Reg. No ----------

(16MMU401)

KARPAGAM ACADEMY OF HIGHER EDUCATION

COIMBATORE-21

DEPARTMENT OF MATHEMATICS

Fourth Semester

Group Theory II

I Internal Test - Jan'2018

Date : 17.01.2018 (AN) **Time : 2 Hours**

Class : II B. Sc Mathematics **Maximum: 50 Marks**

PART - A (20 x 1 = 20 Marks)

Answer all the questions:

1. A nonempty set of element G is said to form a ---------, if in G there is a binary operation satisfying closure, associative, identity and inverse property.
   a) subgroup b) group
   c) kernel d) commutator Subgroup
2. The set of positive rationals is a group under ordinary multiplication , then the inverse of any a is ----------.
   a) 1/a b) -a
   c) a d) 0
3. A group G is said to be ---------- if for every a, b ∈ G, a.b = b.a.
   a) infinite b) subgroup
   c) abelian d) finite
4. Every element of the group G is its own -------then G is abelian.
   a) commutative b) identity
   c) associative d) inverse
5. A nonempty subset H of a group G is said to be a ---------- of G if, under the product in G, H itself forms a group.
   a) subgroup b) group
   c) kernel d) commutator Subgroup
6. A subgroup N of G is said to be a normal subgroup of G if ---------
   a) $gng^{-1} \in G$ b) $gng \in G$
   c) $gng^{-1} \in N$ d) $gng \in N$
7. A homomorphism φ of G into $\overline{G}$ with Kernel K φ is an ---------- of G into $\overline{G}$ iff K φ = (e).
   a) automorphism b) endomorphism
   c) inner automorphism d) isomorphism
8. A group is said to be --------- if it has no non-trivial normal subgroup.
   a) normal subgroup b) commutator Subgroup
   c) group d) kernel
9. If φ is a homomorphism of G into $\overline{G}$,then ---------- is defined by $K=\{x \in G \mid \varphi(x) = \bar{e}\}$.
   a) subgroup b) group
   c) kernel d) commutator Subgroup
10. A homomorphism of a group to itself is called an _____
    a) monomorphism b) canonical homomorphism
    c) homomorphism d) endomorphism
11. If two groups G and G^* are isomorphic then it is denoted by ------
    a) $G \cong G^*$ b) $G \approx G^*$
    c) $G = G^*$ d) $G \sim G^*$
12. The mapping $f : G \rightarrow G/N$ is called a ------- mapping.
    a) natural b) one-to-one
    c) onto d) into
13. Every subgroup of a ---------- group is normal.
    a) abelian b) cyclic
    c) ring d) field
14. For two groups G and $\overline{G}$, a mapping $\varphi: G \rightarrow \overline{G}$ is said to be --------- if φ is homomorphism, one-to-one and onto.
    a) isomorphic b) mesomorphic
    c) homomorphic d) group
15. Every homomorphic image of a group G is ---------- to some quotient group of G.
    a) automorphism b) endomorphism
    c) inner automorphism d) isomorphism

16. If φ is a homomorphism of G into $\bar{G}$ then $\varphi(x^{-1}) =$ -------
    a) $(\varphi(x))^{-1}$ b) $\varphi(x)$
    c) x^{-1} d) x
17. The ---------- of a group G is an isomorphism of G onto itself.
    a) automorphism b) endomorphism
    c) inner automorphism d) isomorphism
18. The ------ of a group G is defined by Z = {z∈G: zx = xz, all x∈G}.
    a) normal subgroup b) center
    c) ideal d) ring
19. If G is a group, then the identity element of G is ----------
    a) zero b) two
    c) unique d) one
20. If a∈G, then N(a)={x∈G: ax = xa} is called the ---------- of a in G.
    a) kernal b) group
    c) subgroup d) normalizer

PART – B (3 x 2 = 6 Marks)

Answer all the questions:

21. Define Homomorphism.
22. Write the statement of Third Isomorphism Theorem.
23. Define Inner Automorphism.

PART – C (3 x 8 =24 Marks)

Answer all the questions:

24. a) If φ is a homomorphism of G into $\bar{G}$, then Prove that
    (i) $\varphi(e) = \bar{e}$, the unit element of $\bar{G}$
    (ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all x ∈ G

(OR)

b) If φ is a homomorphism of G into $\bar{G}$ with kernel K, then prove that K is a normal subgroup of G

25. a) State and prove Cayley's theorem.

(OR)

b) Let φ is a homomorphism of G onto $\bar{G}$ with kernel K, then prove that $G/K \approx \bar{G}$.

26. a) If G is a group then prove that $\mathcal{A}(G)$ is also a group.

(OR)

b) Prove that $\mathcal{I}(G) \approx G/z$ and is the center of G.

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: A.HENNA SHENOFER
SUBJECT NAME: GROUP THEORY II SUB.CODE:16MMU401
SEMESTER: IV CLASS: II B.SC MATHEMATICS

S.No	Lecture Duration Period	Topics to be Covered	Support Material/Page Nos
		UNIT-I	
1	1	Introduction to Group Homomorphism	T1:139-141
2	1	Theorem on Kernels	R2:56-58
3	1	Continuation of the theorem on Kernels	R2:58-60
4	1	Tutorial – I	
5	1	Equivalence relations and partitions	R4:53-55
6	1	Cosets	R4:57-59
7	1	Restriction of homomorphism to a subgroups	R4:59-61
8	1	Tutorial – II	
9	1	Properties of homomorphism	T1:142-144
10	1	Continuation of properties of homomorphism	T1:144-146
11	1	Properties of elements under homomorphism	R3:194
12	1	Tutorial – III	
13	1	Properties of subgroup under homomorphism	R3:195-196
14	1	Introduction to Isomorphism	R3:115-117

15	1	Cayley's theorem	R3:119-120
16	1	Tutorial – IV	
17	1	Properties of isomorphism	R3:121
18	1	First isomorphism theorem	T1:321-322
19	1	Examples for First isomorphism theorem	R3:199-200
20	1	Tutorial – V	
21	1	Second isomorphism theorem	T1:322-323
22	1	Third isomorphism theorem	T1:323-324
23	1	Tutorial – VI	
24	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit 1=24		
		UNIT-II	
1	1	Introduction to Automorphism	T1:154-155
2	1	Theorems on Automorphism	R1:135-137
3	1	Continuation of theorems on Automorphism	R1:137-139
4	1	Tutorial – I	
5	1	Inner Automorphism	R2:68-69
6	1	Theorem on inner automorphism	R3:124-125
7	1	Continuation of theorem on inner automorphism	R3:125-126
8	1	Tutorial – II	
9	1	Theorems on automorphism groups of finite and infinite cyclic groups	R2:66-67
10	1	Continuation of theorems on automorphism groups of finite and infinite cyclic groups	R2:67-68
11	1	Factor groups	T1:151-153
12	1	Tutorial – III	

13	1	Theorem on factor groups	R3:173-175
14	1	Continuation on theorem on factor groups	R3:176-178
15	1	Application of factor groups	R3:178-179
16	1	Tutorial – IV	
17	1	Continuation of application of factor groups	R3:179-180
18	1	Characteristics subgroup	R2:70-71
19	1	Theorem on characteristics subgroup	R2:71-72
20	1	Tutorial – V	
21	1	Commutator subgroup	T1:164-165
22	1	Properties of commutator subgroup	T1:165-166
23	1	Tutorial – VI	
24	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit II=24		
		UNIT-III	
1	1	Introduction to direct product	R1:154
2	1	Theorems on direct problem	R2:104-106
3	1	Continuation of theorem on direct product	R2:149-151
4	1	Tutorial – I	
5	1	External direct product	R3:149-151
6	1	Properties of external direct product	R3:151-152
7	1	Continuation of external direct product	R3:152-154
8	1	Tutorial – II	
9	1	The group of units modulo n as an external direct product	R3:154-155
10	1	Continuation of the group of units modulo n as an external	R3:155-156

		direct product	
11	1	Internal direct product	R2:109
12	1	Tutorial – III	
13	1	Examples of internal direct product	R2:110-111
14	1	Theorem on U(n) as an external direct product	R3:157
15	1	Application of indirect product	R2:111-112
16	1	Tutorial – IV	
17	1	Application of direct product	R3:158-159
18	1	Continuation of application of direct product	R3:161-161
19	1	Finite abelian group	R2:113
20	1	Tutorial – V	
21	1	Fundamental theorem of finite abelian group	T1:122-123
22	1	Continuation of fundamental theorem of finite abelian group	T1:124-125
23	1	Tutorial – VI	
24	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit III=24		
		UNIT-IV	
1	1	Notion of a group action	T1:168-170
2	1	Isotropy subgroups	T1:170-171
3	1	Orbits	T1:172-173
4	1	Tutorial – I	
5	1	Stabilizer	R1:52-53
6	1	Kernels	R1:53-54
7	1	Permutation	R3:90-91
8	1	Tutorial – II	

9	1	Cycle notation	R3:93-95
10	1	Products of disjoint cycle	R3:95-96
11	1	Disjoint cycle commute	R3:96-97
12	1	Tutorial – III	
13	1	Order of permutation	R3:97
14	1	Product of 2 cycle	R3:98-99
15	1	Odd permutation of a group	R3:99-100
16	1	Tutorial – IV	
17	1	Even Permutation of a group	R3:100-101
18	1	Simple group	R3:416-417
19	1	Generalized Cayley's theorem	R3:419-420
20	1	Tutorial – V	
21	1	Index theorem	R3:420-421
22	1	Continuation of Index theorem	R3:421-422
23	1	Tutorial – VI	
24	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit IV=24		
		UNIT-V	
1	1	Groups acting on themselves by conjugacy	R1:124-126
2	1	Class equation	R1:126-127
3	1	Tutorial – I	
4	1	Conjugacy in Sn	R1:127-129
5	1	p-groups	R1:190-192
6	1	Probability that two elements commute	R3:397-398
7	1	Tutorial – II	
8	1	Sylow's first theorem	R3:399
9	1	Cauchy's theorem	R3:400

10	1	Sylow's second theorem	R3:400-401
11	1	Tutorial – III	
12	1	Sylow's third theorem	R3:401-403
13	1	Applications of Sylow theorem	R3:403-405
14	1	Tutorial – IV	
15	1	Continuation of applications of Sylow theorem	R3:406
16	1	Non Simplicity test	R3:417-418
17	1	Continuation of Non Simplicity test	R3:418-419
18	1	Tutorial – V	
19	1	Simplicity of A_5	R3:423
20	1	Tutorial – VI	
21	1	Recapitulation and discussion of possible questions	
22	1	Discussion of previous ESE question papers.	
23	1	Discussion of previous ESE question papers.	
24	1	Discussion of previous ESE question papers.	
	Total No of Hours Planned for unit V=24		
Total Planned Hours	**120**		

TEXT BOOK

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

REFERENCES

1. David S. Dummit and Richard M. Foote, (2004)., Abstract Algebra,. Third Edition., John Wiley and Sons (Asia) Pvt. Ltd., Singapore.
2. Herstein.I.N.,(2010). Topics in Algebra ,Second Edition, Willey and sons Pvt Ltd, Singapore.

3. Joseph A. Gallian., (2001). Contemporary Abstract Algebra, Fourth Edition., Narosa Publishing House, New Delhi.
4. Artin.M., (2008). Algebra, Prentice - Hall of India, New Delhi.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: Group Theory II **Subject Code: 16MMU401**

Class : II - B.Sc. Mathematics **Semester : IV**

Unit I

Group Homomorphisms

Part A (20x1=20 Marks)
(Question Nos. 1 to 20 Online Examinations)

Possible Questions

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
If a finite non abelian simple group G has a subgroup of index n, then show that G is isomorphic to a subgroup of A_n.	subgroup	group	kernel	commutator Subgroup	group
The set of positive rationals is a group under ordinary multiplication , then the inverse of any a is ----------.	1/a	-a	a	0	1/a
A group G is said to be ---------- if for every a, b ∈ G, a.b = b.a.	infinite	subgroup	abelian	finite	abelian
Every element of the group G is its own -------then G is abelian.	commutative	identity	associative	inverse	inverse
A nonempty subset H of a group G is said to be a ---------- of G if, under the product in G, H itself forms a group.	subgroup	group	kernel	commutator Subgroup	subgroup
A subgroup N of G is said to be a normal subgroup of G if ---------	$gng^{-1} \in G$	$gng \in G$	$gng^{-1} \in N$	$gng \in N$	$gng^{-1} \in N$
A homomorphism φ of G into $\bar{G}$ with Kernel K φ is an ---------- of G into $\bar{G}$ iff K φ = (e).	automorphism	endomorphism	inner automorphism	isomorphism	isomorphism
A group is said to be --------- if it has no non-trivial normal subgroup.	normal subgroup	commutator Subgroup	group	kernel	normal subgroup
If φ is a homomorphism of G into $\bar{G}$, then ---------- is defined by K={x G | φ(x) = $\bar{e}$}.	subgroup	group	kernel	commutator Subgroup	kernel

A homomorphism of a group to itself is called an _____	monomorphism	canonical homomorphism	homomorphism	endomorphism	endomorphism
If two groups G and G* are isomorphic then it is denoted by ------	$G \cong G^*$	$G \approx G^*$	$G = G^*$	$G \sim G^*$	$G \approx G^*$
The mapping f : G→G/N is called a ------- mapping.	natural	one-to-one	onto	into	natural
Every subgroup of a ---------- group is normal.	abelian	cyclic	ring	field	cyclic
For two groups G and $\bar{G}$, a mapping φ:G→$(G)^{-}$ is said to be --------- if φ is homomorphism, one-to-one and onto.	isomorphic	mesomorphic	homomorphic	group	isomorphic
15. Every homomorphic image of a group G is ---------- to some quotient group of G.	automorphism	endomorphism	inner automorphism	isomorphism	isomorphism
If φ is a homomorphism of G into $\bar{G}$ then φ (x^{-1}) = ------	$(\varphi(x))^{-1}$	φ (x)	x^{-1}	x	$(\varphi(x))^{-1}$
17. The ---------- of a group G is an isomorphism of G onto itself.	automorphism	endomorphism	inner automorphism	isomorphism	automorphism
The ------ of a group G is defined by Z = {z∈G: zx = xz, all x∈G}.	normal subgroup	center	ideal	ring	center
19. If G is a group, then the identity element of G is ----------	zero	two	unique	one	unique
If a∈G, then N(a)={x∈G: ax = xa} is called the ---------- of a in G.	kernal	group	subgroup	normalizer	normalizer

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: Group Theory II **Subject Code: 16MMU401**

Class : II - B.Sc. Mathematics **Semester : IV**

Unit III

Direct Products

Part A (20x1=20 Marks)

(Question Nos. 1 to 20 Online Examinations)

Possible Questions

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
The ---------- of groups G and H is given by {(g, h)|g ∈ G, h ∈ H}.	internal direct product	finite subgroup	external direct product	infinite subgroup	external direct product
The external direct product is denoted by --------.	G⊗H	G⊕H	G⊖H	G⊙H	G⊕H
When G and H are any two groups, then G⊕H and H⊕G are ---------- groups.	endomorphic	mesomorphic	homomorphic	isomorphic	isomorphic
The external direct product of n groups is ---------- to the external direct product of any permutation of the same n groups.	endomorphic	mesomorphic	homomorphic	isomorphic	isomorphic
If G and H are finite groups with order m and n respectively, then G⊕H is a ---------- group with order mn.	infinite	finite	cyclic	ring	finite
The $Z_m \oplus Z_n \approx Z_{mn}$ when ----------.	gcd(m,n)=0	gcd(m,n)=2	gcd(m,n)=1	gcd(m,n)=3	gcd(m,n)=1
If G and H are infinite groups, then -------- is an infinite group.	G⊗H	G⊕H	G⊖H	G⊙H	G⊕H
If Z_2 and Z_3 are abelian, then ---------- is also abelian.	$Z_2 \oplus Z_3$	$Z_2 \otimes Z_3$	$Z_2 \odot Z_3$	$Z_2 \ominus Z_3$	$Z_2 \oplus Z_3$
Let G, H be finite groups and let (g, h) ∈G⊕H, then O(g, h) = ----------.	gcd{O(g)+ O(h)}	gcd{O(g), O(h)}	lcm{O(g)+ O(h)}	lcm{O(g), O(h)}	lcm{O(g), O(h)}
Let G, H be finite cyclic groups, then G⊕H is cyclic iff ----------	lcm{O(G), O(H)}=1	lcm{O(G)+ O(H)}=1	gcd{O(G), O(H)}=1	gcd{O(G)+ O(H)}=1	gcd{O(G), O(H)}=1

