)εH} then H is a subgroup of G and H>k. if H is normal in G then H is normal in G. moreover this association sets up a one to one mapping from the set of all subgroup of G which contains k.

Proof:

Let us first show that kçH and H is a subgroup of G.

Let kεk.

Then by definition Φ(k)=$\overline{e}$

Now $\overline{e}$ ε $\overline{H}$

Φ(k)εH

.kεH

.kçH

Now $\Phi(e)=\overline{e} \varepsilon \overline{H}$

$e\varepsilon H$

H is a non empty subset of G. let x, y εH

$\Phi(x)\varepsilon\overline{H}$, $\Phi(y)\varepsilon\overline{H}$

Now consider $\Phi(xy)$

$\Phi(xy)=\Phi(x).\Phi(y)\varepsilon\overline{H}$

$xy\varepsilon\overline{H}$

let $x\varepsilon H$ $\Phi(x)\varepsilon\overline{H}$

$[\Phi(x)]^{-1}\varepsilon\overline{H}$

$\Phi(x^{-1})\varepsilon\overline{H}$

$X^{-1}\varepsilon H$

$X^{-1}\varepsilon H$ then by lemma H is a subgroup of G containing kernel k.

ii).. given that $\overline{H}$ is normal in $\overline{G}$

we have to prove that H is normal in g.

let $a\varepsilon G$ and $x\varepsilon H$

then by definition of H $\Phi(x)\varepsilon\overline{H}$

$\Phi(a)\varepsilon\overline{G}$

Now consider $\Phi(axa^{-1})=\Phi(a).\Phi(x).\Phi(a^{-1})$

$=\Phi(a)\Phi(a)[\Phi(a)]^{-1}\varepsilon\overline{H}$

$Axa^{-1}\varepsilon H$ this is true ¥aεg and $x\varepsilon H$

H is normal in G.

Lemma 3.6:

Let G be a group for gεG defined as Tg:G $\Longrightarrow$ G by $xTg=g^{-1}xg$ ¥xεG prove that Tg is an automorphism of G to itself.

Proof:

Let x, y εG then xyεG

Now (xy)Tg=g -1(xy)g

$=g^{-1}xgg^{-1}yg$

$=(g^{-1}xg)(g^{-1}yg)$

=xTg.yTg

Tg is homomorphism.

For every yεG $x=gyg^{-1}$εG such that $xTg=g^{-1}xg$

$=g^{-1}gyg^{-1}g$

=y

Tg is onto.

We shall now prove that Tg is one to one

Now xTg=yTg

$g^{-1}xg=g^{-1}yg$

x=y

Tg is one to one

Thus Tg is an isomorphism of G onto itslf and hence Tg is an sutomorphism of G to itself.

Theorem 3.2:

Let Φ be a homomorphism of G ang $\overline{G}$ with kernel k and let $\overline{N}$ be a normal subgroup of $\overline{G}$,N={xεG/Φ(x)ε$\overline{N}$}. Then G/N≈$\overline{G}$/ $\overline{N}$ equivalently G/N≈G/k/N/k

Proof:

Define a mapping ψ:G⟶ $\overline{G}$ / $\overline{N}$ by

Ψ(g)=$\overline{N}$Φ(g) ¥gεG

Since Φ is onto for every $\overline{g}$ ε $\overline{G}$ F a gεG such that Φ(g)=$\overline{g}$

$\overline{N}$Φ(g)=$\overline{N}$ $\overline{g}$

ψΦ(g)=$\overline{N}$ $\overline{g}$= $\overline{N}$Φ(g)

for every element $\overline{N}$Φ(g)such that ψ(g)=$\overline{N}$Φ(g).

by definition ψ is onto.

Claim:

Ψ is a homomorphism.

Let x, y εG

Then $\psi(xy)=\overline{N}\Phi(xy)$

$=\overline{N}\Phi(x).\Phi(y)$

$\Psi(x).\psi(y)$

Ψ is a homomorphism.

Claim:

the kernel of ψ is N.

assume that T is the kernel of ψ then we prove that N=T

tεT

$\psi(t)=\overline{N}$

$\overline{N}\Phi(t)=\overline{N}$

$\Phi(t)\varepsilon\overline{N}$

tεN

TςN

Let xεN $\Phi(x)\varepsilon\overline{N}$ $\overline{N}\Phi(x)=\overline{N}$ $\psi(x)=\overline{N}$ xεT NςT

N=T

The kernel of ψ is N.

Thus ψ is a homomorphism of G onto $\overline{N}$ is kernel N.

Then by a theorem 3.1 $G/N\approx G/\overline{N}$

We shall now show that

$\overline{G}\approx G/K$ and $\overline{N}\approx N/k$

By theorem 3.1 we have

$G/K\approx\overline{G}$

Since isomorphism is an equivalent relation we can write $\overline{G}\approx G/k$

From the definition of N and $\overline{N}$ Φ is restricted to N as the range $\overline{N}$

$N/k \approx \overline{N}$

$\overline{N} \approx N/k$

$G/N \approx G/k/N/k$

SYLOWS THEOREM:

Statement:

Suppose G is a group of finite order and p is a prime number. If $p^m/o(G)$ and p^{m+1} is not a divisor of o(G), then G has a subgroup of order p^m.

Proof:

We shall prove that the theorem by induction on o(G).

The theorem is true if o(G)=1

if o(G)=1 then $p^o/o(G)$ and $p^{|}*o(G)$ and G has a subgroup G itself of order p*{e}

let us assume the theorem is true for groups of order less than that of G.

let $o(G)=p^m.n$ where p is not a divisor of n. if m=0, then the theorem is p={e} obviously true.

If m=1 the theorem is true by cauchys theorem.

So let m>1 then G is a group of composite order and so G must posses a subgroup H such that $H \neq G$

If p is not a divisor of o(G)/o(H), then $p^m/o(H)$ because $o(G)=p^m.n=o(H).o(G)/o(H)$ also p^{mh} cannot be a divisor of o(H) because p^{mh} will be a divisor of o(G) of while o(H) is divisor.

Further o(H)<o(G) by our induction hypothesis, the theorem is true for H.

H is a subgroup of order p^m and this will also be a subgroup of G. so let us assume that for every subgroup H of G where $H \neq G$,

P is a divisor of o(G)/o(H)

Consider the class equation,

$O(G)=o(z)+\sum a \& z\ o(G)/o(N(a))$

Since $a \& z \quad N(a) \neq G$,

According to our assumption p is a divisor of ∑aεz o(G)/o(N(a))also p/o(G)

We conclude that p is a divisor of o(z).

Then by cauchys theorem z has an element b of order p.

Hence z is the center of G. also N={b} is a cyclic subgroup of z of order p.

Since bεz N is a normal subgroup of G of order p.

Now consider the quotient group $G^{|}$=G/N

Then $o(G^{|})=o(G^{|})/o(N)=p^{m}n/p=p^{m-1}$

$O(G^{|})<o(G)$

By our induction hypothesis $G^{|}$ has a subgroup $s^{|}$ of order p^{m-1}

We know that

Φ: G ⟹ G/N defined as Φ(x)=Nx¥xεG is a homomorphism of G onto G/N with kernel N.

Let S={xεG/Φ(x)εS^{1}}

Then S is a subgroup of G and S^{1}≈S/N

$O(S^{1})=o(S^{*})/o(N)$

$O(s)=o(s^{1}).o(N)=p^{m-1}.p=p^{m}$

S is a subgroup of order p^{m}

Hence the theorem.

CAUCHY'S THEOREM:

Statement:

Suppose G is finite abelian group and p/o(G) i.e., p is a divisor of o(G) where p is a prime number. Then there is an element a≠eεG. Such that a^{p}=e.

Proof:

Let us prove that this theorem by the method of this induction on the order of G.

Assume that the theorem is true for abelian groups of order is less that G.

The theorem is vacuously true for groups of order one.

If G has no proper subgroups then G must be of prime order because every group of composite order possesses proper subgroups.

But p is prime and p/o(G)=o(G) must be p. also we know that every group of prime order is cyclic each element a≠eof G will be a generatorof G.

G has p-1 element as a≠e such that $a^p=a^{o(G)}=e$.

If G has a proper subgroup H H≠{e} and H≠G and if p/o(H) then by our induction hypothesis the theorem is true for H and also H is abelian group with o(H)<o(G).

F an element bεH and b≠e show that $b^p=e$.

Let us assume that p is not a divisor of o(H). since G is a abelian . H is a normal subgroup of G and so G/H is a quotient group.

Since G is a abelian G/H is also abelian.

Since o(G/H)<o(G) since o(H)>1 since p/o(G) and p is not a divisor of o(H).

P is a divisor of o(G)/o(H). hence by our induction hypothesis the theorem is true for the group G/H.

Since H is the identity element of G/H F an element C in G such that H_c≠H is G/H.

So that $(H_c)^p=H$

With quotient group G/H, $o(H_c)=p$

$(H_c)^p=H$

$H_c{}^p=H=C^p$εH

By corollary of lagranges theorem we have $(C^p)^{o(H)}=e$

$(C^{o(H)})^p=e$

$d^p=e$

let us prove that this d≠e.

if we assume that d=e, then consider that

$(H_c)^{o(H)}=H_c{}^{o(H)}$

$=H_d$

$=H_e$

$=H$

$(H_c)^{o(H)}=H$ is the identity of G/H.

But $o(H_c)=p$ as $H_c=G/H$

p/o(H) which is a contradiction our assumption d=e is wrong

$d\neq e$

=dp=e

$d\neq e$ show that $d^p=e$

hence the induction theorem is proved.

CAUCHY THEOREM :

Statement:

If p is a prime number and p/o(G) then G has an element of order p.

Proof:

It is given that let G be a group and let aεG is the order of a is the least +ve integer m show that $a^m=e$

1. P is a prime number.
2. p/o(G).

we shall prove this theorem by the method of induction on o(G).