Let s and t be natural numbers such that ----------, then $U_t(st) \approx U(s)$.	lcm(s, t)=1	gcd(s, t)=1	lcm(s, t)=0	gcd(s, t)=0	gcd(s, t)=1
If ---------- for $i \neq j$, then $U(n_1.n_2....n_k) \approx U(n_1) \oplus U(n_2) \oplus .....\oplus U(n_k)$.	$gcd(n_i, n_j)=1$	$gcd(n_i, n_j)=0$	$gcd(n_i, n_j)=2$	$gcd(n_i, n_j)=3$	$gcd(n_i, n_j)=1$
Which of the following is the application of external direct product?	number theory	RSA public key encryption	data security	all the above	all the above
If G is an internal direct product of H and K, then it is denoted by ----------.	G=H x K	G= H + K	G=H – K	G=H /K	G=H x K
If H and K are normal subgroups of a group G and if G=HK and $H \cap K=\{e\}$, then G is ----------of H and K.	external direct product	finite subgroup	internal direct product	infinite subgroup	internal direct product
A finite abelian group of prime power order is an internal direct product of ---------- groups.	finite	cyclic	infinite	normal	cyclic
If G is a finite abelian group and ----------, then G has a subgroup of order m.	n|O(G)	n∤O(G)	m∤O(G)	m|O(G)	m|O(G)
Every group of order 4 is ----------.	cyclic	normal	abelian	finite	abelian
U(2) is ---------- to {0}.	isomorphic	mesomorphic	homomorphic	group	isomorphic
The ---------- is also called as Cartesian product.	external direct product	finite subgroup	internal direct product	infinite subgroup	internal direct product

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: Group Theory II **Subject Code: 16MMU401**

Class : II - B.Sc. Mathematics **Semester : IV**

Unit IV

Group Actions

Part A (20x1=20 Marks)

(Question Nos. 1 to 20 Online Examinations)

Possible Questions

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
The group with the set of all permutations of a finite set with respect to the operation composition of permutations is known as --------.	symmetric group	asymmetric group	normal group	cyclic group	symmetric group
The set of all permutations of a finite set S is denoted by ----------.	s(S)	Sym(S)	sy(S)	sym(sym)	Sym(S)
Let G be a group, S be a set and suppose that G acts on S. Then the action of G on S is said to be ---if every element of group G induce the distinct permutation of S.	truthful	cyclic	faithful	normal	faithful
For the trivial action, it is faithful if ----------.	O(G)>0	O(G)>-1	O(G)>2	O(G)>1	O(G)>1
The action of G onto itself by ---------- is faithful iff G has a trivial center.	conjugation	normal	trivial	non trivial	conjugation
If the action of group G onto the set S is faithful then the permutation represented associated to the action is always ----------.	bijective	injective	unique	inverse	injective
The ---------- of a action is a subgroup of G.	unique	inverse	kernel	normal	kernel
The ---------- of a action of G on S is defined as {g ∈ G : g . s = s, ∀ s ∈ S}.	unique	inverse	kernel	normal	kernel
For the ---------- action, the kernel of action is whole of G.	non trivial	trivial	kernel	normal	trivial

The ---------- of stabilizers corresponding to every element of group G is always equal to the kernel of action.	addition	subtraction	union	intersection	intersection
The left cosets and right cosets of ---------- of action are same.	kernel	inverse	unique	normal	kernel
The number of distinct ---------- of kernel of action in G is equal to number of distinct permutations induced by elements of G under this action.	group	subgroup	cosets	normal	cosets
Let group G acts on a non-empty set S then the action of group G on S is said to be ---------- if G has exactly one orbit.	symmetric	reflexive	asymmetric	transitive	transitive
If group G acts on the set S, then every s ∈ S, the number of elements in equivalence class of 's' is equal to the index of the ---------- of 's' in G.	orbit	stabilizer	normal	transitive	stabilizer
If group G acts on the set S, the S can be partitioned into unique set of disjoint ---------- of G.	normal	stabilizer	orbit	transitive	orbit
If the action of group G on S is ---------- then for every s, t ∈ S, there exist g ∈ G such that s=g.t.	transitive	reflexive	symmetric	asymmetric	transitive
The ---------- is drawn as a corollary to the Generalized Cayley theorem.	Sylow's theorem	Lagrange's theorem	Embedded theorem	Index theorem	Index theorem
The ---------- of kernel of action are same.	left cosets	right cosets	both left cosets and right cosets	either left cosets or right cosets	both left cosets and right cosets
For the trivial action, the ---------- of action is whole of G.	kernel	inverse	unique	normal	kernel
The Index theorem is drawn as a corollary to the ----------.	Sylow's theorem	Generalized Cayley theorem	Embedded theorem	Lagrange's theorem	Generalized Cayley theorem

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: Group Theory II **Subject Code: 16MMU401**

Class : II - B.Sc. Mathematics **Semester : IV**

Unit V

Group Action and Simplicity

Part A (20x1=20 Marks)

(Question Nos. 1 to 20 Online Examinations)

Possible Questions

Question	Choice 1	Choice 2	Choice 3	Choice 4	Answer
A non-trivial group G is called ---------- if its only normal subgroups are {e} and G itself.	simple	unique	inverse	identity	simple
A infinite ---------- group cannot be simple.	non abelian	abelian	non trivial	trivial	abelian
A finite abelian group is simple iff its ---------- is a prime.	ring	value	abelian	order	order
The alternating group A_n is simple for ----------.	$n\geq 3$	$n\geq 2$	$n\geq 5$	$n\geq 1$	$n\geq 5$
The G must have a subgroup of order equal to the highest power of p that divides |G|. One such subgroup is called a ---------- of G.	sylow p-subgroup	normal subgroup	trivial subgroup	non trivial subgroup	sylow p-subgroup
Using ---------- test , it is possible to sort out numbers which cannot be order of any simple group.	odd	Sylow	even	unique	Sylow
If G is a group of order ------, where n is an odd integer greater than 1 then G cannot be simple.	2+n	2-n	2n	2/n	2n
The ---------- helps to use the known properties of alternating groups to determine non-simplicity of a group.	Sylow's theorem	Lagrange's theorem	Embedded theorem	Index theorem	Embedded theorem
Which is the test of non-simplicity?	Sylow's theorem	odd test	both Sylow's theorem and odd test	neither Sylow's theorem nor odd theorem	both Sylow's theorem and odd test
If the normal subgroups are {e} and G itself then the non-trivial group G is called ----------.	simple	unique	inverse	identity	simple

When does a finite abelian group is simple?	iff order is 2	iff order is not prime	iff order is odd	iff order is prime	iff order is prime
The elements a and b of a group G are conjugate in G, if ----------.	$xax^{-1}=1$	$xax^{-1}=b$	$xax^{-1}=0$	$xax^{-1}=a$	$xax^{-1}=b$
The ---------- of a is the set $cl(a)=\{xax^{-1} \mid x \in G\}$.	normal	subgroup	conjugacy class	prime	conjugacy class
A group of order p^n, where p is prime is called a ----------.	p-group	n-group	p^2-group	n^2-group	p-group
If $\|G\|$ = ----------, then G is abelian.	p	p^2	p^3	–p	p^2
If G is a group of order m and n divides m, G need not have a subgroup of order ------.	m	m^2	n	n^2	n
Which is the most important results in finite group theory?	Sylow's theorem	Lagrange's theorem	Index theorem	both Sylow's and Lagrange theorem	both Sylow's and Lagrange theorem
The ---------- theorem gives a sufficient condition for the existence of subgroups.	Sylow's	Lagrange	Index	Embedded	Sylow's
If p^k divides $\|G\|$, then G has atleast one subgroup of order ----.	p	p^k	p^3	–p	p^k
Any subgroup of order p^k is called a ---------- of G.	normal subgroup	cyclic subgroup	Sylow p-subgroup	abelian subgroup	Sylow p-subgroup

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

SYLLABUS

Semester - IV

		L	T	P	C
16MMU401	**GROUP THEORY II**	**6**	**2**	**0**	**6**

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

Objectives: To enable the students to learn and gain knowledge about group homomorphism, isomorphism, automorphism and its related properties.

UNIT I

Group homomorphisms, properties of homomorphisms, Cayley's theorem, properties of isomorphisms, First, Second and Third isomorphism theorems.

UNIT II

Automorphism, inner automorphism, automorphism groups, automorphism groups of finite and infinite cyclic groups, applications of factor groups to automorphism groups, Characteristic subgroups, Commutator subgroup and its properties.

UNIT III

Properties of external direct products, the group of units modulo n as an external direct product, internal direct products, Fundamental Theorem of finite abelian groups.

UNIT IV

Group actions, stabilizers and kernels, permutation representation associated with a given group action, Applications of group actions: Generalized Cayley's theorem, Index theorem.

UNIT V

Groups acting on themselves by conjugation, class equation and consequences, conjugacy in Sn, *p*-groups, Sylow's theorems and consequences, Cauchy's theorem, Simplicity of An for $n \geq 5$, non-simplicity tests.

SUGGESTED READINGS

TEXT BOOK

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

REFERENCES

1. David S. Dummit and Richard M. Foote, (2004).,Abstract Algebra,. Third Edition., John Wiley and Sons (Asia) Pvt. Ltd., Singapore.

2. Herstein.I.N.,(2010). Topics in Algebra ,Second Edition, Willey and sons Pvt Ltd, Singapore.
3. Joseph A. Gallian., (2001). Contemporary Abstract Algebra, Fourth Edition.,Narosa Publishing House, New Delhi.
4. Artin.M., (2008).Algebra, Prentice - Hall of India, New Delhi.

UNIT-I

SYLLABUS

Group homomorphisms, properties of homomorphism, Cayley's theorem, properties of isomorphisms, First, Second and Third isomorphism theorems

In this chapter, we consider one of the most fundamental ideas of algebra—homomorphisms. The term *homomorphism* comes from the Greek words *homo*, "like," and *morphe*, "form." We will see that a homomorphism is a natural generalization of an isomorphism and that there is an intimate connection between factor groups of a group and homomorphisms of a group. The concept of group homomorphisms was introduced by Camille Jordan in 1870, in his influential book *Traité des substitutions*.

Group Homomorphism

A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Kernel of a Homomorphism

The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by Ker ϕ.

Properties of Homomorphisms

Properties of Elements under Homomorphism

Let ϕ be a homomorphism from a group G to a group G and let g be an element of G. Then

1. *ϕ carries the identity of G to the identity of $\overline{G}$.*
2. *$\phi(g^n) = (\phi(g))^n$ for all n in Z.*
3. *If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.*
4. *Ker ϕ is a subgroup of G.*
5. *$\phi(a) = \phi(b)$ if and only if $a\text{Ker } \phi = b\text{Ker } \phi$.*
6. *If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\text{Ker } \phi$.*

Properties of Subgroups under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. *$\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.*
2. *If H is cyclic, then $\phi(H)$ is cyclic.*
3. *If H is Abelian, then $\phi(H)$ is Abelian.*
4. *If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.*
5. *If $|Ker\ \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.*
6. *If $|H| = n$, then $|\phi(H)|$ divides n.*
7. *If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.*
8. *If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.*
9. *If ϕ is onto and Ker $\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.*

Lemma

If ϕ is a homomorphism of G into $\bar{G}$, then

1. *$\phi(e) = \bar{e}$, the unit element of $\bar{G}$.*
2. *$\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.*

Proof. To prove (1) we merely calculate $\phi(x)\bar{e} = \phi(x) = \phi(xe) = \phi(x)\phi(e)$, so by the cancellation property in $\bar{G}$ we have that $\phi(e) = \bar{e}$.

To establish (2) one notes that $\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$, so by the very definition of $\phi(x)^{-1}$ in $\bar{G}$ we obtain the result that $\phi(x^{-1}) = \phi(x)^{-1}$.

Lemma

If ϕ is a homomorphism of G into $\bar{G}$ with kernel K, then K is a normal subgroup of G.

Proof. First we must check whether K is a subgroup of G. To see this one must show that K is closed under multiplication and has inverses in it for every element belonging to K.

If $x, y \in K$, then $\phi(x) = \bar{e}$, $\phi(y) = \bar{e}$, where $\bar{e}$ is the identity element of $\bar{G}$, and so $\phi(xy) = \phi(x)\phi(y) = \bar{e}\bar{e} = \bar{e}$, whence $xy \in K$. Also, if $x \in K$, $\phi(x) = \bar{e}$, so, by Lemma 2.7.2, $\phi(x^{-1}) = \phi(x)^{-1} = \bar{e}^{-1} = \bar{e}$; thus $x^{-1} \in K$. K is, accordingly, a subgroup of G.

To prove the normality of K one must establish that for any $g \in G$, $k \in K$, $gkg^{-1} \in K$; in other words, one must prove that $\phi(gkg^{-1}) = \bar{e}$ whenever $\phi(k) = \bar{e}$. But $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\bar{e}\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = \bar{e}$.

Group Isomorphism

An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \qquad \text{for all } a, b \text{ in } G.$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.

Cayley's Theorem

Every group is isomorphic to a group of permutations.

PROOF To prove this, let G be any group. We must find a group $\overline{G}$ of permutations that we believe is isomorphic to G. Since G is all we have to work with, we will have to use it to construct $\overline{G}$. For any g in G, define a function T_g from G to G by

$$T_g(x) = gx \qquad \text{for all } x \text{ in } G.$$

(In words, T_g is just multiplication by g on the left.) We leave it as an exercise (Exercise 33) to prove that T_g is a permutation on the set of elements of G. Now, let $\overline{G} = \{T_g \mid g \in G\}$. Then, $\overline{G}$ is a group under the operation of function composition. To verify this, we first observe that for any g and h in G we have $T_gT_h(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$, so that $T_gT_h = T_{gh}$. From this it follows that T_e is the identity and $(T_g)^{-1} = T_{g^{-1}}$ (see Exercise 9). Since function composition is associative, we have verified all the conditions for $\overline{G}$ to be a group.

The isomorphism ϕ between G and $\overline{G}$ is now ready-made. For every g in G, define $\phi(g) = T_g$. If $T_g = T_h$, then $T_g(e) = T_h(e)$ or $ge = he$. Thus, $g = h$ and ϕ is one-to-one. By the way $\overline{G}$ was constructed, we see that ϕ is onto. The only condition that remains to be checked is that ϕ is operation-preserving. To this end, let a and b belong to G. Then

$$\phi(ab) = T_{ab} = T_aT_b = \phi(a)\phi(b). \qquad \blacksquare$$

Properties of Isomorphisms Acting on Elements

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. *ϕ carries the identity of G to the identity of $\overline{G}$.*
2. *For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$.*
3. *For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.*
4. *$G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.*
5. *$|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).*
6. *For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.*
7. *If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.*

Properties of Isomorphisms Acting on Groups

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. *ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.*
2. *G is Abelian if and only if $\overline{G}$ is Abelian.*
3. *G is cyclic if and only if $\overline{G}$ is cyclic.*
4. *If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.*
5. *If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\}$ is a subgroup of G.*
6. *$\phi(Z(G)) = Z(\overline{G})$.*

Theorem

(First Isomorphism Theorem) Let $\phi : G \to G'$ be a homomorphism with kernel K, and let $\gamma_K : G \to G/K$ be the canonical homomorphism. There is a unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_K(x))$ for each $x \in G$.