Hence we may assume this theorem is true for all subgroups of G such that

$o(T)<o(G)$ ⟶ 1

if possible let W≠G be a subgroup of G. hence from equ1 p/o(W). then F an element $b_1\neq e\varepsilon W$ show that $b_1p=e$. hence the theorem.

In this case let us assume that let p is not a divisor of any proper subgroup of G.

Let aȼz(A) ⟶ 3

$N(a) \neq G \longrightarrow 4$

And also let us assume that p is not a divisor of o(N(a)).

$p \not| \ o(N(a)) \longrightarrow 5$

we write the class equation as

$o(G)=o(z(G))+\sum a \not\in z(G)\ \ o(G)/o(N(a)) \longrightarrow 6$

we have $p/o(G) \longrightarrow$ 7 from the hypothesis of the theorem we have

$p \not| \ o(N(a)) \longrightarrow$ 8 from the equ5

$p \not| \sum a \not\in z(a)\ o(G)/o(N(a)) \longrightarrow$ 9

then equ6 can be written as

$p \not| (o(G)-\sum a \not\in z(a)\ o(G)/o(N(a)))=o(z(G)) \longrightarrow$ 10

from 7 and 9 we have $p \not| o(G)- \sum a \in z(a)\ o(G)/o(N(a)) \longrightarrow$ 11

$p/o(z(G)) \longrightarrow$ 12

but in this case we have p is not a divisor of any proper subgroup

from 11 and 12 the only possibility is z(G)=G

G is abelian.

The remaining problem of this theorem will be true by use of cauchys theorem for abelian groups.

Cauchys theorem for abelian group is suppose G is a finite abelian group and p is divide o(G) where p is prime then F an element $a \neq e$ show that $a^p=e$.

SYLOWS THEOREM FOR ABELIAN GROUP:

STATEMENT:

If G is an abelian group of order o(p) and if p is a prime number show that $p\alpha/o(G)$ then G has a subgroup of order $p\alpha$.

Proof:

If $\alpha=0$ then the subgroup satisfies the conclusion of the result so let us suppose that $\alpha \neq 0$ then p/o(G).

Then by cauchys theorem for abelian group there is an element $a \neq e \varepsilon G$, $a^p = e$

Let $S = \{x \varepsilon G / xp^n = e$ for some integer n$\}$ we have $ep^n; e < s$.

$G \varepsilon S$ and $a \neq e$ $s = e$ s is non empty

We claim that S is a subset of G. if possible let $w \neq G$ be a subgroup of G hence p/o(W) then F an element $b_1 \neq e \varepsilon W$ show that $b_1^p = e$ hence the theorem in this case is let us assume that p is not a divisor of the order of any proper subgroup of G.

Let $a \not\varepsilon z(G) \longrightarrow$ 3

$N(a) \neq G \longrightarrow$ 4

P $\not|$ N(A) $\longrightarrow$ 5

We write the class equation as,

$O(G) = o(z(G)) + \sum a \not\varepsilon z(G) o(G)/o(N(G)) \longrightarrow$ 6

We have p/o(G) from the hypothesis of the theorem

P $\not|$ o(N(a)) from equ 5

$p/ a \not\varepsilon z(G) o(G)/o(N(G)) \longrightarrow 9$

then 6 can be written as

$o(G) - a \varepsilon z(G) o(G)/o(N(G)) = 0(Z(a)) \longrightarrow 10$

from 7 and 9 we have

$p/o(G) - \sum a \varepsilon z(G)\ o(G)/o(N(a)) = p/o(z(G)) \longrightarrow$ 11

if H is a non empty finite subset of a group G and H is closed under multiplication then H is a subgroup of G, it is enough if we verify that H is closed.

Let $x, y \varepsilon S$.

$x^{pn} = e$ $yp^m = e$ for some integers.

Now $(xy)^{p\ n+m} = x^{p\ m+n}$

$= xp^n.p^m\ yp^n p^m$

$= (xp^n)p^m.(yp^m)p^n$

$= e.e = e$

$(xy)^{pn+m}=e$ for some integer n+m

xyεs s is closed.

S is a subgroup of G. we next claim that $o(s)=p^{\beta}$

With β as an integer $o<\beta<\alpha$.

FOR IF f A PRIME NUMNER Q SHOW THAT Q/0(S),q≠p then by cauchys theorem for abelian group there is an element cεs, e≠e, show that $c^q=e$ since cεs, $c^{pn}=e$ for some integer n.

Now p^n and q are respectively prime.

We can find integers λ, μ show that $\lambda q+\mu p^n=1$

$C=c^{|}=c\ \lambda q+\mu p^n=c^{\lambda q}.c\ \mu p^n$

$=(c^q).(c^{pn})^{\mu}$

$=e^{\lambda}.e^{\mu}=e$

C=e this is a contradiction to the fact that c≠e. there is no prime number q/o(s) and q≠0 $o(s)=p^{\beta}$ for some β show that $0<\beta<\alpha$. by cauchys theorem o(S)/o(G). $\beta\leq\alpha$. Let us assume that $\beta<\alpha$. Let us consider the abelian group G/s
G is abelian G/S is also abelian.
Now o(G/s)=o(G)/o(S) s is a normal subgroup of an abelian group is normal. And $\beta<\alpha=p/o(G/S)$. there is an element $s_x(x\varepsilon G)$ is G/S, $s_x\neq S$ such that $(S_x)^{pn}=S$ from some integer n>0. But $S=(S_x)^{pn}=s_xp^n=x^{pn}\varepsilon s$. $e=(x^{pn})^{o(s)}=(x^{pn})^{p\beta}=x^{pn+\beta}$ xεs
$s_x=s$ which is a contradiction to the fact that $s_x\neq s$ $\beta<\alpha$ is impossible. the only possibility is

$\beta=\alpha$. $O(s)=p^{\alpha}$.

S is the required subgroup of order p^{α}.

Hence the theorem.

Automorphisms:

Definition:

An automorphism of a group is an isomorphism of an onto itself.

Lemma 3.7:

prove that A(G) is a group or if G is a group then A(G) the set of automorphisms of G is also a group.

Proof:

We know that A(G) is a collection of all one to one mappings of an onto itself and A(G) is also a group under the composition of mappings as binary operation.

We shall now show that A(G) is a subgroup of A(G).

Define i:G $\Longrightarrow$ G by xi=x¥xεG

Obviously I is the automorphism of G onto itself

iεA(G)

A(G) is a non empty subset of A(G) let T_1,T_2εA(G)

We know that T_1,T_2 is one to one and onto whenever both T_1,T_2 are one to one and onto

To show that T_1,T_2 is a homomorphism of G to itself

Let x, yεG

Then (xy) $T_1,T_2=((xy)T_1)T_2$

$=((xT_1)(yT_1))T_2$

$(xT_1)T_2(YT_1)T_2$ ¥x,yεG by definition T_1,T_2 is a homorphism of G to itself.

T_1,T_2εA(G) whenever T_1,T_2εA(G) next we prove that T^{-1}εA(G) whenever TεA(G) to show that T^{-1} is a homomorphism of G to itself

Now consider $(xT^{-1}yT^{-1})T=(xT^{-1})T(yT^{-1}T)$

$=x(T^{-1}T)y(T^{-1}T)$

=xiyi

=xy

Post multiplying on both sides by T^{-1} we get

$(xT^{-1}yT^{-1})TT^{-1}=(xy)T^{-1}$

$(xy)T^{-1}=xT^{-1}yT^{-1}$

T^{-1} is a homomorphism of G to itself

T^{-1}εA(G) whenever TεA(g) is a subgroup of A(G)

Hence A(G) is a group under the composition of mappings as binary operations.

Note:

A(G) is called the group of automorphism of G.

Definition:

Let G be the group for gεG

Define Tg:G $\Longrightarrow$G

By xTg=gxg $^{-1}$ ¥xεG then this mapping Tg is an automorphism of G. this automorphism of G is called an linear automorphism.

Remark:

An automorphism which is not inner is called as outer automorphism.

Lemma 3.8:

Let G be a group for gεG defined as Tg: G$\Longrightarrow$G by xTg=g $^{-1}$xg ¥xεG

Prove that Tg is an automorphism of G to itself.

Proof:

Let x, yεG then xyεG

Now (xy)Tg=g $^{-1}$(xy)g

=g $^{-1}$xgg^{-1}yg

=(g $^{-1}$xg)(g^{-1}yg)

xTg.yTg

Tg is a homomorphism.

For every yεG x=gyg^{-1}εG such that

xTg=g $^{-1}$xg

=g^{-1}gyg^{-1}g

=y

Tg is onto

We shall now prove that Tg is onto.

Now xTg=yTg

G $^{-1}$xg=g^{-1}yg

X=y

Tg is one to one.

Thus Tg is an isomorphism of G onto itself and hence Tg is an automorphism of G to itself.

Group of inner automorphism of G:

Define $\Phi(G)=\{T_g \varepsilon A(G)/g \varepsilon G\}$

We shall prove that $\Phi(G)$ is a subgroup of A(G).

Now $e \varepsilon G$

$.xT_e=e^{-1}xe=e^{-1}x=ex$

$=x$

$=xi¥\ x \varepsilon G$

$T_e=i \varepsilon \Phi(a)$

$\Phi(G)$ is a non empty subset of A(G)

Let $x \varepsilon G$

Let $T_g, T_h \varepsilon \Phi(a)$ where $g,h \varepsilon G$

Now consider,

$xT_g=(gh)^{-1}x(gh)$

$=h^{-1}g^{-1}xgh$

$=h^{-1}(g^{-1}xg)h$

$=(g^{-1}xg)T_h$

$=(xT_g)T_h$

$=xT_gT_h\ ¥\ x \varepsilon G$

$T_{gh}=T_gT_h$ whenever $T_g, T_h \varepsilon \Phi(G)$

Let $T_g \varepsilon \Phi(G)$

We have to show that $T_g^{-1} \varepsilon \Phi(G)$

To ,prove that $T_gT_g^{-1}=c$

We have $T_{gh}=T_gT_h$

$.xT_gT_h=xT_{gh}$

$xT_gT_g^{-1}=xT_{gg^{-1}}$

$=xT_e$

$=e^{-1}xe$

$=x$

$=xi$

$TgTg^{-1}=i\varepsilon\Phi(G)$

$(Tg)^{-1}=Tg^{-1}\varepsilon\Phi(G)$ since $g^{-1}\varepsilon G$.