The lemma that follows will be of great aid in our proof and intuitive understanding of the other two isomorphism theorems.

Lemma

Let N be a normal subgroup of a group G and let $\gamma : G \to G/N$ be the canonical homomorphism. Then the map ϕ from the set of normal subgroups of G containing N to the set of normal subgroups of G/N given by $\phi(L) = \gamma[L]$ is one to one and onto.

Proof

Theorem 15.16 shows that if L is a normal subgroup of G containing N, then $\phi(L) = \gamma[L]$ is a normal subgroup of G/N. Because $N \leq L$, for each $x \in L$ the entire coset xN in G is contained in L. Thus by Theorem 13.15, $\gamma^{-1}[\phi(L)] = L$. Consequently, if L and M are normal subgroups of G, both containing N, and if $\phi(L) = \phi(M) = H$, then $L = \gamma^{-1}[H] = M$. Therefore ϕ is one to one.

If H is a normal subgroup of G/N, then $\gamma^{-1}[H]$ is a normal subgroup of G by Theorem 15.16. Because $N \in H$ and $\gamma^{-1}[\{N\}] = N$, we see that $N \subseteq \gamma^{-1}[H]$. Then $\phi(\gamma^{-1}[H]) = \gamma[\gamma^{-1}[H]] = H$. This shows that ϕ is onto the set of normal subgroups of G/N. ◆

If H and N are subgroups of a group G, then we let

$$HN = \{hn \mid h \in H, n \in N\}.$$

We define the **join** $H \vee N$ of H and N as the intersection of all subgroups of G that contain HN; thus $H \vee N$ is the smallest subgroup of G containing HN. Of course $H \vee N$ is also the smallest subgroup of G containing both H and N, since any such subgroup must contain HN. In general, HN need not be a subgroup of G. However, we have the following lemma.

Theorem

(Second Isomorphism Theorem) Let H be a subgroup of G and let N be a normal subgroup of G. Then $(HN)/N \simeq H/(H \cap N)$.

Proof

Let $\gamma : G \to G/N$ be the canonical homomorphism and let $H \leq G$. Then $\gamma[H]$ is a subgroup of G/N by Theorem 13.12. Now the action of γ on just the elements of H (called γ **restricted to** H) provides us with a homomorphism mapping H onto $\gamma[H]$, and the kernel of this restriction is clearly the set of elements of N that are also in H, that is, the intersection $H \cap N$. Theorem 34.2 then shows that there is an isomorphism $\mu_1 : H/(H \cap N) \to \gamma[H]$.

On the other hand, γ restricted to HN also provides a homomorphism mapping HN onto $\gamma[H]$, because $\gamma(n)$ is the identity N of G/N for all $n \in N$. The kernel of γ restricted to HN is N. Theorem 34.2 then provides us with an isomorphism $\mu_2 : (HN)/N \to \gamma[H]$.

Because $(HN)/N$ and $H/(H \cap N)$ are both isomorphic to $\gamma[H]$, they are isomorphic to each other. Indeed, $\phi : (HN)/N \to H/(H \cap N)$ where $\phi = {\mu_1}^{-1}\mu_2$ will be an isomorphism. More explicitly,

$$\phi((hn)N) = {\mu_1}^{-1}(\mu_2((hn)N)) = {\mu_1}^{-1}(h) = h(H \cap N). \quad \blacklozenge$$

Theorem

(Third Isomorphism Theorem) Let H and K be normal subgroups of a group G with $K \leq H$. Then $G/H \simeq (G/K)/(H/K)$.

Proof

Let $\phi : G \to (G/K)/(H/K)$ be given by $\phi(a) = (aK)(H/K)$ for $a \in G$. Clearly ϕ is onto $(G/K)/(H/K)$, and for $a, b \in G$,

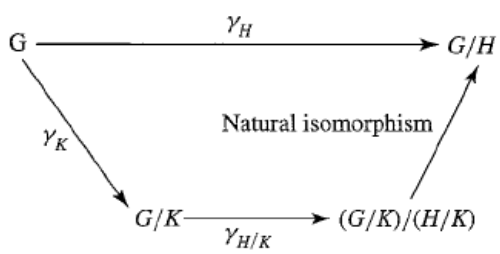
$$\begin{aligned}\phi(ab) &= [(ab)K](H/K) = [(aK)(bK)](H/K)\\ &= [(aK)(H/K)][(bK)(H/K)]\\ &= \phi(a)\phi(b),\end{aligned}$$

so ϕ is a homomorphism. The kernel consists of those $x \in G$ such that $\phi(x) = H/K$. These x are just the elements of H. Then Theorem 34.2 shows that $G/H \simeq (G/K)/(H/K)$. $\blacklozenge$

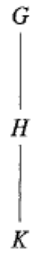
A nice way of viewing Theorem 34.7 is to regard the canonical map $\gamma_H : G \to G/H$ as being factored via a normal subgroup K of G, $K \leq H \leq G$, to give

$$\gamma_H = \gamma_{H/K}\gamma_K,$$

up to a natural isomorphism, as illustrated in Fig. 34.8. Another way of visualizing this theorem is to use the subgroup diagram in Fig. 34.9, where each group is a normal subgroup of G and is contained in the one above it. *The larger the normal subgroup, the smaller the factor group*. Thus we can think of G collapsed by H, that is, G/H, as being smaller than G collapsed by K. Theorem 34.7 states that we can collapse G all the way down to G/H in two steps. First, collapse to G/K, and then, using H/K, collapse this to $(G/K)/(H/K)$. The overall result is the same (up to isomorphism) as collapsing G by H.



34.8 Figure



34.9 Figure

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Define Homomorphism.
2. Define Isomorphism.
3. Define Normalizer.
4. Define centre of a group.
5. Write about Kernel of a group.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Let G be a group of all non zero real number under multiplication and $\bar{G}$={1, -1}be group under multiplication. Prove that φ is a homomorphism.
2. If $\varphi$is a homomorphism of G into $\bar{G}$, then prove that
   (i) $\varphi(e) = \bar{e}$, the unit element in $\bar{G}$.
   (ii) $\varphi(x^{-1}) = \varphi(x)^{-1} \forall\, x \in G$.
3. Let φ be a homomorphism of G into $\bar{G}$ with kernel K, then prove that K is a normal subgroup of G.
4. If φ is a homomorphism of G onto $\bar{G}$ with kernel K, then show that the set of all inverse images $\bar{g} \in \bar{G}$ under φ in G is given by kx where x is any particular inverse image of $\bar{g}$ in G.
5. State and prove fundamental theorem of homomorphism.
6. State and prove first isomorphism theorem.
7. Let φ be the homomorphism of G onto $\bar{G}$with kernel K. For $\bar{H}$ is a subgroup of $\bar{G}$, let H be defined by H = $\{x \in G : \varphi(x) \in \bar{H}\}$. Then prove that H is a subgroup of G and H $\supset$ K. If $\bar{H}$ is normal in $\bar{G}$, then H is normal in G.
8. State and prove third isomorphism theorem.
9. State and prove second isomorphism theorem.
10. State and prove Cayley's theorem.

UNIT-II

SYLLABUS

Automorphism, inner automorphism, automorphism groups, automorphism groups of finite and infinite cyclic groups, applications of factor groups to automorphism groups, Characteristic subgroups, Commutator subgroup and its properties.

Automorphisms

Automorphism is nothing but a special kind of isomorphism.

Definition

"An isomorphism from a group G onto itself is called an automorphism of G. The set of all automorphisms of a group G is usually denoted by $Aut(G)$". Let us now consider a few examples of automorphisms.

Example

Consider the Identity map from a group G onto itself, i.e. $I : G \to G$, such that, $I(x) = x \quad \forall\ x \in G$. I is trivially an automorphism of G. In fact, it is sometimes referred as trivial automorphism of G.

Example

Consider $\mathbb{C}$, the group of complex numbers w.r.t. addition. We define $f : \mathbb{C} \to \mathbb{C}$ as

$$f(a+bi) = a - bi \qquad \forall\, a+bi \in \mathbb{C}$$

- *Well defined and one-one:*

$$f(a+bi) = f(c+di) \quad \text{for } a+bi,\ c+di \in \mathbb{C}$$

$\Leftrightarrow \quad a - bi = c - di$

$\Leftrightarrow \quad a = c \quad \text{and} \quad b = d$

$\Leftrightarrow \quad a + bi = c + di$

- *Onto*: For $a + bi$ in $\mathbb{C}$, $a - bi$ is its pre-image under f.
- *Operation preserving:*

Let $x = a + bi$ and $y = c + di$ be in $\mathbb{C}$

$$f(x+y) = f((a+c)+(b+d)i)$$

$$= (a+c) - (b+d)i$$

$$= (a - bi) + (c - di)$$

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

Hence, f is an automorphism of $\mathbb{C}$.

Inner Automorphisms

Definition

Inner Automorphism induced by *a*

"Let G be a group and $a \in G$. $\phi_a : G \to G$ defined as $\phi_a(x) = axa^{-1} \ \forall \ x \in G$

is called inner automorphism of G induced by a".

Consequently, corresponding to every element a of G, we have an automorphism of G induced by it. Set of all inner automorphisms of G is denoted by $Inn(G)$.

Theorem

"*Aut(G)* and *Inn(G)* both form groups under the operation of composition of mappings".

***Proof*: Aut(G) is a group:**

- *Non-empty:* As identity map is in *Aut(G)*, *Aut(G)* is non-empty.
- *Closure:* Let f and g be in *Aut(G)*. Since f and g are bijective, so is their composition $f \circ g$. Also for x and y in G,

$$(f \circ g)(xy) = f(g(xy))$$

$$= f(g(x)g(y)), \quad \text{as } g \text{ is operation preserving.}$$

$$= f(g(x))f(g(y)), \quad \text{as } f \text{ is operation preserving.}$$

$$= (f \circ g)(x)(f \circ g)(y)$$

Thus, $f \circ g \in Aut(G)$.

- *Associativity:* As composition of mappings is associative, so associativity holds in *Aut(G)* as well.
- *Identity:* Clearly, the identity map serves as the identity element of *Aut(G)*.
- *Inverse:* Let $f \in Aut(G)$. As f is bijective, so f^{-1} exists and is bijective as well. Also for x and y in G, let $f^{-1}(x) = a$, $f^{-1}(y) = b$. As f is operation preserving, $f(ab) = f(a)f(b)$. Consequently $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$. Hence $f^{-1} \in Aut(G)$. ■

Inn(G) is a group:

Clearly $Inn(G) \subseteq Aut(G)$

- *Non-empty:* Inner automorphism induced by the identity of G, i.e. ϕ_e is in *Inn(G)* and thus *Inn(G)* is non-empty.
- *Closure:* Let ϕ_a and ϕ_b be in *Inn(G)*. For $x \in G$,

$$\begin{aligned}
&\phi_a\phi_b(x)\\
&= \phi_a(\phi_b(x))\\
&= \phi_a(bxb^{-1})\\
&= a(bxb^{-1})a^{-1}\\
&= (ab)x(b^{-1}a^{-1})\\
&= (ab)x(ab)^{-1}\\
&= \phi_{ab}(x)
\end{aligned}$$

Thus closure holds in *Inn(G)*.

- *Inverse:* Let $\phi_a \in Inn(G)$. Then

$$\phi_a\phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e = \text{Identity automorphism} = \phi_{a^{-1}}\phi_a$$

Thus, $\phi_{a^{-1}}$ is inverse of ϕ_a .

Hence *Inn(G)* is a subgroup of *Aut(G)* and therefore a group in itself.

Problem: Let g be an element of a group G. Show that the inner automorphism induced by g is same as the inner automorphism induced by zg, where z is in Z(G), the center of G.

Solution: Inner automorphism induced by zg is ϕ_{zg}, which is defined as

$$\begin{aligned}
\phi_{zg}(x) &= (zg)x(zg)^{-1} && \forall\ x \in G\\
&= (gz)x(g^{-1}z^{-1}), && \text{as } z \in Z(G)\\
&= (gz)x(z^{-1}g^{-1}), && \text{as } z \in Z(G) \text{ implies } z^{-1} \in Z(G).\\
&= gxzz^{-1}g^{-1}\\
&= gxg^{-1}\\
&= \phi_g(x)
\end{aligned}$$

Hence $\phi_{zg} \equiv \phi_g$.

Problem: Find $Inn(D_4)$.

Solution: $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.
So, $Inn(D_4)$ can possibly be $\{\phi_{R_0}, \phi_{R_{90}}, \phi_{R_{180}}, \phi_{R_{270}}, \phi_H, \phi_V, \phi_D, \phi_{D'}\}$.

Le us now figure out repetitions in this list.

(i) Consider $\phi_{R_{180}}$. For any x in D_4,

$$\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x, \quad as\ R_{180} \in Z(D_4)$$

$$= \phi_{R_0}(x)$$

Thus, $\phi_{R_{180}} \equiv \phi_{R_0}$.

(ii) Next consider $\phi_{R_{270}}$.

$$\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1}$$

$$= \phi_{R_{90}}(x)$$

Thus, $\phi_{R_{270}} \equiv \phi_{R_{90}}$.

(iii) Again for ϕ_H,

$$\phi_H(x) = HxH^{-1} = R_{180}VxV^{-1}R_{180}^{-1}, \text{ as } H = R_{180}V$$

$$= VxV^{-1} = \phi_V(x)$$

Thus, $\phi_H \equiv \phi_V$.

(iv) Similarly, using the fact that $D' = R_{180}D$, we get $\phi_{D'} \equiv \phi_D$. Therefore, the previous list for $Inn(D_4)$ reduces to $\{\phi_0, \phi_{90}, \phi_H, \phi_D\}$. We are now left to check whether these four inner automorphisms are distinct or not.

If we consider the action of these automorphisms on the element H of D_4, we get $\phi_{R_0} \neq \phi_{R_{90}}$ and $\phi_H \neq \phi_D$. Similarly, considering their action on other elements of D_4, one can easily deduce that all of them are distinct. Consequently, $Inn(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$.

■

Automorphism groups of Finite and Infinite Cyclic Groups

In this section, we shall see that the automorphism groups of finite as well as infinite cyclic groups can be characterized completely.

Theorem

Aut(G), when G is an infinite cyclic group

"If G is an infinite cyclic group, then *Aut(G)* is a cyclic group of order 2".

Proof: Let $G = \langle a \rangle$ and $\phi \in Aut(G)$. We prove the theorem in following steps:

Step 1: We claim that $G = \langle \phi(a) \rangle$, i.e. $\phi(a)$ also generates G.

For that, take $x \in G$. Since ϕ is onto, there exists y in G such that $x = \phi(y)$. As $G = \langle a \rangle$ and y is in G, so $y = a^m$ for some $m \in \mathbb{N}$.

Now $x = \phi(y)$

$= \phi(a^m)$

$= (\phi(a))^m$, as ϕ is a homomorphism.

Hence the claim.

Step 2: G, being an infinite cyclic group, can have at the most two generators, namely a and a^{-1}. Thus $\phi(a)$ and hence ϕ has got only two choices:

$\phi(a) = a$ or $\phi(a) = a^{-1}$

Therefore, $|Aut(G)| \leq 2$.

Step 3: Define $f : G \to G$ as $f(x) = x^{-1}$ $\forall x \in G$. G, being cyclic, is Abelian and thus f defines an automorphism of G

It is important to see that f is different from the identity automorphism, for if

$f(x) = x$ $\forall x \in G$

$\Rightarrow f(a) = a$

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

$\Rightarrow a^2 = e$

$\Rightarrow |a|$ is finite, a contradiction.