$Tg^{-1}=Tg^{-1}\varepsilon\Phi(G)$ since $g^{-1}\varepsilon G$

$Tg^{-1}\varepsilon\Phi(G)$ whenever $Tg\varepsilon\Phi(G)$

Then by lemma $\Phi(G)$ is a subgroup of A(G).

$\Phi(G)$ is a group.

This group is called the group of inner automorphism of G.

Note:

$\Phi(G)\varsigma A(G)\varsigma$

Lemma 3.9:

If $g\approx G/z$where I(G) is the group of inner automorphism of G and z is the center of G.

Proof:

Define a map ψ: $G \Longrightarrow A(G)$

By $\psi(g)=Tg$ ¥ $g\varepsilon G$

Let $g, h\varepsilon G$ then $gh\varepsilon G$

Now $\psi(gh)=Tgh$

$=TgTh$

$=\psi(g)\psi(h)$

Ψ is a homomorphism of G into A(G) whose image is I(G).

We shall now prove that the kernel of ψ is z.

Suppose that k is the kernel of ψ then we prove that k=z

Let $k\varepsilon k$, then

$\Psi(k)$=identity element of A(G)

$Tk=i$

$xTk=xi$

$k^{-1}xk=x$

$xk=kx$

$k\varepsilon z$

$k\varsigma Z$

$z\varepsilon Z$ then by the definition of center of z we have $zx=xz$ ¥ $x\varepsilon G$

$x=z^{-1}xz$

$xi=xTz$

$i=Tz$

$i=\psi(Z)$

$z\varepsilon k$

$z=k$

ψ is a homomorphism of G into A(G) whose image is I(g) and kernel k=z then by theorem 2.7.1

$G/z\approx$the range of ψ is A(G)

$G/Z\approx I(G)$

$I(G)\approx G/Z$

Lemma 3.10:

Let G be a group and Φ an automorphism of G. if $a\varepsilon G$ is of order $o(a)>0$, then

$O(\Phi(a))=o(a)$.

Proof:

Let us suppose that $o(a)=n$

Then $a^n=e\longrightarrow 1$

Now consider $(\Phi(a))^n=\Phi(a).\Phi(a)……..\Phi(a)$

$=\Phi(a, a, a, ……..a)$

$=\Phi(a^n)$

$=\Phi(e)=e$ by lemma 2.7.2

If possible let $(\Phi(a))^m=e$ for $o<m<n$

Then $(\Phi(a))^m=e=\Phi(e)$

$\Phi(a^m)=\Phi(e)=a^m=e$

This is a contradiction since o(a)=n

Our assumption that $(\Phi(a))^m=e$ is false

$\Phi(a^n)=e$ for the least =ve integer n

$[\Phi(a)]^n=e$

$\Phi(a)$ has order n

$O(\Phi(a))=n=0(a)$. hence the lemma.

Cayley's theorem:

Every group is isomorphic to a subgroup of A(S) for some appropriate S.

Proof:

Let G be a group put s=G, then for gεG.

Define the mapping $\tau g:G \Longrightarrow G$

By $x\tau G=xg$ ¥ xεG

Let x, yεG

Then $x\tau g=xg$

$y\tau g=yg$

If $x\tau g= y\tau g$

Then xg=yg x=y τg is one to one.

If yεG then $y=yg^{-1}g$

$=(yg^{-1})g$

$=(yg^{-1})\tau g$

Now $yg^{-1}\varepsilon G$ yg^{-1} is the pre image of y in G under τg. Tg is onto.

Tg ε A(G) ¥ gεG

Now define the mapping $\psi:G \Longrightarrow A(G)$ by $\psi(g)=\tau g$ ¥gεG

Let us know prove that ψ is hpomomorphism.

Let a, bεG then for any xεG we have $x\tau ab=xab$ ¥ xεG

Now consider $x\tau a\tau b=(x\tau a)\tau b$

$=(xa)\tau b$

$=xab \quad ¥\ x\varepsilon G$

$x\tau a\tau b=x\tau ab$

$\tau a\tau b=\tau ab$

now consider $\psi(ab)=\tau ab$

$=\tau a\tau b$

$=\psi(a).\psi(b)$

Ψ is a homomorphism of G into A(G) suppose that k is the kernel of ψ. Let $k\varepsilon K$ then $\psi(k)=I$ by definition of kernel.

$\tau k=i$

$x\tau k=xi$

$xk=xe$

$k=e$

Ψ is one to one.

Ψ is isomorphism of G into A(G).

Also ψ is onto upto the range of ψ. We know that the range of a homomorphism is a subgroup of A(G).

Hence every group is isomorphic to a subgroup of A(S) for some appropriate S.

Theorem 3.3:

If G is a group H a subgroup of G and S is the set of all right cosets of H in G, then there is a homomorphism. Θ of G into A(S) and the kernel of Θ is the largest normal subgroup of G which is contained in H.

Proof:

Given that $s=\{Hg/g\varepsilon G\}$ we oberve that s need not be a group and still be a group only if H is a normal subgroup of G.

On s defines a mapping $tg:s \Longrightarrow S$

By $(Hx)tg=Hxg$, $g\varepsilon G$, $x\varepsilon G$

Let $x, y\varepsilon G$ then

(Hx)tg=(Hy)tg

Hxg=Hyg= Hx=Hy=x=y tg is one to one.

If HxεS for gεG then $Hx=Hxg^{-1}g$

$=(Hxg^{-1})g$

$=(Hxg^{-1})tg$

Hxg^{-1} is the preimage of Hx for any HxεS under tg

=tg is onto thus tgεA(S) for gεG

Then define a mapping Θ:G⟹ A(S)

By Θ(g)=tg ¥gεG

Let g, hεG then Hx tgth=(Hxtg)th

=(Hxg)th

=Hxgh

=Hxtgh

Tgh=tg th

Now consider Θ(gh)=tgh

=tgth

=Θ(g).Θ(H)

Then by definition Θ is a homomorphism of G into A(S).

Let k be the kernel of Θ then

K={xεG/Θ(x)=i}

={xεG/tc=i}

={xεG/Hgtx=Hg ¥gεG}

={ xεG/Hgx=Hg ¥gεG }

K is the kernel of Θ iff xεk

Hgx=Hg ¥gεG

We shall know prove that k is the largest normal subgroup of G contained in H. since k is the kernel of Θ by lemma 2.7.3 k is the normal subgroup of G. since is true for all gεG

We choose g=e

Hex=He Hx=H xεH

kçH

k is a normal subgroup of G contained in H. now we prove that k is the largest normal subgroup of G contained in H. if N is a normal subgroup of G such that NçH then we prove that Nçk let nεN then gng^{-1}εN ¥gεG and nεN

. gng^{-1}εH ¥gεG and nεN

$Hgng^{-1}$=H

Hgn=Hg

Nçk

K is the largest normal subgroup of G contained in H. hence the proof.

Remarks:

The above theorem can be applied to decide whether the group is simple as follows.

Suppose the homomorphism Θ is not an isomorphism then k≠{e} k is a non trivial subgroup contained in H. G is simple.

Lemma 3.11:

If G is a finite group and H≠G is a subgroup of G such that o(G)*i(H) then H must contain a non trivial normal subgroup of G. in particular G cannot be simple.

Since o(A)*i(H)! there are 2 possibilities

o(G)> i(H)!

o(G)< i(H)!

suppose that o(G)> i(H)! by theorem , Θ:G ⟹A(S) is a homomorphism where s is the collection of all right cosets of H in G.

.. o(A(s))=i(H)

=o(G)/o(H)

O(A(S))=i(H)!

We also know that the kernel k is the largest normal subgroup of G contained in H. in this case Θ cannot be an isomorphism as seen below. If Θ were an isomorphism between G and A(S) then Θ(G) would have o(G) elements and yet would be a subgroup of A(S)

. o(A(S))≥o(G)

. i(H)!≥o(G) which is contradiction. Θ is not an isomorphism but a homomorphism then by the corollary under lemma 2.7.4 k≠e hence this homomorphism ensures the existence of a non trivial normal subgroup K in H and hence is in G. G is not simple.

Let us know that o(G)<i(H)!

Given that o(G)*i(H)=o(A(S))

By lagranges theorem A(S) can have no subgroup of order o(G). there is no subgroup isomorphism to G. however A(S) contains Θ(G).

Θ(G) cannot be isomorphism in G. Θ cannot be an isomorphism. H must contain a non trivial normal subgroup of G. in this case also G is not simple.

Hence the lemma

Permutation groups:

We know that every group can be represented isomorphically as a subgroup of A(S) for some set S and in particular a finite group G can be represented as a sungroup of S_n, for some n where S_n is the symmetric group of degree n.

Suppose that S is a finite set having four elements x_1, x_2, x_3, x_4 if $\Phi \varepsilon A(S)=S_4$ then Φ is a one to one mapping of s onto itself.

For example if $\Phi: x_1 \longrightarrow x_2$

$x_2 \longrightarrow x_4$

$x_3 \longrightarrow x_1$

$x_4 \longrightarrow x_3$ this mapping can be represented as $\begin{pmatrix} x1 & x2 & x3 & x4 \\ x2 & x4 & x1 & x3 \end{pmatrix}$ we can represent this permutation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

if Φ is a permutation is represented by $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and ψ is a permutation can be represented by $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ then the permutation Φψ is given by

$\begin{pmatrix} & & & \end{pmatrix}$ $\begin{pmatrix} & & & \end{pmatrix}$ $\begin{pmatrix} & & & \end{pmatrix}$

$\Phi\psi = \begin{matrix}1&2&3&4\\2&4&1&3\end{matrix} \quad \begin{matrix}1&2&3&4\\1&3&2&4\end{matrix} = \begin{matrix}1&2&3&4\\2&1&3&4\end{matrix}$

Let S be a set and $\Theta \varepsilon A(S)$

Given two elements a,bεs we define $a \equiv \Theta^b$ iff $b = a\Theta^i$ for some integer I, where I can be positive, negative, zero. We claim this defines an equivalence relation since $a \equiv \Theta^{\Theta}$¥aεs then we have $a \equiv \Theta^a$ relaxitivity is true. Now assume that $a \equiv \Theta^b$ then by definition $b = a\Theta^i$ where I is some integer from this we have $a = b\Theta^{-I}$ where –I is a negative integer.

$b \equiv \Theta^a$ symmetry is true. Now we assume that $a \equiv \Theta^b$ and $b \equiv \Theta^c$ then by definition $b = a\Theta^i$

$c = a\Theta^j$ where I and j are some integers now $c = b\Theta^j$

$= a\Theta^i\Theta^j$

$= a\Theta^{i+j}$

$a \equiv \Theta^c$ transitivity is true. The relation defined above is an equivalance relation on s. hence by theorem 1.1.1 this equivalance relation ≡ indices a decomposition of s into disjoint subsets, namely the equivalance classes. The equivalance classes of an element sεS is called the orbit of s under Θ.

Orbit of $s = \{s\Theta^i / i = 0, \pm 1, \pm 2, \ldots\ldots\}$

When s is finite, Θ is called as permutation and corresponding orbits are called ccles. In this case F a smallest +ve integer and depending on s such that $s\Theta^i = s$

By a cycle of Θ we mean an ordered set $\{s, s\Theta, s\Theta^2, \ldots\ldots s\Theta^{l-1}\}$, l is called the length of the cycle.

Definition:

A cycle with 2 elements is called as 2-cycles.

Definition:

A transposition is defined to be a permutation with effects only two elements.

Example:

In the cycle (1 3 4) we associate the permutation (1 3 4)= $\begin{pmatrix}1&2&3&4&5\\3&2&4&1&5\end{pmatrix}$

The permutation under the cycle has the same effect on the elements of the cycle but the permutation leaves other elements fixed.

The permutation corresponding to a cycle (2 5) is a permutation (2 5)= $\begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix}$

Lemma 3.12:

Every permutation is the product of its cycles or every permutation can be uniquely expressed as a product of disjoint cycles.

Proof:

Let S be a finite set. Let Θ be the permutation. Let ψ be the product of the disjoint cycles of Θ. The cycles of Θ are of the form $(s, s\Theta, s\Theta^2, \ldots\ldots s\Theta^{l-1})$.

By the multiplication of cycles and since the cycles of Θ are disjoint. The image of $s^{|}$εs under Θ namely $s^{|}\Theta$ is the same as the image of $s^{|}$ under ψ.

Θ and ψ have the same effect on every element of s. hence Θ=ψ.

Every permutation is the product of its cycles.

Lemma 3.13:

Every permutation is a product of 2cycles(transposition).

Proof:

Consider 'm' cycle (1, 2, 3…..m)

A single permutation show that

(1, 2, 3….m)=(1,2)(1,3)…(1,m)

More generally the m-cycles

$(a_1, a_2 \ldots\ldots a_m)=(a_1, a_2)(a_1 a_3)\ldots.(a_1 a_m)$

This decomposition is not unique.

By this we mean an m-cycle can be written as a product of two cycles is more than one way

For example,

(1 2 3)=(1 2)(13)

=(3 1)(3 2)

Now since every permutation is a product of disjoint cycles and every cycle is a product of two cycles, we have every permutation is a product of 2 cycles.

Remarks:

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

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

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

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

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

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

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

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

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

$(3\ 1)(3\ 2)$

Definitions:

1. A permutation $\Theta \varepsilon S_n$ is called an even permutation if it can be represented as a product of even no of transpositions.
2. A permutation is called an odd permutation if it is not an even permutation

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. If f is a homomorphism of a group G into G', then prove that
   i) f(e) = e', where e is the identity of G and e' is the identity of G'
   ii) $f(a^{-1}) = [f(a)]^{-1}$, $\forall a \in G$

2. State and prove fundamental theorem on homomorphism of groups.

3. State and prove Cayley's theorem.

4. State and prove Cauchy's theorem for abelian groups.

5. State and prove Sylow's theorem for abelian groups.

6. Suppose G is a group and N is a normal subgroup of G. Let f be a mapping from G to G/N defined by f(x)= Nx, $\forall$ x$\in$G. Then f is a homomorphism of G onto G/N and kernel f =N.

7. Show that $a \rightarrow a^{-1}$ is an automorphism of a group G iff G is abelian.

8. If φ is a homomorphism of G into $\bar{G}$ with kernel K, then prove that K is a normal subgroup of G.

9. The set I(G) of all inner automorphisms of a group G is a normal subgroup of the group of its automorphisms isomorphic to the quotient group G/Z of G where Z is the centre of G.

10. Define a permutation. If A= $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and B =$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ then find AB and BA.

UNIT-IV

SYLLABUS

External direct product of a finite number of groups, normal subgroups, factor groups, Cauchy's theorem for finite abelian groups

INTRODUCTION TO RING THEORY

In algebra, ring theory is the study of rings—algebraic structures in which addition and multiplication are defined and have similar properties to those operations defined for the integers. Ring theory studies the structure of rings, their representations, or, in different language, modules, special classes of rings (group rings, division rings, universal enveloping algebras), as well as an array of properties that proved to be of interest both within the theory itself and for its applications, such as homological properties and polynomial identities **.**

Definition

A non empty set R is said to be an associative ring if in R these are defined two operations denoted by '+' and '.' Called addition and multiplication respectively such that for all a,b,c ϵR

i. a +b ϵ R

ii. a +b=b+a

iii. a+(b+c)=(a+b)+c

iv. There is an element 0 in R such that a+0=0+a=a ∀ a ϵ R

v. There exist an element –a in R such that a+(-a)=0=(-a)+a

vi. a.b ϵ R

vii. (a.b).c=a.(b.c)

viii. (i) Left Distributive law:
a.(b+c)=a.b+a.c

(ii) Right distributive law:

(b=c).a=b.a=c.a

Definition

A nonempty set R is called a ring, if it has two binary operations called addition denoted by a + b and multiplication denoted by ab for a, b $\in$ R satisfying the following axioms:
Multiplication is associative, i.e. a(bc) = (ab)c for all a, b, c $\in$ R.

Distributive laws hold: a(b + c) = ab + ac and (b + c)a = ba + ca for all a, b, c $\in$ R.

Definition

. Let R be a ring.

(1) If multiplication in R is commutative, it is called a commutative ring.

(2) If there is an identity for multiplication, then R is said to have identity.

(3) A nonzero element a ∈ R is said to have a left (resp. right) inverse b if ba = 1 (resp. ab = 1) We say that a is invertible or a unit in R if it has a left and a right inverse.

(4)A commutative division ring is called a field.

(5)An element a of a commutative ring R is called a zerodivisor if there is a nonzero b ∈ R such that ab = 0. An element a ∈ R that is not a zerodivisor is called a nonzerodivisor. If all nonzero elements of a commutative ring are nonzerodivisors, then R is called an integral domain.

(6) A nonempty subset S of a ring R is called a subring of R if S is a ring with respect to addition and multiplication in R.

Example of rings

The set of integers Z, the set of rational numbers Q, the set of real numbers R and the set of complex numbers C are commutative rings with identity.

NOTE

i. In this case we also say that (R,+,.) is a ring
ii. 0 is called the zero element of the ring and it is the additive identity element
iii. If there is an element 1 in R such that a.1=1.a=a ∀ a ϵ R then R is called a ring with unit element.
iv. If for all a,b ϵ R a.b=b.a then R is called a commutative ring

Some Special Classes Of Rings

Definition

If R is a commutative ring then a≠0 ϵ R is said to be a zero-devisor if there exist a,b ϵ R,b≠ 0 such that ab=0

[Eg : define (a1,b1,c1) (a2,b2,c2)=(a1a2,b1b2,c1c2)

(1,2,0) (0,0,7)=(0,0,0)]

Examples

1.Some M is a ring of 2*2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring composition then M is a ring with zero-devisors

2.The ring of integer is a ring without zero-devisors

Definition

A commutative ring is an integral domain if it has no zero devisors

Example : The ring of integers

Definition

A ring is said to be a division ring if its non-zero element form a group under multiplication

Remark

Sometimes a division ring is called a skew field.

Definition

A field is a commutative division ring

Lemma 4.1

If R is ring, then for all a,b ϵ R

1. a.0 = 0.a = 0
2. a(-b)=(-a)b=-(ab)
3. (-a)(-b)=ab

If in addition,R has a unit element 1 then

4. (-1) a =-a
5. (-1)(-1)=1

1) Let a ϵ R then consider

a.0 = a.(0+0)

=a.0+a.0 (L.D.L)

(i.e) a.0=0 = A. + A.0

=> 0 = a.0 (by L.C.L)

Since R is a group under addition we have

a.0 = 0

Similarly we can prove 0.a = 0

Thus we have a.0 = 0.a = 0

2) We shall first show that a(-b) = -(ab)

(i.e) To P.T a(-b) + ab = 0

Now consider, a(-b) + ab = a(-b + b)

=a(0)

= 0 by 1

(i.e) a(-b) + ab = 0

(i.e) a(-b) = -ab

Similarly we can P.T (-a)b = -ab

⇨ a (-b) = (-a)b = -ab

3)Now consider (-a)(-b)

(-a) (-b) = -(a(-b)) by 2

= -(-ab)

=ab

4)Given that R has a unit element 1

By definition 1.a = a.1 = a ∀ a ϵ R

Now consider (-10a = a = (-a) a + 1.a

= (-1 + 1) a

= 0.a = 0

⇨ (-1) a = -a

5)In a proof of fourth result we have,

(-1) a = -a ∀ a ϵ R

If we take a = -1 then we have (-1)(-1) = -(-1)

(-1) (-1) = 1

The Pigeon Hole Principle

Definition

If n objects are distributed over m places and if n > m then some places receives at least two objects.