Therefore, $|Aut(G)| \geq 2$.

From steps 2 and 3, it follows that $|Aut(G)| = 2$. $Aut(G)$, being a group of order 2 (prime), is cyclic.

Theorem

$Aut(Z_n) \approx U(n)$

"For every natural number n, $Aut(Z_n)$ is isomorphic to $U(n)$".

Proof: Define $\phi : Aut(Z_n) \to U(n)$ as

$$\phi(\alpha) = \alpha(1) \qquad \forall\ \alpha \in Aut(Z_n)$$

- *well defined:* 1 being generator of Z_n and α an automorphism of Z_n, we have $\alpha(1)$ also generates Z_n. But generators of Z_n are of the form $\underbrace{(1+1+.....+1)}_{k\ times} = k$, where g.c.d. (k, n) = 1.

So, $\alpha(1) \in U(n)$.

- *One-one:* Let $\phi(\alpha_1) = \phi(\alpha_2)$; α_1, α_2 are in $Aut(Z_n)$.

$\Rightarrow \alpha_1(1) = \alpha_2(1)$

$\Rightarrow k\alpha_1(1) = k\alpha_2(1)$ for all k in Z_n.

$\Rightarrow \alpha_1(k) = \alpha_2(k)$ for all k in Z_n.

$\Rightarrow \alpha_1 \equiv \alpha_2$.

- *Onto:* Let $m \in U(n)$. This means m < n and gcd(m, n) = 1. We need to find f ∈ Aut(Z_n), such that $f(1) = m$ .Define $f : Z_n \to Z_n$ as

$f(x) = mx(\mathrm{mod}\, n)$ for all x in Z_n.

First we prove that $f \in Aut(Z_n)$. Clearly f is well defined.

Also, $f(x_1) = f(x_2)$, for some x_1 and x_2 in Z_n.

$\Rightarrow mx_1(\mathrm{mod}\, n) = mx_2(\mathrm{mod}\, n)$

$\Rightarrow mx_1 = mx_2(\mathrm{mod}\, n)$

$\Rightarrow n$ divides $m(x_1 - x_2)$.

As m and n are co-prime, so n has to divide $(x_1 - x_2)$. Hence $x_1 = x_2$ in Z_n. This shows that f is one-one. Being a one-one map from a finite set to itself it is onto as well. Lastly to see that f is operation preserving we take x_1 and x_2 in Z_n.

Consider

$f(x_1 + x_2) = m(x_1 + x_2)(\mathrm{mod}\, n)$

$= (mx_1 + mx_2)(\text{mod}\, n)$

$= mx_1(\text{mod}\, n) + mx_2(\text{mod}\, n)$

$= f(x_1) + f(x_2)$

Hence we have $f \in Aut(Z_n)$.

Also $\phi(f) = f(1) = m(\text{mod}\, n) = m$.

Thus, ϕ is onto.

- *Operating Preserving:* Let $\alpha, \beta \in Aut(Z_n)$.

Consider $\phi(\alpha \circ \beta) = (\alpha \circ \beta)(1)$

$= \alpha(\beta(1))$

$= \alpha(\underbrace{1 + 1 + ... + 1}_{\beta(1)\ times})$

$= \underbrace{\alpha(1) + \alpha(1) + ... + \alpha(1)}_{\beta(1)\ times}$, as α is an automorphism.

$= \alpha(1)\beta(1) = \phi(\alpha)\phi(\beta)$.

Hence $Aut(Z_n) \approx U(n)$.

Example

Find $Aut(Z_6)$.

Solution: $Aut(Z_6) \approx U(6) = \{1, 5\}$ mod 6.

Thus, $Aut(Z_6)$ being a group of order 2 (prime) is cyclic and hence isomorphic to Z_2.

Applications of factor groups to Automorphism groups

In this section we study a theorem which connects the group of inner automorphisms to factor groups.

Theorem

"$G / Z(G) \approx Inn(G)$"

For any group G, $G / Z(G)$ is isomorphic to $Inn(G)$ where $Z(G)$ is the center of G.

Proof: Define a map $f: G/Z(G) \to Inn(G)$ as

$f(gZ(G)) = \phi_g$ for all $gZ(G) \in G/Z(G)$, where

$\phi_g : G \to G$ is $\phi_g(x) = gxg^{-1}$ for all x in G.

- *Well defined and one-one:*

$aZ(G) = bZ(G)$

$\Leftrightarrow a^{-1}b \in Z(G)$

$\Leftrightarrow (a^{-1}b)x = x(a^{-1}b) \forall x \in G$

$\Leftrightarrow bxb^{-1} = axa^{-1} \forall x \in G$

$\Leftrightarrow \phi_b \equiv \phi_a$

$\Leftrightarrow f(bZ(G)) = f(aZ(G))$

- *Onto:* Clearly for $\phi_g \in Inn(G)$, $gZ(G)$ is its pre-image under f.
- *Operation*-preserving: Let $aZ(G), bZ(G) \in G/Z(G)$.

Consider $f((aZ(G)))(bZ(G))) = f((ab)Z(G)) = \phi_{ab}$

$f(aZ(G))f(bZ(G)) = \phi_a\phi_b$.

Since we know $\phi_{ab} \equiv \phi_a\phi_b$ for all a and b in G, we have f is an isomorphism.

Characteristic Subgroups

Definition

"A subgroup N of a group G is called a *characteristic subgroup* if $\varphi(N) = N$ for all automorphisms φ of G".

Example

Every subgroup of the group of integers $(\mathbb{Z}, +)$ is a characteristic subgroup.

Let H be any subgroup of $(\mathbb{Z}, +)$. Then $H = m\mathbb{Z}$ for some m≥0.

Also, from Theorem 5.1 we know that $Aut(\mathbb{Z}) = \{I, \varphi\}$ where

$$I(n) = n \; \forall \; n \in \mathbb{Z}$$

and

$\varphi(n) = -n \; \forall \; n \in \mathbb{Z}$.

Clearly $I(H) = H$. Also,

$$\varphi(H) = \varphi(m\mathbb{Z}) = -m\mathbb{Z} = m\mathbb{Z} = H.$$

Hence H is a characteristic subgroup of $\mathbb{Z}$.

Example

Center of a group is a characteristic subgroup.

Let G be a group and Z(G) be its center.
Let $\varphi \in Aut(G)$
In order to prove that Z(G) is a characteristic subgroup of G, we need to show that $\varphi(Z(G)) \subseteq Z(G)$.
For this, let $y \in \varphi(Z(G))$. Then $y = \varphi(z)$ for some $z \in Z(G)$.
Let $g \in G$. As φ is onto, $g = \varphi(g')$ for some $g' \in G$.
Also as $z \in Z(G)$, $zg' = g'z$.
$\therefore \varphi(zg') = \varphi(g'z)$.
$or\ \varphi(z)\varphi(g') = \varphi(g')\varphi(z)$.
$or\ yg = gy$.
Hence $y \in Z(G)$.
Thus, Z(G) is a characteristic subgroup of G.

Theorem

Characteristic subgroups are normal

"Every characteristic subgroup N of a group G is normal in G ".

Proof: Let N be a characteristic subgroup of G. Then $\varphi(N) \subseteq N$ for all $\varphi \in Aut(G)$.
In particular, for $g \in G$ and $n \in N$ we have
$\varphi_g(N) \subseteq N$, where φ_g denotes the inner automorphism of G induced by g.
Thus, $gng^{-1} = \varphi_g(n) \in N$ and hence N is a normal subgroup of G.

Theorem

Characteristic property is transitive

"If N is a characteristic subgroup of K and K is a characteristic subgroup of G then N is a characteristic subgroup of G".

Proof: Let $\varphi \in Aut(G)$. As K is a characteristic subgroup of G, $\varphi(K) = K$ and hence $\tau = \varphi|_K$ is an automorphism of K. Since N is a characteristic subgroup of K, $\tau(N) = N$.
But $\tau(N) = \varphi(N)$. Hence N is invariant under all automorphisms of G. This concludes the proof. ■

Commutator Subgroup

Definition

"Let G be a group and $x, y \in G$. The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y".
If S denotes the set of all commutators of G then the subgroup of G generated by S is called the *commutator subgroup* of G and is denoted by G'.

Theorem

Commutator subgroup is a characteristic subgroup

"G' is a characteristic subgroup of G".

Proof: Let $\varphi \in Aut(G)$. We show that $\varphi(G') \subseteq G'$.

Observe that if c is a commutator in G then c= $x^{-1}y^{-1}xy$ for some x and y in G. As φ is an automorphism, $\varphi(c) = \varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)$. Thus, $\varphi(c)$ is also a commutator in G.

Now let $z \in G'$. Then $z = c_1c_2 \dots c_k$, where each c_i is a commutator in G.

$\therefore \varphi(z) = \varphi(c_1)\varphi(c_2)\dots\varphi(c_k)$, where each $\varphi(c_i)$ is a commutator as seen above.

$\therefore \varphi(z) \in G'$.

Hence G′ is a characteristic subgroup of G.

Corollary

(Commutator subgroup is a normal subgroup) As characteristic subgroups are normal, G′ is a normal subgroup of G. [It is easy to prove that commutator subgroup is normal using the definition of normal subgroups as well. We leave it as an exercise for the reader].

Theorem

The factor group G/G′

a) G/G′ is Abelian.

b) G′ is the smallest subgroup of G such that G/G′ is Abelian, i.e. if N is any subgroup of G such that G/N is Abelian then N≥G′.

Proof:

a) Let $x, y \in G$.

Now $G'xG'y = G'yG'x$

iff $G'xy = G'yx$

iff $(xy)(yx)^{-1} \in G'$

iff $xyx^{-1}y^{-1} \in G'$, which is true by definition of G′.

Hence, G/G′ is Abelian.

b) Let N be a subgroup of G such that G/N is Abelian.
Then for any $x, y \in G$, $NxNy = NyNx$.
i.e. $Nxy = Nyx$
i.e. $xyx^{-1}y^{-1} \in N$.
Thus N contains the set of all commutators of G. As G′ is the smallest subgroup of G containing the set of commutators, it follows that G' ⊆ N. ■

Corollary

G is Abelian iff G′= {e}.

Proof: Let G be Abelian and N= {e}.

Then G/N= G/{e} is Abelian. So, by above theorem G' ⊆ N = {e}. Also, {e} ⊆ G'. Hence G′={e}. Conversely, if G′={e} then G/G′= G/{e} is Abelian by above theorem. But, G/{e} ≅ G, so G is Abelian.

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Define Automorphism.
2. Define Inner Automorphism.
3. Define factor group.
4. Write about generator of a group.
5. Define Characteristic subgroup.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Prove that if G is a group, the Aut(G) is also a group.
2. Let G be a group and $g \in G$. Prove that Tg is an automorphism.
3. Prove that $Inn(G) \approx G/Z$.
4. Determine $Aut(Z_{10})$.
5. Prove that $Aut(Z_n) \approx U(n)$.
6. Let G be a group and let Z(G) be the centre of G. If G/Z(G) is cyclic , then prove that G is abelian.
7. For any group G, show that G/Z(G) is isomorphic to Inn(G).
8. Prove that every characteristic subgroup N of a group G is normal in G.
9. Show that characteristic property is transitive.
10. Prove that commutator subgroup is a characteristic subgroup.

UNIT-II

SYLLABUS

Automorphism, inner automorphism, automorphism groups, automorphism groups of finite and infinite cyclic groups, applications of factor groups to automorphism groups, Characteristic subgroups, Commutator subgroup and its properties.

Automorphisms

Automorphism is nothing but a special kind of isomorphism.

Definition

"An isomorphism from a group G onto itself is called an automorphism of G. The set of all automorphisms of a group G is usually denoted by $Aut(G)$". Let us now consider a few examples of automorphisms.

Example

Consider the Identity map from a group G onto itself, i.e. $I : G \to G$, such that, $I(x) = x \quad \forall\ x \in G$. I is trivially an automorphism of G. In fact, it is sometimes referred as trivial automorphism of G.

Example

Consider $\mathbb{C}$, the group of complex numbers w.r.t. addition. We define $f : \mathbb{C} \to \mathbb{C}$ as

$$f(a+bi) = a - bi \qquad \forall\, a+bi \in \mathbb{C}$$

- *Well defined and one-one:*

$$f(a+bi) = f(c+di) \quad \text{for } a+bi,\ c+di \in \mathbb{C}$$

$\Leftrightarrow \quad a - bi = c - di$

$\Leftrightarrow \quad a = c \quad \text{and} \quad b = d$

$\Leftrightarrow \quad a + bi = c + di$

- *Onto*: For $a + bi$ in $\mathbb{C}$, $a - bi$ is its pre-image under f.
- *Operation preserving:*

Let $x = a + bi$ and $y = c + di$ be in $\mathbb{C}$

$$f(x+y) = f((a+c)+(b+d)i)$$

$$= (a+c) - (b+d)i$$

$$= (a - bi) + (c - di)$$

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

Hence, f is an automorphism of $\mathbb{C}$.

Inner Automorphisms

Definition

Inner Automorphism induced by *a*

"Let G be a group and $a \in G$. $\phi_a : G \to G$ defined as $\phi_a(x) = axa^{-1} \ \forall \ x \in G$

is called inner automorphism of G induced by a".

Consequently, corresponding to every element a of G, we have an automorphism of G induced by it. Set of all inner automorphisms of G is denoted by $Inn(G)$.

Theorem

"*Aut(G)* and *Inn(G)* both form groups under the operation of composition of mappings".

***Proof*: Aut(G) is a group:**

- *Non-empty:* As identity map is in *Aut(G)*, *Aut(G)* is non-empty.
- *Closure:* Let f and g be in *Aut(G)*. Since f and g are bijective, so is their composition $f \circ g$. Also for x and y in G,

$$(f \circ g)(xy) = f(g(xy))$$

$$= f(g(x)g(y)), \quad \text{as } g \text{ is operation preserving.}$$

$$= f(g(x))f(g(y)), \quad \text{as } f \text{ is operation preserving.}$$

$$= (f \circ g)(x)(f \circ g)(y)$$

Thus, $f \circ g \in Aut(G)$.

- *Associativity:* As composition of mappings is associative, so associativity holds in *Aut(G)* as well.
- *Identity:* Clearly, the identity map serves as the identity element of *Aut(G)*.
- *Inverse:* Let $f \in Aut(G)$. As f is bijective, so f^{-1} exists and is bijective as well. Also for x and y in G, let $f^{-1}(x) = a$, $f^{-1}(y) = b$. As f is operation preserving, $f(ab) = f(a)f(b)$. Consequently $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$. Hence $f^{-1} \in Aut(G)$. ■

Inn(G) is a group:

Clearly $Inn(G) \subseteq Aut(G)$

- *Non-empty:* Inner automorphism induced by the identity of G, i.e. ϕ_e is in *Inn(G)* and thus *Inn(G)* is non-empty.
- *Closure:* Let ϕ_a and ϕ_b be in *Inn(G)*. For $x \in G$,

$$\begin{aligned}
&\phi_a\phi_b(x)\\
&= \phi_a(\phi_b(x))\\
&= \phi_a(bxb^{-1})\\
&= a(bxb^{-1})a^{-1}\\
&= (ab)x(b^{-1}a^{-1})\\
&= (ab)x(ab)^{-1}\\
&= \phi_{ab}(x)
\end{aligned}$$

Thus closure holds in *Inn(G)*.

- *Inverse:* Let $\phi_a \in Inn(G)$. Then

$$\phi_a\phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e = \text{Identity automorphism} = \phi_{a^{-1}}\phi_a$$

Thus, $\phi_{a^{-1}}$ is inverse of ϕ_a .

Hence *Inn(G)* is a subgroup of *Aut(G)* and therefore a group in itself.