Equivalently, if n objects are distributed over n places in such a way that no place receive more than one object, then each place receives exactly one object.

Lemma: 4.2

A finite integral domain is a field.

Proof

An integral domain is a commutative ring such that ab=0 if atleast one of a or b is 0.

A field is a commutative ring with unit element in which every non zero element has a multiplicative inverse in the ring.

Let D be the finite integral domain with n elements

In order to show that D is a field we have to P.T

I. There exist an element $1 \in D$ such that

$a.1 = 1.a = a \ \forall \ a \in D$

II. For every element $a \neq 0 \in D \ \exists \ a \ b \in D$ show that ab=1

Let $x_1, x_2 \ldots x_n$ be the n elements of D

Let $a \neq 0 \in D$

Consider the elements,

$x_1a, x_2a, \ldots x_na$ they are in D

we claim that they are all distinct

if possible let us assume that

$x_ia = x_ja$ for $i \neq j$

then $x_ia - x_ja = 0$

$(x_i - x_j)a = 0$ (R.D.L)

Since D is an integral domain and $a \neq 0$ (by assumption)

We have $x_i - x_j = 0 \Rightarrow x_i - x_j$

This is contradiction since $i \neq j$

Our assumption that xia = xja is false

$xia \neq xja$ for $i \neq j$

x1a,x2a…xna are distinct and these n-distinct elements lie in D.

therefore by the pigeon hole principle these elements are the elements of D

if $Y \in D$ then y=xia for some xi

in particular since $a \in D$ we must have

a=x a for some $xi0 \in D$

since D is commutative we have

a = xi0 a=axi0

we shall P.T xi0 is a unit element for every element of D

now yxi0 = (xi a)xi0

=xi(axi0)

=xi.a

=y

Xi0 is the unit element of D and we write it as 1

xi0=1

Now $1 \in D$ .. a.1 = a ∀ $a \in D$

1 must be of the form xia for some $xi \in D$

1 = xia

~~7~~ a,b ϵ b such that 1 = ba

Ab = ba = 1 => Innverse exist

Thus we proved two conditions

Hence every finite integral domain is a field

Corollary:

If p is a prime no then jp, the ring of integers mod p is a field.

Proof:

Jp has a finite no of elements $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{(p-1)}$ where $\overline{i}$, is the class of integers which give remainder i on division by p.

Then by the above lemma it is enough to prove that jp is an integral domain but we know that jp is a commutative ring. Let a,b ϵ jp and ab = 0 then p must divide a or b

Either a = 0 mod p or b = 0 mod p

(i.e) a = 0 or b = 0

Jp has no zero divisor

By definition jp is a finite integral domain

Hence by the above lemma, jp is a field

NOTE

Let f be an finite field having m elements like jp, by corollary (ii) of lagranges theorem we have $a^{0(f)} = e$

Under addition we have

a + a +…= 0

m terms

(i.e) ma = 0

Definition

An integral domain D is said to be of characteristic '0' in the relation ma = 0 where $a \neq 0$ is in D and where m is an integer can hold only if m = 0

Example

i. The ring of integers
ii. The ring of even integers
iii. The ring of rationals

Definition

An integral domain D is said to be of finite characteristic if ~~∄~~ a +ve integer 'm' such that ma = 0 for all $a \in D$

NOTE

1. If D is of finite characteristic then we define the characteristic of D to be the smallest the integer p, S.T pa = 0 ~~∀~~ $a \in D$
2. If D is of finite characteristic then its characteristics is a prime number
3. An integral domain which has an finite characteristics

Definition

An element 'a' of a ring R is said to be Idompotent if $a^2 = a$

A ring R is called a Boolean ring if all elements are idempotent

Homomorphisms

Definition

A mapping from ring R into the ring R is said to be a homomorphism if

i. $\Phi(a + b) = \Phi(a) + \Phi(b)$
ii. $\Phi(ab) = \Phi(a) . \Phi (b)$ ~~∀~~ $a,b \in R$

Lemma 4.3

If Φ is a homo morphism of R into R then

i. $\Phi (0) = 0$
ii. $\Phi (-a) = - \Phi(a)$ for every $a \in R$

Proof

i. Let $a \in R$ then $\Phi(a) \in R$ now $\Phi(a) + 0 = \Phi(a)$

(i.e) $\Phi(a) + 0 = \Phi(a + 0)$

(i.e) $\Phi(a) + 0 = \Phi(a) + \Phi(0)$

$\Rightarrow \Phi(0) = 0$ by L.C.L

ii. From (i) we have $\Phi(0) = 0$

(i.e) $0 = \Phi(o)$

$= \Phi(a + -a)$

$= \Phi(a) + \Phi(-a)$

$\Rightarrow \Phi(-a) = - \Phi(a)$

Hence the proof

NOTE

If both R and R' have the respective unit element as 1 and 1' for their multiplication, it need not follow that $\Phi(1)=1'$

However if R' is a integral domain (or) R' is arbitrary but Φ is onto then $\Phi(1) = 1'$

Definition

If Φ is a homomorphism of R onto R' then the kernel of Φ, denoted by $I(\Phi)$ is the set of all elements $a \in R$ such that $\Phi 9a)=0$ where 0 is the zero element of R'.

(i.e) $I(\Phi) =\{ a \in R / \Phi(a)=0$,the zero element of R'$\}$

Lemma : 4.4

If Φ is a homomorphism of R into R' with kernel $I(\Phi)$,then

1. I(Φ) is a subgroup of R under addition
2. If a ϵ I(Φ) and r ϵ R then both ar and ra are in I(Φ)

Proof

1. We know that Φ(0) = 0 by lemma3.3.3

   0 ϵ I(Φ)

   I(Φ) is a non-empty subset of R

   Let a,b ϵ I(Φ)

   Φ(a) = 0 and Φ(b) = 0

   Since Φ is a homomorphism we have,

   Φ(a+b) = Φ(a) + v9b)

   = 0 + 0

   =0

⇨ a+b ϵ I(Φ)

let a ϵ I(Φ)

Φ(a) = 0

But we know Φ(-a) = - Φ(a)

=0

-a ϵ I(Φ) whenever a ϵ I(Φ) then by a lemma I(Φ) is a subgroup of R under addition.

Since a ϵ I(Φ) by definition Φ(a)=0

Now consider Φ(ar)

Φ(ar)= Φ(a). Φ(r)

=0

⇨ $ar \in I(\Phi)$

similarly $\Phi(ra) = \Phi(r).\Phi(a)$

$= \Phi(r).0$

$=0$

⇨ $ra \in I(\Phi)$

Hence if $a \in I(\Phi)$ and $r \in R$, then both ar and ra are in $I(\Phi)$

Definition

1. A homomorphism of R into r' is said to be an isomorphism if it is a one to one mapping.
2. Two rings are said to be isomorphic if ther is an isomorphism of one onto the other

Lemma:4.5

The homomorphism Φ of R in R' is an isomorphism iff $I(v) = \{0\}$

Proof

Let us assume that Φ is an isomorphism of R into R'. then by definition Φ is one to one.

Let $a \in I(\Phi)$

$\Phi(a) = 0$ where 0 is the identity element of R'

$\Phi(a) = \Phi(0)$ $[\Phi(0)=0]$

⇨ $a = 0$ [ϕ is one to one]

Conversely,

Assume that $I(\Phi)=\{0\}$

It is enough to prove that Φ is one to one.

Let $x,y \in R$

Then $\Phi(x), \Phi(y) \in R'$

Now $\Phi(x) - \Phi(y) = \Phi(x) + \Phi(-y)$

$= \Phi(x - y)$

If $\Phi(x) = \Phi(y)$ then

$\Phi(x) - \Phi(y) = 0$

Thus $\Phi(x - y) = 0$

- ⇨ $x - y \in I(\Phi) = \{0\}$
- ⇨ $x - y = 0$
- ⇨ $x = y$
- ⇨ Φ is one to one

Hence the homomorphism Φ of R into R' is an isomorphism iff $I\{\Phi\} = 0$.

Theorem:
The intersection of any two left ideals of a ring is again a left ideal of the ring.

Proof:

Let I_1 and I_2 be two left ideals of a ring R. Then I_1 and I_2 are subgroups of R under addition.

Therefore $I_1 \cap I_2$ is also a subgroups of R under addition.

Now to show that $I_1 \cap I_2$ is a left ideal of R, we are only to show that $r \in R, s \in I_1 \cap I_2 \Rightarrow rs \in I_1 \cap I_2$

We have $s \in I_1 \cap I_2 \Rightarrow s \in I_1$ and $s \in I_2$

But I_1 and I_2 are left idals of 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 $rs \in I$ and $rs \in I_2 \Rightarrow rs \in I_1 \cap I_2$.

Therfore $I_1 \cap I_2$ is also a left ideal of R.

Theorem:
Fundamental theorem on homomorphism of rings.

Every homomorphic image of a ring R is isomorphic to some residue class ring thereof.

Proof:

Let R' be the homomorphic image of a ring R and f be the corresponding homomorphism.

Then f is a homomorphism of R onto R'. Let S be the kernel of this homomorphism.

Then S is an idealof R. Therefore R/S is a ring of residue classes of R relative to S.