Problem: Let g be an element of a group G. Show that the inner automorphism induced by g is same as the inner automorphism induced by zg, where z is in Z(G), the center of G.

Solution: Inner automorphism induced by zg is ϕ_{zg}, which is defined as

$$\begin{aligned}
\phi_{zg}(x) &= (zg)x(zg)^{-1} && \forall\ x \in G\\
&= (gz)x(g^{-1}z^{-1}), && \text{as } z \in Z(G)\\
&= (gz)x(z^{-1}g^{-1}), && \text{as } z \in Z(G) \text{ implies } z^{-1} \in Z(G).\\
&= gxzz^{-1}g^{-1}\\
&= gxg^{-1}\\
&= \phi_g(x)
\end{aligned}$$

Hence $\phi_{zg} \equiv \phi_g$.

Problem: Find $Inn(D_4)$.

Solution: $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.
So, $Inn(D_4)$ can possibly be $\{\phi_{R_0}, \phi_{R_{90}}, \phi_{R_{180}}, \phi_{R_{270}}, \phi_H, \phi_V, \phi_D, \phi_{D'}\}$.

Le us now figure out repetitions in this list.

(i) Consider $\phi_{R_{180}}$. For any x in D_4,

$$\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x, \quad as\ R_{180} \in Z(D_4)$$

$$= \phi_{R_0}(x)$$

Thus, $\phi_{R_{180}} \equiv \phi_{R_0}$.

(ii) Next consider $\phi_{R_{270}}$.

$$\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1}$$

$$= \phi_{R_{90}}(x)$$

Thus, $\phi_{R_{270}} \equiv \phi_{R_{90}}$.

(iii) Again for ϕ_H,

$$\phi_H(x) = HxH^{-1} = R_{180}VxV^{-1}R_{180}^{-1}, \text{ as } H = R_{180}V$$

$$= VxV^{-1} = \phi_V(x)$$

Thus, $\phi_H \equiv \phi_V$.

(iv) Similarly, using the fact that $D' = R_{180}D$, we get $\phi_{D'} \equiv \phi_D$. Therefore, the previous list for $Inn(D_4)$ reduces to $\{\phi_0, \phi_{90}, \phi_H, \phi_D\}$. We are now left to check whether these four inner automorphisms are distinct or not.

If we consider the action of these automorphisms on the element H of D_4, we get $\phi_{R_0} \neq \phi_{R_{90}}$ and $\phi_H \neq \phi_D$. Similarly, considering their action on other elements of D_4, one can easily deduce that all of them are distinct. Consequently, $Inn(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$.

■

Automorphism groups of Finite and Infinite Cyclic Groups

In this section, we shall see that the automorphism groups of finite as well as infinite cyclic groups can be characterized completely.

Theorem

Aut(G), when G is an infinite cyclic group

"If G is an infinite cyclic group, then *Aut(G)* is a cyclic group of order 2".

Proof: Let $G = \langle a \rangle$ and $\phi \in Aut(G)$. We prove the theorem in following steps:

Step 1: We claim that $G = \langle \phi(a) \rangle$, i.e. $\phi(a)$ also generates G.

For that, take $x \in G$. Since ϕ is onto, there exists y in G such that $x = \phi(y)$. As $G = \langle a \rangle$ and y is in G, so $y = a^m$ for some $m \in \mathbb{N}$.

Now $x = \phi(y)$

$= \phi(a^m)$

$= (\phi(a))^m$, as ϕ is a homomorphism.

Hence the claim.

Step 2: G, being an infinite cyclic group, can have at the most two generators, namely a and a^{-1}. Thus $\phi(a)$ and hence ϕ has got only two choices:

$\phi(a) = a$ or $\phi(a) = a^{-1}$

Therefore, $|Aut(G)| \leq 2$.

Step 3: Define $f : G \to G$ as $f(x) = x^{-1}$ $\forall x \in G$. G, being cyclic, is Abelian and thus f defines an automorphism of G

It is important to see that f is different from the identity automorphism, for if

$f(x) = x$ $\forall x \in G$

$\Rightarrow f(a) = a$

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

$\Rightarrow a^2 = e$

$\Rightarrow |a|$ is finite, a contradiction.

Therefore, $|Aut(G)| \geq 2$.

From steps 2 and 3, it follows that $|Aut(G)| = 2$. $Aut(G)$, being a group of order 2 (prime), is cyclic.

Theorem

$Aut(Z_n) \approx U(n)$

"For every natural number n, $Aut(Z_n)$ is isomorphic to $U(n)$".

Proof: Define $\phi : Aut(Z_n) \to U(n)$ as

$$\phi(\alpha) = \alpha(1) \qquad \forall\ \alpha \in Aut(Z_n)$$

- *well defined:* 1 being generator of Z_n and α an automorphism of Z_n, we have $\alpha(1)$ also generates Z_n. But generators of Z_n are of the form $\underbrace{(1+1+.....+1)}_{k\ times} = k$, where g.c.d. (k, n) = 1.

So, $\alpha(1) \in U(n)$.

- *One-one:* Let $\phi(\alpha_1) = \phi(\alpha_2)$; α_1, α_2 are in $Aut(Z_n)$.

$\Rightarrow \alpha_1(1) = \alpha_2(1)$

$\Rightarrow k\alpha_1(1) = k\alpha_2(1)$ for all k in Z_n.

$\Rightarrow \alpha_1(k) = \alpha_2(k)$ for all k in Z_n.

$\Rightarrow \alpha_1 \equiv \alpha_2$.

- *Onto:* Let $m \in U(n)$. This means m < n and gcd(m, n) = 1. We need to find f ∈ Aut(Z_n), such that $f(1) = m$ .Define $f : Z_n \to Z_n$ as

$f(x) = mx(\mathrm{mod}\, n)$ for all x in Z_n.

First we prove that $f \in Aut(Z_n)$. Clearly f is well defined.

Also, $f(x_1) = f(x_2)$, for some x_1 and x_2 in Z_n.

$\Rightarrow mx_1(\mathrm{mod}\, n) = mx_2(\mathrm{mod}\, n)$

$\Rightarrow mx_1 = mx_2(\mathrm{mod}\, n)$

$\Rightarrow n$ divides $m(x_1 - x_2)$.

As m and n are co-prime, so n has to divide $(x_1 - x_2)$. Hence $x_1 = x_2$ in Z_n. This shows that f is one-one. Being a one-one map from a finite set to itself it is onto as well. Lastly to see that f is operation preserving we take x_1 and x_2 in Z_n.

Consider

$f(x_1 + x_2) = m(x_1 + x_2)(\mathrm{mod}\, n)$

$= (mx_1 + mx_2)(\text{mod}\, n)$

$= mx_1(\text{mod}\, n) + mx_2(\text{mod}\, n)$

$= f(x_1) + f(x_2)$

Hence we have $f \in Aut(Z_n)$.

Also $\phi(f) = f(1) = m(\text{mod}\, n) = m$.

Thus, ϕ is onto.

- *Operating Preserving:* Let $\alpha, \beta \in Aut(Z_n)$.

Consider $\phi(\alpha \circ \beta) = (\alpha \circ \beta)(1)$

$= \alpha(\beta(1))$

$= \alpha(\underbrace{1 + 1 + ... + 1}_{\beta(1)\ times})$

$= \underbrace{\alpha(1) + \alpha(1) + ... + \alpha(1)}_{\beta(1)\ times}$, as α is an automorphism.

$= \alpha(1)\beta(1) = \phi(\alpha)\phi(\beta)$.

Hence $Aut(Z_n) \approx U(n)$.

Example

Find $Aut(Z_6)$.

Solution: $Aut(Z_6) \approx U(6) = \{1, 5\}$ mod 6.

Thus, $Aut(Z_6)$ being a group of order 2 (prime) is cyclic and hence isomorphic to Z_2.

Applications of factor groups to Automorphism groups

In this section we study a theorem which connects the group of inner automorphisms to factor groups.

Theorem

"$G / Z(G) \approx Inn(G)$"

For any group G, $G / Z(G)$ is isomorphic to $Inn(G)$ where $Z(G)$ is the center of G.

Proof: Define a map $f: G/Z(G) \to Inn(G)$ as

$f(gZ(G)) = \phi_g$ for all $gZ(G) \in G/Z(G)$, where

$\phi_g : G \to G$ is $\phi_g(x) = gxg^{-1}$ for all x in G.

- *Well defined and one-one:*

$aZ(G) = bZ(G)$

$\Leftrightarrow a^{-1}b \in Z(G)$

$\Leftrightarrow (a^{-1}b)x = x(a^{-1}b) \forall x \in G$

$\Leftrightarrow bxb^{-1} = axa^{-1} \forall x \in G$

$\Leftrightarrow \phi_b \equiv \phi_a$

$\Leftrightarrow f(bZ(G)) = f(aZ(G))$

- *Onto:* Clearly for $\phi_g \in Inn(G)$, $gZ(G)$ is its pre-image under f.
- *Operation*-preserving: Let $aZ(G), bZ(G) \in G/Z(G)$.

Consider $f((aZ(G)))(bZ(G))) = f((ab)Z(G)) = \phi_{ab}$

$f(aZ(G))f(bZ(G)) = \phi_a\phi_b$.

Since we know $\phi_{ab} \equiv \phi_a\phi_b$ for all a and b in G, we have f is an isomorphism.

Characteristic Subgroups

Definition

"A subgroup N of a group G is called a *characteristic subgroup* if $\varphi(N) = N$ for all automorphisms φ of G".

Example

Every subgroup of the group of integers $(\mathbb{Z}, +)$ is a characteristic subgroup.

Let H be any subgroup of $(\mathbb{Z}, +)$. Then $H = m\mathbb{Z}$ for some m≥0.

Also, from Theorem 5.1 we know that $Aut(\mathbb{Z}) = \{I, \varphi\}$ where

$$I(n) = n \; \forall \; n \in \mathbb{Z}$$

and

$\varphi(n) = -n \; \forall \; n \in \mathbb{Z}$.

Clearly $I(H) = H$. Also,

$$\varphi(H) = \varphi(m\mathbb{Z}) = -m\mathbb{Z} = m\mathbb{Z} = H.$$

Hence H is a characteristic subgroup of $\mathbb{Z}$.

Example

Center of a group is a characteristic subgroup.

Let G be a group and Z(G) be its center.
Let $\varphi \in Aut(G)$
In order to prove that Z(G) is a characteristic subgroup of G, we need to show that $\varphi(Z(G)) \subseteq Z(G)$.
For this, let $y \in \varphi(Z(G))$. Then $y = \varphi(z)$ for some $z \in Z(G)$.
Let $g \in G$. As φ is onto, $g = \varphi(g')$ for some $g' \in G$.
Also as $z \in Z(G)$, $zg' = g'z$.
$\therefore \varphi(zg') = \varphi(g'z)$.
$or\ \varphi(z)\varphi(g') = \varphi(g')\varphi(z)$.
$or\ yg = gy$.
Hence $y \in Z(G)$.
Thus, Z(G) is a characteristic subgroup of G.

Theorem

Characteristic subgroups are normal

"Every characteristic subgroup N of a group G is normal in G ".

Proof: Let N be a characteristic subgroup of G. Then $\varphi(N) \subseteq N$ for all $\varphi \in Aut(G)$.
In particular, for $g \in G$ and $n \in N$ we have
$\varphi_g(N) \subseteq N$, where φ_g denotes the inner automorphism of G induced by g.
Thus, $gng^{-1} = \varphi_g(n) \in N$ and hence N is a normal subgroup of G.

Theorem

Characteristic property is transitive

"If N is a characteristic subgroup of K and K is a characteristic subgroup of G then N is a characteristic subgroup of G".

Proof: Let $\varphi \in Aut(G)$. As K is a characteristic subgroup of G, $\varphi(K) = K$ and hence $\tau = \varphi|_K$ is an automorphism of K. Since N is a characteristic subgroup of K, $\tau(N) = N$.
But $\tau(N) = \varphi(N)$. Hence N is invariant under all automorphisms of G. This concludes the proof. ■

Commutator Subgroup

Definition

"Let G be a group and $x, y \in G$. The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y".
If S denotes the set of all commutators of G then the subgroup of G generated by S is called the *commutator subgroup* of G and is denoted by G'.

Theorem

Commutator subgroup is a characteristic subgroup

"G' is a characteristic subgroup of G".

Proof: Let $\varphi \in Aut(G)$. We show that $\varphi(G') \subseteq G'$.

Observe that if c is a commutator in G then c= $x^{-1}y^{-1}xy$ for some x and y in G. As φ is an automorphism, $\varphi(c) = \varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)$. Thus, $\varphi(c)$ is also a commutator in G.

Now let $z \in G'$. Then $z = c_1c_2 \dots c_k$, where each c_i is a commutator in G.

$\therefore \varphi(z) = \varphi(c_1)\varphi(c_2)\dots\varphi(c_k)$, where each $\varphi(c_i)$ is a commutator as seen above.

$\therefore \varphi(z) \in G'$.

Hence G′ is a characteristic subgroup of G.

Corollary

(Commutator subgroup is a normal subgroup) As characteristic subgroups are normal, G′ is a normal subgroup of G. [It is easy to prove that commutator subgroup is normal using the definition of normal subgroups as well. We leave it as an exercise for the reader].

Theorem

The factor group G/G′

a) G/G′ is Abelian.

b) G′ is the smallest subgroup of G such that G/G′ is Abelian, i.e. if N is any subgroup of G such that G/N is Abelian then N≥G′.

Proof:

a) Let $x, y \in G$.

Now $G'xG'y = G'yG'x$

iff $G'xy = G'yx$

iff $(xy)(yx)^{-1} \in G'$

iff $xyx^{-1}y^{-1} \in G'$, which is true by definition of G′.

Hence, G/G′ is Abelian.

b) Let N be a subgroup of G such that G/N is Abelian.
Then for any $x, y \in G$, $NxNy = NyNx$.
i.e. $Nxy = Nyx$
i.e. $xyx^{-1}y^{-1} \in N$.
Thus N contains the set of all commutators of G. As G′ is the smallest subgroup of G containing the set of commutators, it follows that G' ⊆ N. ■

Corollary

G is Abelian iff G′= {e}.

Proof: Let G be Abelian and N= {e}.

Then G/N= G/{e} is Abelian. So, by above theorem G' ⊆ N = {e}. Also, {e} ⊆ G'. Hence G′={e}. Conversely, if G′={e} then G/G′= G/{e} is Abelian by above theorem. But, G/{e} ≅ G, so G is Abelian.

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Define Automorphism.
2. Define Inner Automorphism.
3. Define factor group.
4. Write about generator of a group.
5. Define Characteristic subgroup.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Prove that if G is a group, the Aut(G) is also a group.
2. Let G be a group and $g \in G$. Prove that Tg is an automorphism.
3. Prove that $Inn(G) \approx G/Z$.
4. Determine $Aut(Z_{10})$.
5. Prove that $Aut(Z_n) \approx U(n)$.
6. Let G be a group and let Z(G) be the centre of G. If G/Z(G) is cyclic , then prove that G is abelian.
7. For any group G, show that G/Z(G) is isomorphic to Inn(G).
8. Prove that every characteristic subgroup N of a group G is normal in G.
9. Show that characteristic property is transitive.
10. Prove that commutator subgroup is a characteristic subgroup.

UNIT-III

SYLLABUS

Properties of external direct products, the group of units modulo n as an external direct product, internal direct products, Fundamental Theorem of finite abelian groups.

EXTERNAL DIRECT PRODUCT

Definition

Let G and H be two groups. The **External Direct Product** of groups G and H, is given by $\{(g,h) | g \in G, h \in H\}$ and is denoted by $G \oplus H$.

The operation on this set is the component-wise operation as given below:

$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$, where $g_1, g_2 \in G$, $h_1, h_2 \in H$,

g_1g_2 is product of g_1 and g_2 as in G

and h_1h_2 is product of h_1 and h_2 as in H.