We shall prove that R/S≅R'.

If a∈R, then S+a∈R/S and f(a) ∈R'.

Consider the mapping ϕ:R/S→R' such that ϕ(S+a) = f(a) $\forall\ a \in R.$

To prove: ϕ is well defined

If a.b ∈R and S+a = S+b then ϕ(S+a) = ϕ(S+b)

We have S+a = S+b

⇒ a-b∈S

⇒f(a-b) =0'

⇒f[a+(-b)] = 0'

⇒f(a) + f(-b) = 0'

⇒f(a) =f(b)

⇒ϕ(S+a)= ϕ(S+b)

⇒ ϕ is well defined.

To Prove : ϕ is 1-1

We have ϕ(S+a) = ϕ(S+b)

⇒f(a) =f(b)

⇒f(a) -f(b) = 0'

⇒f(a) + f(-b) = 0'

⇒f(a-b) = 0'

⇒ a-b∈S

⇒ S+a = S+b

Therefore ϕ is 1-1.

To Prove : ϕ is onto

Let y be any element of R'. Then y=f(a) for some a∈R because f is onto R'.

Now S+a∈R/S and we have ϕ(S+a) = f(a) = y.

Therefore ϕ is onto R'.

Finally we have $\phi[(S+a) + (S+b)]= \phi[(S+(a+b)] = f(a+b)$

$= f(a)+f(b) = \phi(S+a) +\phi(S+b)$

$\phi[(S+a) (S+b)]= \phi[(S+(ab)] = f(ab) = f(a)f(b) = [\phi(S+a)][\phi(S+b)]$

Therefore ϕ is an isomorphism of R/s onto R'.

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. If R is a ring, then foe all a,b $\in$ R,

   (i) a0 = 0a = 0.

   (ii) a(-b) = (-a)b = -(ab)

   (iii) (-a)(-b) = ab.

   (iv) a(b-c) = ab - ac

2. i) Define Integral domain with example.

   ii) Prove that every finite integral domain is a field.

3. Prove that every field is an integral domain.

4. i) Define field with example.

   ii) Prove that a skew field has no divisors of zero.

5. Show that the set of numbers of the form $a+b\sqrt{2}$, with a and b as rational numbers is a field.

6. Prove that a ring R has zero divisors iff cancellation law is valid in R.

7. Prove that a finite commutative ring R without zero divisors is a field.

8. Let R and R' be a rings and $f:R\rightarrow R'$ be an isomorphism. Then prove that
   i) R is commutative $\Rightarrow$ R' is commutative
   ii) R is ring with identity $\Rightarrow$ R' is ring with identity
   iii) R is an integral domain$\Rightarrow$ R' is an integral domain
   iv) R is a field$\Rightarrow$ R' is a field

9. Prove that the homomorphism ϕ of a ring into a ring R' is an isomorphism of R into R' iff $I(\phi) = (0)$, where $I(\phi)$ denotes the kernel of ϕ.

10. State and Prove fundamental theorem on homomorphism of rings.

UNIT-V

SYLLABUS

Abelian groups, finitely generated abelian group, divisible and reduced groups, Torsion group,

INTRODUCTION TO IDEALS AND QUOTIENT RINGS

In ring theory, an **ideal** is a special subset of a ring. Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any other integer results in another even number; these closure and absorption properties are the defining properties of an ideal.Among the integers, the ideals correspond one-for-one with the non-negative integers: in this ring, every ideal is a principal ideal consisting of the multiples of a single non-negative number. However, in other rings, the ideals may be distinct from the ring elements, and certain properties of integers, when generalized to rings, attach more naturally to the ideals than to the elements of the ring. For instance, the prime ideals of a ring are analogous to prime numbers, and the Chinese remainder theorem can be generalized to ideals. There is a version of unique prime factorization for the ideals of a Dedekind domain (a type of ring important in number theory). An ideal can be used to construct a quotient ring similarly to the way that modular arithmetic can be defined from integer arithmetic, and also similarly to the way that, in group theory, a normal subgroup can be used to construct a quotient group.

IDEALS AND QUOTIENT RINGS

Definition

If R is any ring then a subset L of R is called a left Ideal of R, if

i. L is a subgroup of R under addition
ii. $r \in R, a \in L \Rightarrow ra \in L$

In a similar way we can define a right ideal

Definition

A non empty subset u of R is said to be a (two sided) ideal of R if

i. u is a subgroup of R under addition

ii. For every u ϵU and r ϵ R, both ur and ru ϵ U

NOTE

i. An ideal is thus simultaneously a left ideal and right ideal of R

ii. Since the ring R is an abelian group w.r.to addition it follows that any ideal U is normal subgroup of r (since any subgroup of an abelian group is normal)

iii. If u is an ideal of the ring R then $\frac{R}{U}$ is a ring and is homomorphic of R

Lemma:5.1

If U is an ideal of R, U is a normal subgroup of R (by note (i))

w.r.to addition $\frac{R}{U}$ is the set of all distinct cosets of U in R, mearly we say that coset and we donot say left coset or right coset. Since R is an abelian group w.r.to addition,

a + U = U + a

$\frac{R}{U}$ consists of all cosets a+u,a ϵ R

From a theorem 2.6.1 we know that $\frac{R}{U}$ is a group under addition (prove here), where the composition law is (a + u) + (b+ u) = (a + b) + U ∀ a,b ϵ R

$\frac{R}{U}$ is also abelian since R is abelian w.r.t.addition. let us define the multiplication in $\frac{R}{U}$ as follows

(a + u) + (b + u) = ab + u ∀ a,b ϵ R

Now we prove, the above said multiplication is well defined

If a + u = a' + u

And b +u = b' + u

Then by our definition of multiplication ,we have to prove that

(a + u) (b + u) =(a' + u) (b' + u)

(i.e) to prove that (ab + u) = (a'b' + u)

Since a + u =a' + 0

We have

A= a' + u1 where u1 ϵ u

Similarly since b + u =b' + u

We have b= b'+u2 where u2 ϵ u

ab= (a' + u1) (b' + u2)

=a'b' + a'u2 +b'u1 + u1u2

Since u is an ideal of R we have

a'u2 + b'u1 and u1u2 ϵ u

a'u2 + b'u1 + u1u2 ϵ U

ab=a'b' + u3 where u3=a'u2 + b'u1 + u1u2 ϵ u

ab + u =a'b' + u3 = u

=a'b' + u

⇨ ab+u =a'b' = u

The multiplication defined above is well defined now (a + u) (b + u) =ab+u ϵ $\frac{R}{U}$

As a,b ϵ R by closure property ab ϵ u

$\frac{R}{U}$ is closed with respect is multiplication

Since R is associative w.r.to multiplication,

$\frac{R}{U}$ is also associative w. r. to multiplication

Let x,y,z ϵ $\frac{R}{U}$

Then x = a + u

y=b + u

z=c + u where a,b,c ϵ R

now we P.T x(y + z) =xy + xz

L.H.S = x(y + z)

=(a + u) (b + u + c + u)

=(a + u) [(b + c) + u]

=(a(b + c) + u)

=ab + ac + u

=(ab + u) + (ac + u)

=(a + u) (b + u) + (a + u) 9c + u)

=xy + yz

=R.H.S

Similarly we prove that (y + z) x =yx + zy

If R is commutative then $\frac{R}{U}$ is also commutative as seen below,

Consider (a + u) (b + u) = ab + u

=ba + u (R is commutative ab=ba)

=(b + u) (a + u)

$\frac{R}{U}$ is also commutative, if R is commutative

If R has an unit element 1, then $\frac{R}{U}$ has unit element 1 + u

Define a mapping ϕ:R -> $\frac{R}{U}$

By ϕ(a) = a = u for a ϵ R

Let a,b ϵ R

Then ϕ (a + b) = (a + b) + U

=(a + u) + (b + u)

= ϕ (a) + ϕ((b)

And ϕ (ab) = ab + u

=(a + u) (b + u)

Φ (a). ϕ (b)

⇨ by def ϕ is a homomorphism

let y ϵ $\frac{R}{U}$ then y= a + u for a ϵ R and ϕ (a) = a + u = Y

a is the pre image of Y in $\frac{R}{U}$

ϕ is onto

If u ϵ U then ϕ(u) = u + U = u whih is the identity element of $\frac{R}{U}$

The kernel of ϕ is exactly U

Hence the lemma

Remark :

The ring $\frac{R}{U}$ is known as quotient Ring

Theorem 5.1

let R, R' be ring and ϕ a homomorphism of R onto R' with kernel U. then R' is isomorphic

To $\frac{R}{U}$

Moreover there is a one to one correspondence between the set of ideals of R' and the set of ideals of R which contain U. this correspondence can be achieved by associating with an idel W' in R', the ideal W in R defined by

W = { x ϵ R / ϕ (x) ϵ W so defined $\frac{R}{W}$ -> R' by

Ψ (u + a) = ϕ (a) -------- 1

Where u + a is an arbitrary element of $\frac{R}{U}$ and a ϵ R

Let us prove that the mapping is well defined (i.e) to show that U + a = U + b

⇨ ψ(u + a) = ψ(u + b) ∀ u + a, U +b ϵ $\frac{R}{U}$ where a,b ϵ R

let us prove that the mapping is well defined

(i.e) to show that U + a = U + b

=> ψ (u + a) = ψ(U + b) ∀ u +a, U +b ϵ $\frac{R}{U}$ where a,b ϵ R

Now assume that u + a = u + b

Since a =0 = a ϵ u + a ……(o ϵ u)

a ϵ u + a = u +b by an assumption

a = u + b for some u ϵ U

now ψ (u + a) =ϕ(a)

= ϕ(u + b)

=Φ(u) + ϕ(b)

= 0' + ϕ(b)

=ψ (u + b) by 1

ψ is well defined

ψ[(u + a) = (u + b)] = ψ (u + (a+b))

= ϕ(a + b)

=Φ(a) + ϕ(b)

=ψ (u + a) + ψ (u + b)

ψ[(u + a) = (u + b)] = ψ (u + ab)

$= \phi(ab)$

$=\Phi(a) . \phi(b)$

$=\psi (u + a)\ \psi (u + b)$

Ψ is a homomorphism

Given that ϕ is onto'.

For every r' ϵ R' $\exists$ ar ϵ R such that $\phi(r) = r'$

$\Psi(u + r) = r'$

U + r is thepre image of r' under ψ

Ψ is onto

Let us now show that ψ is one to one

Now we prove the result by proving that the kernel of ψ namely U_ψ consist of only one element U which is the identity element of $\frac{R}{U}$

By definition of kernel we have,

U_ψ= { U +a ϵ $\frac{R}{U}$ / $\psi(u + a)^{=0'}$ the zero element of R'}

={ u + a $\epsilon \frac{R}{U}$ / $\phi(a)^{=0'}$} by 1

={u} since $\phi(a) =0'$

⇨ a ϵ u

⇨ u + a =U

ψ is one to one

$\psi : \frac{R}{U}$ -> R' is an onto isomorphism

$\frac{R}{U} \sim$ R'

(i.e) R' ~ $\frac{R}{U}$ (isomorphism is an equivalence relation)

(ii) Given that W = { x ϵ R / ϕ(x) W'} and W' is an ideal of R'

To prove

U C W and W is an ideal of R

Let x ϵ U

Φ(x) = 0' ϵ W'

⇨ x ϵ W

x ϵ U => x ϵ W

U C W

Now ϕ(0) = 0' ϵ W' (W' is an ideal of R')

Φ(0) ϵ W'

0 ϵ W… W is an non empty subset of R

Let x,y ϵ W,

Φ(x) ϵ W', Φ(y) ϵ W'

Φ(x + y) = Φ(x) + Φ(y) ϵ W' (W' is closed under addition)

⇨ x + y ϵ W whenever x,y ϵ W

let x ϵ W

Φ(x) ϵ w'

Now Φ(-x) = - Φ(x) ϵ W'

Φ(-x) ϵ W'

⇨ -x ϵ W' whenever x ϵ W

Then by a lemma W is a subgroup of R under addition

Next we prove that W is an ideal of R let r ϵ R and x ϵ W

Φ(r) ϵ R' and Φ(x) ϵ W' …. x ϵ R

Xr and rx ϵ R (R is closed under multiplication)

Φ(xr) = Φ(x). Φ(r) ϵ W' (W' is an ideal of R')

xr ϵ W

similarly we can prove that

rx ϵ W ∀r ϵ W , x ϵ W

W is an ideal of R containing U

(i.e) inverse image of an ideal W' of R' is also an ideal W of R containing U

Conversely assume that w is an ideal of R and we prove that w' is an ideal of R'

Define W'={ x' ϵ R'/ x'=ϕ(y), y ϵW}

Now 0 ϵ W ϕ(0) =0' ϵ w'

W' is a non empty subset of R'

Let x1',x2' ϵ w'

x1'= $\phi(y_1)$

x2'= $\phi(y_2)$

$y_1, y_2 \epsilon$ W

x1' + x2'= $\phi(y_1)+ \phi$(y2)

= $\phi(y_1+y_2)$

ϵ w' since $y_1+y_2 \epsilon$ w

thus $x_1' + x_2' \epsilon$ w'

then x'= ϕ(y), y ϵ w

- y ϵ w

-x'= - ϕ(y)

= ϕ(-y) ϵ w' …..(- y ϵ w)

-x' ϵ w' whenever x' ϵ w'

Then by lemma w' is a subgroup of R' under addition

Let x' ϵ w, r' ϵ R'

Let r ϵ R, ϕ(r)=r'

X'= ϕ(y), y ϵ w

ϕ(yr)= ϕ(y). ϕ(x)

=x'r'

yr ϵ w as w is an ideal of R

ϕ(yr) ϵ w'

x'r' ϵ w'

Similarly we can prove that r'x' ϵ w'

w' is an ideal of R'

next we prove that the ideal w of R is unique

let T be another ideal of R

T= { y ϵ R/ ϕ(y) ϵ w'}

We have to prove that W= T

Let y ϵ w

ϕ(y) ϵ w' (by def of W)

y ϵ T (by def of T)

W C T

Let t ϵ T

ϕ(t) ϵ w'

t ϵ w

T C W

⇨ W = T

Thus W is unique

Thus there is a one to one correspondence between the ideals of R' and the ideals of R containing U

(iii) Now we define a mapping F : R -> $\frac{R'}{W'}$

By F(a) =W' +ϕ(a), a ϵ R

Since ϕ is onto,for every a' ϵ R' ∄ an element a ϵ R s.t ϕ(a) = a'

Now W' + ϕ(a) = W' + a'

= F9a)

A is the pre image of w' + ϕ(a)

F is onto

Let x,y ϵ R

F(x + y) = W' + ϕ(x + y)

=W' + ϕ(x)+ ϕ(y)

==W' + ϕ(x)W'+ ϕ(y)

=F(x) + F (y) ∀ x,y ϵ R

We shall show that the kernel of F namely K_F is W

Assume that L is the kernel of F and we prove that W = L

Now by def L = { x ϵ R / F(x) = w'}

Let $x \in L$ … $F(x) = w'$

$w' + \phi(x) = w'$

$\phi(x) \in w'$

$x \in w$

$L \subset W$

Let $x \in W$ … $\phi(x) \in w'$

$w' + \phi(x) = w'$

$F(x) = w'$

$x \in L$

$W \subset L$

Hence $w = L$

The kernel of F is W and is unique

F is a homo of R onto $\frac{R'}{W'}$ with kernel W

Then by a theorem (2.7.1) $\frac{R}{W}$ is isomorphic to $\frac{R'}{W'}$

$\frac{R}{W} \sim \frac{R'}{W'}$

Lemma 5.2

Let R be a commutative ring with unit element whose only ideas are {0} and R itself ,then R is a field

Proof

In order to prove this result, it is enough if we prove that $\forall$ a $\neq 0 \in R$ $\exists$ a b $\neq 0 \in R$ s.t

ab = 1

Let a $\neq 0 \in R$

Consider the set Ra = { xa / x $\in$ R}

We claim that Ra is an ideal of R

Since 0 = 0.a $\in$ Ra

Ra is a non empty subset of R

Let u,v $\in$ Ra

Then u = x` a and v = x2a for some x1,x2 $\in$ R)

Now u – v = x1a –x2a

= (x1-x2)a

$\in$ …[x1-x2 $\in$ Ra]

Ra is a subgroup of R under addition

Let r $\in$ R let u = xa

Then consider ru = r(xa) = (rx) a $\in$ Ra (rx $\in$ R)

Similarly we can prove that ur $\in$ Ra

By deff Ra is an ideal of R

From the given hypothesis it follows that Ra = { 0} or Ra = R

(i.e) every multiply of R is a multiple of a by some element of R

There exist an element b $\neq 0$ s.T ab=1

R is a field

Definition

An ideal M ≠ R in a ring R is said to be a maximal ideal of R, if whenever u is an ideal of R such that M C U C R then either R = U or M = U

In otherwords, an ideal of R is a maximal ideal, if it is impossible to sqneeze an ideal between it and full ring.

NOTE

i. An ring need not have a maximal ideal
ii. Ring in the unit element has maximal ideal**s**

Examples

1) Let R be the ring of integers and U be an ideal of R. since U is a subgroup of R under addition from group theory (eg subgroup of even integers$_0$) we know that U consists of all multiples of a fixed integer say n_0 (i.e) u = (n_0) if P is a prime no we claim that p = (p) is a maximal ideal of R

Proof

If U is an ideal of R and U) R then U = (n_0) for some integer n_0

Since p ϵ P C U , p=m n_0 for some integer m

since p is a prime no,

p = m n_0 => n_0 =1 or n_0 = p

if n_0 =1 then u = (p) = p

U = P

If n_0 = 1 then 1ϵ U

Let r ϵ R, then r = 1.r ϵ U for all r ϵ R

[U is an ideal of R]

R $\underline{C}$ U

Since u is an ideal other than R (or) P itself between them

P is a maximal ideal of R

2) Let R be the ring of all real valued continous functions on the closed unit interval

Let M = { f(x) ϵ R / f (u2)=0} M is certainly an ideal of R. then M is a maximal ideal of R

Proof

If there is an ideal U of R such that m c u and m ≠ u, then there is a function g(x) ϵ u and g(x) ∉ m

Since g(x) ∉m ,g($^1/_2$) = α ≠ 0

Let h(x) = g(x) – α

Now h($^1/_2$)= g($^1/_2$) – α

= α – α

= 0

h(x) ϵ m c u (i.e) h(x) ϵ u

α = g(x) – h(x) ϵ u ….[u is an ideal of r so a subgroup of r]

now 1 = α α^{-1}ϵ u

since α^{-1} = $^1/_\alpha$

= $\frac{1}{g(x)-h(x)}$ ϵ R …… α^{-1} is continuous and u is an ideal of R

Thus for any t(x) ϵ R we have

t(x) = 1.t(x) ϵ u …[u is an ideal of R]

R $\underline{C}$ U

But U $\underline{C}$ R [u is an ideal of R]

U=R

Thus m is a maximal ideal of R

Theorem 5.2

If R is a commutative ring with unit element and m is an ideal of R then m is a maximal ideal of R iff $R/_M$ is a field

Proof

Given that m is an ideal of R

Assume that $R/_M$ is a field

We shall P.T m is a maximal field of R

Since $R/_M$ is a field , its only ideals are {0} and $R/_M$

Then by theorem 93.4.1) there I a one to one correspondence between the set of ideals of $R/_M$ and the set of ideals of R which contain m. the ideal M of R corresponds to the ideal {0} of $R/_M$ whereas the ideal R of R corresponds to the ideal $R/_M$ of $R/_M$ in this one to one correspondence. Thus there is no ideal between m and R other than these two

Hence m is a maximal ideal of R

Conversely assume that m is a maximal ideal of R

Then by the correspondence mentioned above $R/_M$ has only {0} and itself an ideals. Further

since R is a commutative ring with unit element hen by lemma 3.5.1 , R/M is a field.