Result

$G \oplus H$ is a group where G and H are groups under the binary operation

$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ where $(g_1,h_1), (g_2,h_2) \in G \oplus H$.

Proof: As both G and H are groups, therefore both are non-empty. Let e_G, e_H denote the identity of G and H, respectively. Then $e = (e_G, e_H) \in G \oplus H$ and thus, $G \oplus H$ is non-empty.

Let $x = (g_1,h_1)$, $y = (g_2,h_2)$, $z = (g_3,h_3) \in G \oplus H$.

Closure: $xy = (g_1g_2, h_1h_2) \in G \oplus H$ as the group operations of G and H are well defined.

Associativity: $x(yz) = (g_1(g_2g_3), h_1(h_2h_3)) = ((g_1g_2)g_3), (h_1h_2)h_3) = (xy)z$.

This is so as associativity holds in G and H.

Existence of Identity: $\exists\, e = (e_G, e_H) \in G \oplus H$, such that $xe = ex = x$ for every $x \in G \oplus H$. This happens as e_G, e_H are the identity of G and H respectively.

Existence of Inverse: For every $x = (g,h) \in G \oplus H$, such that $xa = ax = e$ where $e = (e_G, e_H) \in G \oplus H$ and $g^{-1} \in G$ and $h^{-1} \in H$ denotes the inverse of $g \in G$ and $h \in H$ respectively.

Thus, $G \oplus H$ is a group.

Result

Let G, H be finite groups and let $(g,h) \in G \oplus H$. Then $o(g,h) = lcm\{o(g), o(h)\}$

Proof: Let $o(g, h) = t$ and $LCM\{o(g), o(h)\} = s$.

We show $t \mid s$ and $s \mid t$, as it gives $t = s$.

It is known that the order of an element 'a' of a group is defined as the least positive integer n such that $a^n = e$. Further, $a^m = e$ for some $m \in \mathbb{N}$ iff $n \mid m$.

Since, $o(g, h) = t$. Therefore, $(g,h)^t = (e_G, e_H)$, that is $(g^t, h^t) = (e_G, e_H)$.

Thus, $g^t = e_G$ and $h^t = e_H$. Thereby, we get $o(g) \mid t$, $o(h) \mid t$ which gives $LCM\{o(g), o(h)\} \mid t$. So, $s \mid t$.

Now, $(g,h)^s = (g^s, h^s) = (e_G, e_H)$ since $LCM\{o(g), o(h)\} = s$ and $o(g) \mid s$, $o(h) \mid s$.

Thus, $t \mid s$ (as $o(g, h) = t$)

Example:

Find out the number of elements of order 5 in $Z_{25} \oplus Z_{10}$.

Let $(a,b) \in Z_{25} \oplus Z_{10}$ such that $o(a, b) = 5$ i.e. $LCM\{o(a), o(b)\} = 5$. The following cases arise:

Possible $o(a)$	Possible $o(b)$	No. of choices for a	No. of choices for b	No. of elements of form (a,b) with order 5
1	5	1	4	4
5	1	4	1	4
5	5	4	4	16

In total, there are 4 + 4 +16 = 24 elements with order 5.

We use the result that in a cyclic group of order k, if a natural number d is such that $d \mid k$, then the number of elements in the cyclic group with order d is $\phi(d)$.

As 5 | 25 and 5 | 10, and groups Z_{25} and Z_{10} are both cyclic groups, so the number of elements of order 5 in both the groups is $\phi(5) = 4$.

Result

Let G, H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if

$\gcd\{o(G), o(H)\} = 1$.

Proof: Let $G = < a >, H = < b >$ such that

$o(G) = o(a) = m,\ \ o(H) = o(b) = n,\ \ o(G \oplus H) = mn$.

Let $G \oplus H$ be cyclic group of order mn. Let $\gcd\{o(G), o(H)\} = t$ and $t \neq 1$.

Then, $o(a^{m/t}) = \dfrac{o(a)}{\gcd(m/t, m)} = \dfrac{m}{m/t} = t$ and similarly, $o(b^{n/t}) = t$.

Thus, $o(< (a^{m/t}, e_H) >) = o[(a^{m/t}, e_H)] = LCM\{o(a^{m/t}), o(e_H)\} = t$, and

$o(< (e_G, b^{n/t}) >) = o[(e_G, b^{n/t})] = LCM\{o(e_G), o(b^{n/t})\} = t$.

It is known that if a natural number d is such that $d \mid k$, where k is the order of a cyclic group, then there exists a unique cyclic group of order d.

But here, $G \oplus H$ is cyclic and $t \mid mn$ and there are two distinct cyclic groups of order t, which is a contradiction.

Thus, $t = 1$ (as with $t = 1$, these subgroups coincide).

Conversely, let $\gcd\{o(G), o(H)\} = 1$.

Consider element (a, b) of $G \oplus H$.

Then, $o(a,b) = LCM\{m,n\} = mn \qquad (\because \gcd\{m,n\} = 1)$.

Since $\exists (a,b) \in G \oplus H$ such that $o(a,b) = mn$, so $G \oplus H$ is cyclic.

Result

The groups G and H are abelian if and only if their external direct product $G \oplus H$ is abelian.

Proof: Let group G and H be abelian. Let $x = (m, n)$, $y = (g,h) \in G \oplus H$.

Then $xy = (mg, nh) = (gm, hn) = yx$ (as G and H are abelian).

Thus, $G \oplus H$ is abelian.

Conversely, let $G \oplus H$ be abelian.

Let $a,b \in G; c,d \in H$.

So, $x = (a,c), y = (b,d) \in G \oplus H$.

Since $xy = yx$ which gives $ab = ba$ and $cd = dc$, that is, G and H are abelian.

GROUP $U(n)$ AND EXTERNAL DIRECT PRODUCT

We know that group $U(n)$ consists of natural numbers less than n which are co-prime to n under group operation of multiplication modulo n, that is, $U(n)=\{x\in\{1,2,\ldots,n\}\mid \gcd(x,n)=1\}$.

Let us take n = 18, then $U(18)$ = {1, 5, 7, 11, 13, 17}. But one can notice that {1, 7, 13} is a subgroup of $U(18)$ and all the elements of this subgroup are congruent to 1(mod 3). This can be generalized as follows:

Consider group $U(n)$. Let k be a natural number such that $k \mid n$.

Then define the set $U_k(n)=\{x\in U(n)\mid x\equiv 1(\mathrm{mod}\,k)\}=\{x\in U(n)\mid k\mid x-1\}$

In terms of terminology introduced below, the group {1, 7, 13} mentioned above is $U_3(18)$.

Clearly, $U_k(n)$ is non-empty as $1\in U_k(n)$.

Further, it can be observed that $U_k(n)$ is a subgroup of $U(n)$.

As $U(n)$ is a finite group and $U_k(n)$ is its subset, thus we only check closure with respect to multiplication modulo n in $U_k(n)$ as done below:

Let $a,b\in U_k(n)$. This gives $a, b\in U(n)$ and $a\equiv 1(\mathrm{mod}\,k)$, $b\equiv 1(\mathrm{mod}\,k)$.

Claim: $ab(\mathrm{mod}\,n)\in U_k(n)$ (since the operation is multiplication modulo n)

Using Division Algorithm, $ab=nq+r$ for some integer q and $0\le r<n$.

So, $n|(ab-r)$ and $k|n$ which gives $k|(ab-r)$ (*)

and $r=ab(\mathrm{mod}\,n)$

We show $r\in U(n)$ and $r\equiv 1(\mathrm{mod}\,k)$

As $U(n)$ is a group, thus, $r\in U(n)$.

Also since $a, b\in U_k(n)$, we get $a=1+kp$ and $b=1+kq$ for some integers p and q and thus, $ab=1+k(p+q+kpq)$.

So, $ab\equiv 1(\mathrm{mod}\,k)$.

Therefore, $k|(ab-1)$.

Using (*) and above relation, $k|(r-1)$ i.e. $r\equiv 1(\mathrm{mod}\,k)$.

Hence, $U_k(n)$ is a subgroup of $U(n)$.

Now, we attempt to write the $U(n)$ group as an external direct product of some U-groups. In this direction, we have the following result.

Result

Let s and t be natural numbers such that gcd(s, t) = 1, then

$$U(st)\approx U(s)\oplus U(t).$$

Proof: Define $\phi : U(st) \to U(s) \oplus U(t)$

as $\phi(x) = (x(\mathrm{mod}\, s), x(\mathrm{mod}\, t))$

Map is well-defined:

It may be observed that $x(\mathrm{mod}\, s) \in \{0,1,\ldots,s-1\}$. But $x(\mathrm{mod}\, s)$ can't be 0 as in that case, x will be a multiple of s which implies gcd(x, st) ≠ 1 i.e. $x \notin U(st)$. So, $x(\mathrm{mod}\, s) \in \{1,\ldots,s-1\}$. Similarly, $x(\mathrm{mod}\, t) \in \{1,\ldots,t-1\}$.

Let $x = y$. Since mod operation is well-defined, $x(\mathrm{mod}\, s) = y(\mathrm{mod}\, s)$ and $x(\mathrm{mod}\, t) = y(\mathrm{mod}\, t)$.

Map preserves operation:

Let $x, y \in U(st)$.

Claim: $\phi(x * y) = \phi(x)\phi(y)$

i.e., $((x * y)(\mathrm{mod}\, s),\ (x * y)(\mathrm{mod}\, t)) = ((x(\mathrm{mod}\, s)y(\mathrm{mod}\, s))\,\mathrm{mod}\, s,\ (x(\mathrm{mod}\, t)y(\mathrm{mod}\, t))\,\mathrm{mod}\, t)$

i.e., $(x * y)(\mathrm{mod}\, s) = [x(\mathrm{mod}\, s)y(\mathrm{mod}\, s)]\,\mathrm{mod}\, s$, and $(x * y)(\mathrm{mod}\, t) = [x(\mathrm{mod}\, t)y(\mathrm{mod}\, t)]\,\mathrm{mod}\, t$

where * is multiplication *mod st* operation.

We first show: $(x * y)(\mathrm{mod}\, s) = [x(\mathrm{mod}\, s)y(\mathrm{mod}\, s)]\,\mathrm{mod}\, s$

Let $x(\mathrm{mod}\, s) = b, y(\mathrm{mod}\, s) = c$.

Thus, $x = sq_1 + b$, $y = sq_2 + c$ for some integers q_1 and q_2.

So, $xy = bc + s(q_1 + q_2 + sq_1q_2)$

Using Division Algorithm, $xy = st.q + r$ for some integers q and r where $0 \le r < st$.

So, $(x * y) = r$.

Equating the two expressions of xy, we get $st.q + r = bc + s(q_1 + q_2 + sq_1q_2)$

Thus, $(x * y)\,\mathrm{mod}\, s = r(\mathrm{mod}\, s) = bc(\mathrm{mod}\, s) = [x(\mathrm{mod}\, s)y(\mathrm{mod}\, s)]\,\mathrm{mod}\, s$

Similarly, it can be shown that

$(x * y)(\mathrm{mod}\, t) = [x(\mathrm{mod}\, t)y(\mathrm{mod}\, t)]\,\mathrm{mod}\, t$.

Map is one-one:

Let $x \in Ker(\phi)$. Then $\phi(x) = (1, 1)$

i.e., $(x(\mathrm{mod}\, s), x(\mathrm{mod}\, t)) = (1, 1)$

Thus, $x - 1 = sq_1 = tq_2$ for some integers q_1 and q_2.

As, $s \mid sq_1$, so using above relation, we get $s \mid tq_2$.

Since $\gcd(s,t) = 1$, therefore, $s \mid q_2$ and $q_2 = sz$ for some integer z.

Thus, $x - 1 = stz$ which implies $x \equiv 1(\mathrm{mod}\, st)$ i.e. ϕ is one-one.

Map is onto:

It is known that order of group $U(n)$ is $\varphi(n)$ and $\varphi(st)=\varphi(s)\varphi(t)$ if gcd(s,t) = 1.

Thus, $|U(st)|=\varphi(st)=\varphi(s)\varphi(t)=|U(s)||U(t)|=|U(s)\oplus U(t)|$

As ϕ is a one-one map such that its domain and co-domain have same orders, thus the map ϕ is onto as well.

Lemma:

If $a\equiv b(\mathrm{mod}\, c)$, then $\gcd(a,c)=\gcd(b,c)$.

Result

Let s and t be natural numbers such that gcd(s, t) = 1, then

$$U_t(st)\approx U(s)$$

Proof: Define $\phi: U_t(st)\to U(s)$

as $\phi(x)=x(\mathrm{mod}\, s)$

Map is well-defined:

It may be observed that if $x\in U_t(st)$, then $x\in U(st)$

and $t\,|\,x-1$ and $x(\mathrm{mod}\, s)\in\{0,1,\ldots,s-1\}$.

As done in proof of previous result, $x(\mathrm{mod}\, s)\in\{1,\ldots,s-1\}$.

Let $x = y$. Since mod operation is well-defined, $x(\mathrm{mod}\, s)=y(\mathrm{mod}\, s)$.

Map preserves operation:

Let $x, y\in U_t(st)$.

Claim: $\phi(x*y)=\phi(x)\phi(y)$

i.e., $(x*y)(\mathrm{mod}\, s)=[x(\mathrm{mod}\, s)y(\mathrm{mod}\, s)]\mathrm{mod}\, s$ where * is multiplication *mod st* operation.

Let $x(\mathrm{mod}\, s)=b, y(\mathrm{mod}\, s)=c$.

Thus, $x=sq_1+b$, $y=sq_2+c$ for some integers q_1 and q_2.

So, $xy=bc+s(q_1+q_2+sq_1q_2)$

Using Division Algorithm, $xy=st.q+r$ for some integers q and r where $0\le r<st$.

So, $(x*y)=r$.

Equating the two expressions of xy, we get $st.q+r=bc+s(q_1+q_2+sq_1q_2)$.

Thus, $(x*y)\,\mathrm{mod}\, s=r(\mathrm{mod}\, s)=bc(\mathrm{mod}\, s)=[x(\mathrm{mod}\, s)y(\mathrm{mod}\, s)]\mathrm{mod}\, s$.

Map is one-one:

Let $x\in Ker(\phi)$. Then $\phi(x)=1$ i.e. $x(\mathrm{mod}\, s)=1$ and since $x\in U_t(st)$, then $t\,|\,x-1$.

Thus, $x-1=sq_1=tq_2$ for some integers q_1 and q_2.

As, $s\,|\,sq_1$, so using above relation, we get $s\,|\,tq_2$.

Since $\gcd(s,t)=1$, therefore, $s\,|\,q_2$ and $q_2=sz$ for some integer z.

Thus, $x-1=stz$ which gives $x\equiv 1(\mathrm{mod}\, st)$ i.e. ϕ is one-one.

Map is onto:

Let $y \in U(s)$.

Claim: $\exists\ x \in U_t(st)$ such that $x \pmod{s} = y$.

i.e. $\exists\ x \in U(st)$ such that $x \equiv 1 \pmod{t}$ and $x \equiv y \pmod{s}$.

As $\gcd(s,t) = 1$, using Chinese Remainder Theorem, $\exists\ x \pmod{st}$ such that $x \equiv 1 \pmod{t}$ and $x \equiv y \pmod{s}$

It only remains to show that $\gcd(x, st) = 1$ which will give $x \in U(st)$.

Since $y \in U(s)$, thus $\gcd(y, s) = 1$ and also $x \equiv y \pmod{s}$, therefore, $\gcd(x, s) = 1$. (using Lemma)

Also, since $\gcd(1, t) = 1$ and $x \equiv 1 \pmod{t}$, by using above Lemma, $\gcd(x, t) = 1$.