Definition .

If all ideals of a ring R are finitely generated then R is called a Noetherian ring.

Theroem 5.3

A commutative ring with identity is Noetherian if and only if given any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there exists an m such that $I_m = I_{m+i}$ for all $i \geq 0$.

Proof.

Let R be Noetherian. Since $\{I_n\}^{\infty}_{n=1}$ is an ascending chain, I =

$\cup^{\infty}_{n=1} I_n$ is an ideal of R. Hence we can find $a_1, a_2, \ldots, a_g \in I$ such that $I = (a_1, a_2, \ldots, a_g)$. It is easy to see that there is an m such that $a_i \in I_m$ for all i = 1, 2, . . . , g. Hence $I \subseteq I_m$ which implies that $I_m = I_{m+i}$ for all $i \geq 0$.

Conversely let every ascending chain of ideals be stationary. Let I be an ideal of R which is not finitely generated. Then I is nonzero and I < R.

Inductively, we can find $a_1, a_2, \ldots \in I$ such that $I_n = (a_1, a_2, \ldots, a_n)$ and the chain I_n, n = 1, 2, . . . is not stationary. This is a contradiction.

Hence I is finitely generated.

THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

Definition

A ring R can be imbedded in a ring R' if there is an isomorphism of R into R'.

If R and R' have unit elements 1 and 1' we insist in addition that this isomorphism takes 1 and 1'

R' is called an over ring or extension of R . if R can be imbedded in r'

Definition

Let R be an integral domain. A nonzero element a ∈ R is called irreducible if it is not a unit and whenever a = bc then either b or c is a unit. We say a is a prime if (a) is a prime ideal.

Theorem 5.4

Every integral domain can be imbedded in a field

Proof

let d be an integral domain

Let m_o be the set of all ordered pairs(a,b) where a,b ϵ D and b ≠ 0 [consider (a,b) as $\frac{a}{b}$]

In m_o we define a relation '~' as follows

(a,b) ~ (c,d) iff ad = bc ----------1

We claim that this is an equivalence reletion on m_o

Let (a,b) , (c,d) , (e,f) ϵ m_o

Since ab= ba

We can write (a,b) ~ (a,b)

(i.e) reflexivity is satisfied

Now let us assume that (a,b) ~ (c,d)

Then by the definition ad=bc

Cb=da (the ring is commutative0

⇨ (c,d) ~ (a,b)

Summary is true

Let (a,b) ~ (c,d) and (c,d) ~ (e,f)

(ie) ad= bc and cf = de

a=$\frac{bc}{d}$ and f=$\frac{de}{c}$

now consider af = $\frac{bc}{d} \cdot \frac{de}{c}$

(i.e) af = be

(i.e) (a,b) ~ (e,f)

(i.e) transitivity is true

Hence the relation '~' defined above is an equivalence relation on m_0

Let [a,b] be the equivalence class of (a,b) in M_0

Let F be the set of all such equivalence classes [a,b] where a,b ϵ D and b $\neq$ 0

We shall prove that F is a field w.r.to two operations addition and multiplication defined below

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

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

Since D is an integral domain and both d $\neq$ 0 and b $\neq$ 0

We have bd $\neq$ 0

[ad + bc,bd] ϵ F and

[ac ,bd] ϵ F

We now P.T the addition defined above is well defined

(I.e) if [a,b] = [a', b']

[c,d] = [c',d']

Then we have to prove that

[a,b] +[c,d] = [a',b'] +[c',d']

To p.T

[ad + bc, bd] =(a'd' + b'c', b'd']

(i.e) to P.T

(ad +bc)b'd' = (a'd' + b'c'+ bd

Since [a,b] =[a'b']

We have $\frac{a}{b} = \frac{a'}{b'}$ => ab' = a'b

Similarly [c,d] = [c',d'] $\frac{c}{d} = \frac{c'}{d'}$ => cd' = c'd

Now consider

(ad + bc)b'd' = ad b'd + bcb'd'

=ab'dd' + bb'cd'

=ba'dd' + bbb'dc'

=bd(a'd' = b'c')

Addition defined above well defined

[0,b] acts as a zero element for this addition and [-a,b] is the additive inverse of [a,b]. then we can verify that F is an abelian group under the addition defined above.we can also verify that the non-zero elements of F namely the elements [a,b] , a $\neq$ 0 form an abelian group under multiplication

Here [d,d] acts as the unit element and $[c,d]^{-1}$ =[d,e] { c $\neq$ 0, [d,c] is in F}

The distributive laws also hold in F

F is a field

We have to s.t D can be imbedded in F for $x \neq 0$, $y \neq 0$ in D, we note that

[ax,x] =[ay,y]

Let us denote [ax,x] by [a,1]

Define $\phi : D \to F$ by $\phi(a) = [a,1]$ ∀ $a \in D$

Let $a,b \in D$

Then $\phi(a + b) = [a + b,1]$

$=[a,1] + [b,1]$

$=\phi(a) + \phi(b)$

Φ is homomorphism of D into F

Let $y \in F$ then $Y=[a,1] \in F, a \in D$ and $\phi(a)=[a,1]=y$

A is the pre image of Y under ϕ

Then by def ϕ is onto.

Now $\phi(a) = \phi(b)$

- ⇨ [a,1] =[b,1]
- ⇨ a= b

ϕ is onto

ϕ is an homomorphism of D into F

F is the homomorphic image of D under ϕ

If 1 is the unit element of D then $\phi(1) \in F$

Let a' be any element of F then

$\phi(a) = a'$ for some $a \in D$

now consider $\phi(1).a' = \phi(1).\ \phi(a)$

$= \phi(1.a)$

$=\phi(a)$

$=a'$

Also $a'.\ \phi(1)= \phi(a).\ \phi(1)$

$= \phi(a.1)$

$= \phi(a)$

$=a'$

$\phi(1)$ is the unit element of F

thus every integral domain can be imbedded in a field

Definition

Let R be a commutative ring. An ideal P of R is said to be a prime ideal of R. If $ab \in P$, $ab \in R$ $\Rightarrow a \in P$ or $b \in P$

Theorem 5.5

Let R be a commutative ring and S an ideal of R then the ring of residue classes $\frac{R}{S}$ is an integral domain iff S is a prime ideal

Proof

Let R be a commutative ring and S an ideal of R.

Then $\frac{R}{S} = \{ S + a / a \in R\}$

Let S + a, s + b be any two elements of $\frac{R}{S}$

Then ab ϵ R

$\frac{R}{S}$ is also a commutative ring

Now let S be a prime ideal of R

Then we have to prove that $\frac{R}{S}$ is an integral domain

The zero element of $\frac{R}{S}$ is the residue class S itself

Let S + a, S + b ϵ $\frac{R}{S}$

Then (s + a) (s + b) = s

- ⇨ s + ab = s
- ⇨ ab ϵ s
- ⇨ either a or b is in s …(s is a prime ideal)
- ⇨ either s = a =s or s + b = s
- ⇨ either s +a or s + b is the zero element of $\frac{R}{S}$

$\frac{R}{S}$ is without zero divisor

Since $\frac{R}{S}$ is a commutative ring without zero divisor, $\frac{R}{S}$ is a integral domain

Conversely , let $\frac{R}{S}$ be an integral domain then we have to P.T S is an prime ideal of R

Let a,b be any two element in r s.t ab ϵ s

We have ab ϵ s

- ⇨ s + ab = s
- ⇨ (s +a) (s + b) = s

$\frac{R}{S}$ is an integral domain it is without zerp divisor

Either $s + a = s$ or $s + b = s$

Either $a \in s$ or $b \in s$

Then by def s is a prime ideal of R

IMPORTANT RESULTS.

Let R be an integral domain and $a, b \in R$. Then

(1) a is a unit in R if and only if (a) = R.

(2) a and b are associates if and only if (a) = (b)

(3) a | b if and only if $(b) \subset (a)$

(4) a is a proper divisor of b if and only if $(b) < (a) < R$.

(5) a is irreducible if and only if (a) is maximal among proper principal ideals.

Definition

An integral domain R is called a factorization domain, abbreviated as FD, if every non-zero element of R can be expressed as a product of irreducible elements.

Definition

. A ring R is said to satisfy ascending chain condition
(acc) on principal ideals if for any chain $(a_1) \subset (a_2) \subset \ldots$ of principal ideals of R, there exists an n such that $(a_n) = (a_{n+i})$ for all i = 1, 2, 3, ...

POSSIBLE QUESTIONS:

Part-B(5X8 = 40 Marks)

Answer all the questions:

1. i) Define an ideal. Prove that the intersection of any two left ideals of a ring is again a left ideal of the ring.

2. Prove that every integral domain can be imbedded into a field.

3. i) If U is an ideal of a ring R with unity and $1 \in U$, prove that U=R.

   ii) If F is a field then prove that its only ideals are (0) and F itself

4. If R is a commutative ring with unit element and M is an ideal of R, then prove that M is a maximal ideal of R iff R | M is a field.

5. Prove that a commutative ring without zero divisor can be imbedded in a field

6. Let R be a commutative ring and S an ideal of R. Then prove that the ring of residue classes R/S is an integral domain iff S is a prime ideal.

7. State and prove unique factorization theorem.

8. Prove that the ring of Gaussian integers is a Euclidean ring.

9. i) Prove that a Euclidian ring possesses a unit element
   ii) Prove that every field is a Euclidean ring.

10. Prove that every euclidean ring is a principal ideal ring.