If $\gcd(x, st) \neq 1$, then $\exists$ prime p such that $p \mid \gcd(x, st)$. Then $p \mid x$ and $p \mid st$

i.e. $p \mid x$ and ($p \mid s$ or $p \mid t$)

i.e. ($p \mid x$ and $p \mid s$) or ($p \mid x$ and $p \mid t$)

i.e. $\gcd(x, s) \neq 1$ or $\gcd(x, t) \neq 1$ which is a contradiction.

Thus, $\gcd(x, st) = 1$.

INTERNAL DIRECT PRODUCT

Definition

Let G be a group and let H, K be normal subgroups of G. Then G is **Internal Direct Product** of H and K (denoted by $G = H \times K$) if $G = HK$ and $H \cap K = \{e\}$

Example:

$\mathbf{R}^*$ denotes the abelian group of non-zero real numbers under multiplication.

Let H be the subgroup containing all positive real numbers

and $K = \{-1, 1\}$.

Then H and K are normal subgroups of $\mathbf{R}^*$.

Clearly, $H \cap K = \{e\}$.

Then for each $0 \neq r \in R$, we have

$$r = \begin{cases} 1.r & ;\ r > 0 \\ (-1).(-r) & ;\ r < 0 \end{cases}$$

Then $\boldsymbol{R}^* = H \times K$.

Definition

Internal direct product of *n* normal subgroups of group

Let $H_1, H_2, ..., H_n$ be a finite collection of normal subgroups of group G. Then G is Internal Direct Product of $H_1, H_2, ..., H_n$ (denoted by $G = H_1 \times H_2 \times ... \times H_n$) if

(i) $G = H_1 H_2 ... H_n$,

(ii) $H_1 H_2 ... H_i \cap H_{i+1} = \{e\} \quad \forall\, i = 1, 2, ..., n-1$

Lemma

If G is Internal Direct Product of its normal subgroups $H_1, H_2, ..., H_n$, then for $1 \le i, j \le n, i \ne j$, $H_i \cap H_j = \{e\}$.

Proof: Let $x \in H_i \cap H_j$ for $1 \le i,\ j \le n,\ i \ne j$.

Without Loss Of Generality, let $i < j$.

Then $x \in H_j$ and $x \in H_1 H_2 ..... H_{j-1}$ as $x = e...e.x.e..e$.

So, $x \in H_1 H_2 ..... H_{j-1} \cap H_j = \{e\}$. Thus, $x = e$.

As $x \in H_i \cap H_j$ for $1 \le i, j \le n, i \ne j$ is arbitrary, therefore $H_i \cap H_j = \{e\}$.

Lemma

If G is Internal Direct Product of its normal subgroups $H_1, H_2, ..., H_n$, and if $h_i \in H_i$ for $1 \le i \le n$, then $h_i h_j = h_j h_i$ for $1 \le i, j \le n, i \ne j$.

Proof: Let $1 \le i, j \le n, i \ne j$. Consider $x = h_i h_j h_i^{-1} h_j^{-1}$

Then using the fact that $H_j \lhd G$, we get $x = h_i h_j h_i^{-1} h_j^{-1} = \left(h_i h_j h_i^{-1}\right) h_j^{-1} \in H_j$

Similarly, since $H_i \lhd G$, we get $x = h_i h_j h_i^{-1} h_j^{-1} = h_i \left(h_j h_i^{-1} h_j^{-1}\right) \in H_i$

$H_i \cap H_j = \{e\}$, so $x = e$, i.e. $h_i h_j = h_j h_i$

Fundamental Theorem Of Finite Abelian Groups

Fundamental theorem of finite abelian groups states the following:

"If G is a finite abelian group, then G can be expressed as a direct product of cyclic groups of prime-power order. Further, the factorization is unique except for the rearrangement of factors."

Lemma

Let G be a finite abelian group of prime-power order. Let $a \in G$ be an element of maximal order. Then $G = \langle a \rangle \times K$ for some $K \le G$.

Proof: Let $|G| = p^n$ where p is a prime and n is a natural number. We prove the result by induction on n.

For $n = 1$, $|G| = p$ (prime). As every group of prime order is cyclic and $a \in G$ is an element of maximal order, therefore, $G = < a >$ and $G = < a > \times \{e\}$.

Induction hypothesis: Assume that the result is true for abelian groups of order p^k where $k < n$.

Now we prove for n:

Let $a \in G$ be an element of maximal order p^m (as $a \in G$, $o(a) | o(G)$)

Let $x \in G$. Then $o(x) | o(G)$ (by corollary to Lagrange's Theorem) and thus, $o(x) = p^t$ for some natural number t. But the maximal order is p^m, so $t \le m$ and $p^t | p^m$.

Thus, $x^{p^m} = e$.

As $x \in G$ was arbitrary, thus $\forall x \in G, x^{p^m} = e$.

If $G = < a >$, then $G = < a > \times \{e\}$ and we are done.

Assume $G \neq < a >$. Choose $b \in G$ of smallest possible order such that $b \notin < a >$. Clearly, $b \neq e$.

Claim 1: $o(b) = p$

Since $b \in G$ and $b \neq e$. Thus, $o(b) = p^\alpha$ where $0 < \alpha \le m$ and, therefore, $\gcd(p, p^\alpha) = p$

Consider, $o(b^p) = \dfrac{o(b)}{\gcd(p, o(b))}$

$= \dfrac{o(b)}{p}$

Thus, $o(b^p) < o(b)$.

But b is element of smallest order such that $b \notin < a >$, thus $b^p \in < a >$.

Let $b^p = a^i$ for some integer i.

Then, $e = b^{p^m}$ (because $\forall x \in G, x^{p^m} = e$)

Note, $e = b^{p^m} = b^{p.p^{m-1}} = \left(b^p\right)^{p^{m-1}} = \left(a^i\right)^{p^{m-1}}$

So, $o(a^i) \le p^{m-1}$

Thus, a^i is not a generator of $< a >$ (as $o(a) = p^m$) and therefore, $\gcd(i, p^m) \neq 1$

It gives us that $i = pt$ for some t and $b^p = a^i = a^{pt}$.

Define $c = a^{-t} b$

If $c \in < a >$, then $c = a^s$, and therefore, $b = a^{t+s} \in < a >$, which is a contradiction.

Thus, $c \notin < a >$.

Observe that using that G is an abelian group, $c^p = a^{-ps} b^p = b^{-p} b^p = e$

Thus, $o(c) \mid p$ (p prime), and therefore, $o(c) = 1 \text{ or } p$

If $o(c) = 1$, then $c = e$ which gives $c \in < a >$, a contradiction.

Therefore, $o(c) = p$.

Thus, $\exists$ element, viz., c of smallest possible order 'p' such that $c \notin < a >$.

Also, b is element of smallest possible order such that $b \notin < a >$.

Thus, $o(b) = p$.

Claim 2: $< a > \cap < b > = \{e\}$.

Clearly, $< a > \cap < b > \subseteq < b >$

Therefore, $o(< a > \cap < b >) \mid o(< b >)$ (using Lagrange's Theorem)

i.e. $o(< a > \cap < b >) \mid p$ $[\because o(b) = o(< b >) = p]$

If $o(< a > \cap < b >) = p$, then it together with $< a > \cap < b > \subseteq < b >$ gives us that $< a > \cap < b > = < b >$ i.e. $< b > \subseteq < a >$ and thus, $b \in < a >$, which is a contradiction.

So, $o(< a > \cap < b >) = 1$ and $< a > \cap < b > = \{e\}$.

We show existence of K:

Define $\overline{G} = \dfrac{G}{< b >}$.

Let $\overline{x} \in \overline{G}$. Then $\overline{x} = x < b >$ for some $x \in G$.

Consider $\overline{a} = a < b >$.

If $o(\overline{a}) < o(a) = p^m$, then $o(\overline{a}) \le p^{m-1}$ i.e. $\overline{a}^{p^{m-1}} = \overline{e} = < b >$.

which gives $(a < b >)^{p^{m-1}} = < b >$ and therefore, $a^{p^{m-1}} < b > = < b >$ i.e. $a^{p^{m-1}} \in < b >$

Clearly, $a^{p^{m-1}} \in < a >$.

So, $a^{p^{m-1}} \in < a > \cap < b >$ but $< a > \cap < b > = \{e\}$.

Thus, $a^{p^{m-1}} = e$, which is a contradiction as $o(a) = p^m$.

Hence, $o(\overline{a}) = o(a) = p^m$ $[\because o(\overline{a}) \mid o(a)]$

Claim 3: $\bar{a}$ is element of maximal order of $\overline{G}$.

Let, if possible, $\exists\, \bar{t} \in \overline{G} : o(\bar{t}) > p^m$ that is $o(\bar{t}) = p^\alpha$ where $m+1 \le \alpha < n$

As $\bar{t} \in \overline{G}$, therefore, $\bar{t} = t < b >$ for some $t \in G$.

Since, $o(\bar{t}) = p^\alpha$, therefore, $\bar{t}^{p^\alpha} = \bar{e}$ i.e. $(t < b >)^{p^\alpha} = < b >$.

So, $t^{p^\alpha} < b > = < b >$ which gives $t^{p^\alpha} \in < b >$

As $< b >$ is a group of order p (because $o(b) = p$), therefore all the non-identity elements of $< b >$ will have order p.

If $t^{p^\alpha} = e$, then $p^\alpha = o(\bar{t}) \le o(t) \le p^\alpha$, so $o(t) = p^\alpha$.

This is a contradiction as the maximal order of an element of G is p^m and $m+1 \le \alpha < n$.

Thus, $t^{p^\alpha} \ne e$ and $o(t^{p^\alpha}) = p$

But $o(t^{p^\alpha}) = \dfrac{o(t)}{\gcd(o(t), p^\alpha)} = p$

Therefore, $o(t) = p \times \gcd(o(t), p^\alpha)$

Let $o(t) = p^q$ for some q (as $t \in G$ and $|G| = p^n$)

Since, $o(\bar{t}) \mid o(t)$ and $o(\bar{t}) = p^\alpha$ therefore, $\alpha \le q$.

Using $o(t) = p \times \gcd(o(t), p^\alpha)$ and $\alpha \le q$, we get $o(t) = p \times p^\alpha = p^{\alpha+1} > p^m$.

This is a contradiction as the maximal order of an element of G is p^m

Thus, the maximal possible order of an element in $\overline{G}$ is p^m, $\bar{a}$ is element of maximal order of $\overline{G}$ and claim 3 holds.

As $\bar{a}$ is element of maximal order of $\overline{G}$, thus, by induction hypothesis, $\overline{G} = < \bar{a} > \times \overline{K}$ for some subgroup $\overline{K}$ of $\overline{G}$ i.e. $\overline{G} = < \bar{a} > \overline{K}$, and $< \bar{a} > \cap \overline{K} = \{e\}$.

Let $K = \left\{ x \in G \,\middle|\, \bar{x} = x < b > \in \overline{K} \right\}$

Claim 4: $< a > \cap K = \{e\}$

Let $x \in < a > \cap K$.

Then $x \in < a >$ and $x \in K$ which gives, $\bar{x} \in \overline{K}$ and $x = a^j$ for some integer j.

i.e. $x<b>=a^j<b>$

i.e. $x<b>=(a<b>)^j$

i.e. $\bar{x}=x<b>=\bar{a}^j\in<\bar{a}>$

Hence, $\bar{x}\in\overline{K}\cap<\bar{a}>=\{\bar{e}\}=\{<b>\}$

i.e. $x<b>=<b>$ which gives $x\in<b>$

But $x\in<a>$. Thus, $x\in<a>\cap<b>=\{e\}$

Hence, $<a>\cap K=\{e\}$.

Claim 5: $K\le G:<b>\subseteq K$ and $\overline{K}=\frac{K}{<b>}$

Clearly, K is non-empty as $e\in K$.

Further, if $x,y\in K$, then $x<b>,y<b>\in\overline{K}$.

As $\overline{K}\le\overline{G}$, $(x<b>)(y<b>)^{-1}\in\overline{K}$ i.e. $(xy^{-1})<b>\in\overline{K}$.

So, $xy^{-1}\in K$ which gives $K\le G$.

Also, for all integers t, $b^t<b>=<b>\in\overline{K}$. (as $<b>$ is identity of $\overline{K}$)

Thus, $<b>\subseteq K$

In order to show that $\overline{K}=\frac{K}{<b>}$, consider $\bar{x}\in\overline{K}$

Then $\bar{x}=x<b>$ for some $x\in G$ and using the definition of K, we get $x\in K$.

This gives $\bar{x}=x<b>\in\frac{K}{<b>}$. So, $\overline{K}\subseteq\frac{K}{<b>}$

Now, let $x<b>\in\frac{K}{<b>}$. Thus, $x\in K$ and so, $\bar{x}=x<b>\in\overline{K}$.

Hence, $\frac{K}{<b>}\subseteq\overline{K}$. Combining, we get $\overline{K}=\frac{K}{<b>}$.

Claim 6: $G=<a>K$

Let $y\in G$. Then, $y<b>\in\overline{G}=<\bar{a}>\overline{K}$

i.e. $y<b>=\bar{a}^j\bar{k}$ for some integer j and $\bar{k}\in\overline{K}$.

i.e. $y < b >= a^j k < b >$

i.e. $y(a^j k)^{-1} \in < b > \subseteq K$

i.e. $y = a^j k k'$ for some $k' \in K$

Hence, $y \in < a > K$

Thus, $G = < a > K$ and using claim 4, we get $G = < a > \times K$.

Theorem

(Fundamental theorem of finite abelian groups) If G is a finite abelian group, then G can be expressed as a direct product of cyclic groups of prime-power order. Further, the factorization is unique except for the rearrangement of factors.

Proof: Let G be an abelian group such that $|G| = p_1^{n_1} p_2^{n_2} \ldots\ldots p_k^{n_k}$ where p_i s are distinct primes.

Define for all $i = 1, 2, \ldots., k$, $G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$.

Using induction on k and applying Lemma 6.1, we get that $G(p_i)$ is an abelian subgroup of G with $|G(p_i)| = p_i^{n_i}$ and $G = G(p_1) \times G(p_2) \times \ldots\ldots \times G(p_k)$. These $G(p_i)$ are uniquely determined.

Since each $G(p_i)$ is an abelian group with $|G(p_i)| = p_i^{n_i}$ i.e. $G(p_i)$ is of prime power order and thus, applying Lemma 6.3 on $G(p_i)$, we get that $G(p_i)$ is expressible as an Internal Direct Product of cyclic subgroups which will be again of prime power order being subgroups of $G(p_i)$ which is of prime power order (using Lagrange's Theorem). Further since $G = G(p_1) \times G(p_2) \times \ldots\ldots \times G(p_k)$, and $G(p_i)$ is expressible as an Internal Direct Product of cyclic subgroups, then G is expressible as an Internal Direct Product of its cyclic subgroups.

In order to prove Fundamental Theorem, it is sufficient to show that uniqueness (upto isomorphism and rearrangement) of factors of $G(p_i)$.

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Define external direct product.
2. Define internal direct product.
3. Write the statement of fundamental theorem of finite abelian groups.
4. Write an example for external direct product.
5. Write an example for internal direct product.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Prove that the order of an element of a direct product of a finite number of finite group is the least common multiple of the orders of the components of the element.
2. Let G and H be the finite cyclic groups. Then prove that $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.
3. Find out the number of elements of order 5 in $Z_{25} \oplus Z_{10}$.
4. Let s and t be natural numbers such that cd(s, t)= 1, then prove that $U(t) \approx U(s) \oplus U(t)$.
5. If G is the internal direct product of its normal subgroups $H_1, H_2, \ldots, H_n$ then prove that $G \approx H_1 \oplus H_2 \oplus \ldots \oplus H_n$.
6. If G is an internal direct product of its normal subgroups $H_1, H_2, \ldots, H_n$, then prove that every element of G can be uniquely expressed as $h_1 h_2 \ldots h_n$ where $h_i \in H_i$ for $1 \leq i \leq n$.
7. Let G be a finite abelian group of order $p^n m$ where p is a prime that does not divide m. Then prove that G=H x K. Moreover $|H| = p^n$.
8. Let G be an abelian group of prime –power order and let a be an element of maximal order in G. Prove that = $< a >$ x K for some $K \leq G$.
9. Show that a finite abelian group of prime –power order is an internal direct product of cyclic groups.
10. State and prove the fundamental theorem of finite abelian groups.

UNIT-IV

SYLLABUS

Group actions, stabilizers and kernels, permutation representation associated with a given group action, Applications of group actions: Generalized Cayley's theorem, Index theorem.

group action

Definition

Let G be a group with identity element e and S be any set. Then a ***action of G on S*** is a map

$$G \times S \mapsto S \quad \text{defined by}$$
$$(g,s) \mapsto g.s \in S, \quad s \in S \text{ and } g \in G$$

satisfying following conditions:

1. $g_1.(g_2.s) = (g_1g_2).s, \quad g_1, g_2 \in G$ and $s \in S$.
2. $e.s = s, \quad s \in S$.

Example

Let G be a group with identity element e and S be any non-empty set. Define a map $G \times S \mapsto S$ as

$$g.s = s, \quad g \in G \text{ and } s \in S.$$

Then, we have

1. $g_1.(g_2.s) = (g_1g_2).s$
   $= s, \quad g_1, g_2 \in G$ and $s \in S$.
2. $e.s = s, \quad s \in S$.

Thus G is acting on S.

The action defined in Example 1.2 of any group on a non-empty set is refer to as ***trivial action***.

Example

Let G be a group with identity element e and $S = G$. Define a map $G \times S \mapsto S$ as

$g.s = gs$, $g \in G$ and $s \in S = G$.

Then we have

1. $g_1.(g_2.s) = g_1.(g_2s)$
   $= (g_1g_2).s, \quad g_1, g_2, s \in G$.
2. $e.s = es$
   $= s, \quad s \in G$.

Thus G acts on itself by left multiplication.

The action defined in Example
of any group on to itself is refer to as ***left regular action***.

Example

Let G a group with identity element e and $S = G$. Define a map
$G \times S \mapsto S$ as
$g.s = gsg^{-1},\ g,\ s \in G$.

Then we have

1. $g_1.(g_2.s) = g_1.(g_2 s g_2^{-1})$
$= (g_1 g_2)s(g_2^{-1} g_1^{-1})$
$= (g_1 g_2)s(g_1 g_2)^{-1}$
$= (g_1 g_2).s,\ \ g_1,\ g_2,\ s \in G.$
2. $e.s = ese^{-1}$
$= s,\ \ s \in S.$

Thus group G acts on itself.
The action defined in Example

of any group on to itself is refer to as ***conjugation***.

Proposition

Let G be a group with identity element e, S be a set and suppose that G acts on S. Then for each $g \in G$, the map $\sigma_g: S \to S$ defined by

$$\sigma_g(s) = g.s,\ \ g \in G \text{ and } s \in S$$

is a permutation on S.

Proof. In order to show that $\sigma_g: S \to S$ is a permutation it suffices to show that σ_g is a bijection. Suppose that $\sigma_g(s_1) = \sigma_g(s_2)$, where $s_1,\ s_2 \in S$

$$\Rightarrow g.s_1 = g.s_2$$
$$\Rightarrow g^{-1}(g.s_1) = g^{-1}(g.s_2)$$
$$\Rightarrow (g^{-1}g).s_1 = (g^{-1}g).s_2$$
$$\Rightarrow e.s_1 = e.s_2$$
$$\Rightarrow s_1 = s_2.$$

So σ_g is injective. Also for each $s \in S$, there exist $g^{-1}.s \in S$ such that

$$\sigma_g(g^{-1}.s) = g.(g^{-1}.s)$$
$$= e.s$$
$$= s.$$

Thus σ_g is onto. Hence σ_g is a permutation.

Let S be a finite set and $Sym(S)$ be the set of all permutations (bijections) of S. Then, we know that $Sym(S)$ is a group with respect to the operation composition of permutations (maps) and it is known as ***symmetric group*** *of S*.

If we take $S = \{1, 2, \cdots, n\}$, then $sym(S)$ is called symmetric group of order n and in this case we write $Sym(S) = S_n$.

Proposition

Let G be a group, S be a set and suppose that G acts on S. Then, the map

$\phi: G \to Sym(S)$ *defined by*

$$\phi(g) = \sigma_g, \quad g \in G$$

is a homomorphism.

Proof. Let $g_1, g_2 \in G$. Then for each $s \in S$

$$\begin{aligned}\phi(g_1g_2)(s) &= \sigma_{g_1g_2}(s)\\ &= (g_1g_2).s\\ &= g_1.(g_2.s)\\ &= \sigma_{g_1}(\sigma_{g_2}(s))\\ &= (\sigma_{g_1} \circ \sigma_{g_2})(s)\\ &= (\phi(g_1) \circ \phi(g_2))(s).\end{aligned}$$

Thus

$$\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2), \quad \text{for all } g_1, g_2 \in G.$$

Hence, ϕ is a homomorphism.

Definition

Let G be a group, S be a set and suppose that G acts on S. Then the homomorphism $\phi : G \to Sym(S)$ defined by $\phi(g) = \sigma_g$, $g \in G$ is known as ***permutation representation associated to the given action.***

Proposition

Let G be a group with the identity element e, S be a set and suppose that G acts on S. If $\phi : G \to Sym(S)$ is a homomorphism, then the map

$$G \times S \mapsto S \text{ defined by}$$

$$g.s = \phi(g)(s), \ g \in G \text{ and } s \in S$$

is a action of G on S.

Proof. As $\phi : G \to Sym(S)$ is a homomorphism, therefore

$$\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2), \ g_1, g_2 \in G.$$

Then, for $g_1, g_2 \in G$ and $s \in S$, we have

$$\begin{aligned}g_1.(g_2.s) &= \phi(g_1)(g_2.s)\\ &= \phi(g_1)(\phi(g_2)(s))\\ &= (\phi(g_1) \circ \phi(g_2))(s)\\ &= \phi(g_1g_2)(s)\\ &= (g_1g_2).s\ .\end{aligned}$$

Also, for each $s \in S$, we have

$$\begin{aligned}e.s &= \phi(e)(s)\\ &= I(s)\\ &= s.\end{aligned}$$

Thus, G acts on S.

Faithful action

Definition

Let G be a group, S be a set and suppose that G acts on S. Then the action of G on S is said to be ***faithful*** if every distinct element of group G induces the distinct permutation of S.

Example

Let G a group and $S = G$. Suppose G acts on to itself by left regular action. Then, for $g_1, g_2, s \in G$ such that $g_1 \neq g_2$, we have

$$\begin{aligned} & g_1 s \neq g_2 s \\ \Rightarrow\ & g_1.s \neq g_2.s \\ \Rightarrow\ & \sigma_{g_1}(s) \neq \sigma_{g_2}(s),\ s \in S \\ \Rightarrow\ & \sigma_{g_1} \neq \sigma_{g_2}. \end{aligned}$$

Thus left regular action is faithful.

Kernel of the action

Definition

Let G be a group, S be a set and suppose that G acts on S. Then, **the *kernel of the action*** of G on S is defined as

$$\{g \in G :\ g.s = s, \text{ for all } s \in S\}.$$

Next, we show that the kernel of action forms a subgroup of G.

Proposition

Let G be a group, S be a set and suppose G acts on S. Then kernel of action is a subgroup of G.

Proof. Let K be the kernel of action. As

$$\begin{aligned} & e.s = s, \text{ for all } s \in S \\ \Rightarrow\ & e \in K. \end{aligned}$$

Therefore K is non-empty. Let $k_1, k_2 \in K$ and $s \in S$, then

$$\begin{aligned} (k_1 k_2).s &= k_1.(k_2.s) \\ &= k_2.s \\ &= s. \\ \Rightarrow\ & k_1 k_2 \in K. \end{aligned}$$

Also, let $k \in K$ and $s \in S$, then

$$\begin{aligned} k^{-1}.s &= k^{-1}.(k.s) \\ &= (k^{-1}k).s \\ &= s. \\ \Rightarrow\ & k^{-1} \in K. \end{aligned}$$

Thus K is a subgroup of G.

We know that, if $\phi: G \to G'$ is a homomorphism then kernel of ϕ denoted as $ker\,\phi$ is defined as

$$ker\,\phi = \{g \in G:\ \phi(g) = e'\}.$$

It is easy to verify that kernel of a homomorphism is always a normal subgroup of G. In view of above definitions we have following observation:

Proposition

Let G be a group, S be a set and suppose that G acts on S and let $\phi : G \to Sym(S)$ be the permutation representation associated to the action then

$$kernel\ of\ action = ker\ \phi.$$

Proof.

$$\begin{aligned} ker\ \phi &= \{g \in G:\ \phi(g) = I\} \\ &= \{g \in G:\ \sigma_g = I\} \\ &= \{g \in G:\ \sigma_g(s) = I(s),\quad s \in S\} \\ &= \{g \in G:\ g.s = s,\quad s \in S\} \\ &= kernel\ of\ action. \end{aligned}$$

Stabilizer of group action

Definition

Let G be a group, S be a set and suppose that G acts on S. Then, for each $s \in S$, define the ***stabilizer*** *of* s *in* G denoted as G_s as

$$G_s = \{g \in G : g.s = s\}.$$

In the next result, we prove that if group G acts on the set S. Then, for each $s \in S$, stabilizer G_s of s is a subgroup of G.

Proposition

Let G be a group and S be a set. Suppose that G acts on S. Then, for each $s \in S$, the stabilizer G_s of s in G is a subgroup of G.

Proof. As $e.s = s$, for all $s \in S$, so $e \in G_s$. Therefore

$$G_s \neq \emptyset.$$

Let $x, y \in G_s$, then $x.s = s$ and $y.s = s$. So, we have

$$\begin{aligned} (xy).s &= x.(y.s) \\ &= x.s \\ &= s. \end{aligned}$$

$$\Rightarrow xy \in S.$$

Also for each $x \in G_s$,

$$\begin{aligned} x^{-1}.s &= x^{-1}.(x.s) \\ &= (x^{-1}x).s \\ &= e.s \\ &= s. \end{aligned}$$

$$\Rightarrow x^{-1} \in S.$$

Hence G_s is a subgroup of G.

Theorem

Let G be a group and S be a set. Suppose that G acts on S. Then, any two elements of G induce same permutation if and only if they are in the same coset of kernel of action.

Proof. Let K be the kernel of action and $\sigma_{g_1} = \sigma_{g_2}$ for some $g_1, g_2 \in G$. Then we have

$$\sigma_{g_1}(s) = \sigma_{g_2}(s), \text{ for all } s \in S$$
$$\Rightarrow g_1.s = g_2.s, \text{ for all } s \in S$$
$$\Rightarrow g_2^{-1}g_1.s = s, \text{ for all } s \in S$$
$$\Rightarrow g_2^{-1}g_1 \in K$$
$$\Rightarrow Kg_1 = Kg_2.$$

Conversely, let $g_1, g_2 \in Kg$. Then, we have

$$g^{-1}g_1 \in K \text{ and } g^{-1}g_2 \in K$$
$$\Rightarrow g_2^{-1}gg^{-1}g_1 \in K$$
$$\Rightarrow g_2^{-1}g_1 \in K$$
$$\Rightarrow (g_2^{-1}g_1).s = s \text{ for all } s \in S$$
$$\Rightarrow g_1.s = g_2.s \text{ for all } s \in S$$
$$\Rightarrow \sigma_{g_1}(s) = \sigma_{g_2}(s), \text{ for all } s \in S.$$

Thus, g_1 and g_2 induces same permutation.

Normalizer as a Special Case of Stabilizer

Let G be a group and S be a subset of G. Then ***normalizer*** of S in G denoted as $N_G(S)$ is defined by

$$\{g \in G : gS = Sg\}.$$

It is easy to verify that normalizer is a subgroup of G. In this section we show that normalizer is a special case of stabilizer.

Proposition

Let G be a group with identity element e and $P(G)$ be the set of all subsets of G. Then the map

$$G \times P(G) \mapsto P(G) \text{ defined by}$$
$$g.B = gBg^{-1}, \ g \in G \text{ and } B \in P(G)$$

is a action of G on $P(G)$. Further, for every $B \in P(G)$, $G_B = N_G(B)$, where G_B is the stabilizer of B in G.

Proof. For each $g_1, g_2 \in G$ and $B \in P(G)$, we have

$$\begin{aligned} g_1.(g_2.B) &= g_1.(g_2Bg_2^{-1}) \\ &= g_1(g_2Bg_2^{-1})g_1^{-1} \\ &= (g_1g_2)B(g_1g_2)^{-1} \\ &= (g_1g_2).B \ . \end{aligned}$$

Also

$$\begin{aligned} e.B &= eBe^{-1} \\ &= B, \quad \text{for all } B \in P(G). \end{aligned}$$

Thus G acts on $P(G)$. Further

$$\begin{aligned} G_B &= \{g \in G : g.B = B\} \\ &= \{g \in G : gBg^{-1} = B\} \\ &= \{g \in G : gB = Bg\} \\ &= N_G(B). \end{aligned}$$

stabilizer is a subgroup of G therefore, $N_G(B)$ is also a subgroup of G.

Centralizer as a Special Case of Stabilizer

Let G be a group and S be a subset of G. Then ***centralizer*** of S in G denoted as $C_G(S)$ is defined as

$$\{g \in G : gs = sg, \quad \text{for all} \quad s \in S\}.$$

It is easy to verify that centralizer is a subgroup of G. In this section, we show that centralizer is a special case of stabilizer.

Proposition

Let G be a group with identity element e and $N_G(S)$ be the normaliser of S in G. Then, a map

$$N_G(S) \times S \mapsto S \quad \text{defined as}$$
$$g.s = gsg^{-1}, \ g \in N_G(S) \quad \text{and } s \in S.$$

is a action of $N_G(S)$ on S. Further, kernel of action of $N_G(S)$ on S is same as the centralizer of S in G.

Proof. For each $g \in N_G(S)$, $gS = Sg$

$$\Rightarrow gsg^{-1} \in S, \quad \text{for all} \quad s \in S.$$

Therefore the map $N_G(S) \times S \mapsto S$ defined by

$$g.s = gsg^{-1}, \ g \in N_G(S) \quad \text{and } s \in S.$$

is well-defined. Also, for each $g_1, g_2 \in N_G(S)$ and $s \in S$, we have

$$\begin{aligned} g_1.(g_2.s) &= g_1.(g_2 s g_2^{-1}) \\ &= g_1(g_2 s g_2^{-1})g_1^{-1} \\ &= (g_1 g_2)s(g_1 g_2)^{-1} \\ &= (g_1 g_2).s \ . \end{aligned}$$

Also,

$$\begin{aligned} e.s &= ese^{-1} \\ &= s, \quad \text{for all } s \in S. \end{aligned}$$

Thus $N_G(S)$ acts on S. Further, if K be the kernel of action

$$\begin{aligned} K &= \{g \in G:\ g.s = s \quad \text{for all} \quad s \in S\} \\ &= \{g \in G:\ gsg^{-1} = s \quad \text{for all} \quad s \in S\} \\ &= \{g \in G:\ gs = sg \quad \text{for all} \quad s \in S\} \\ &= C_G(S). \end{aligned}$$

Furthermore, as kernel of action is a subgroup of G therefore

$$C_G(S) < N_G(S)$$

Also we know that $N_G(S)$ is a subgroup of G. Hence we have

$$C_G(S) < G.$$

Orbits

We begin this section by showing that if group G acts on a non-empty set S, then the action of G on S defines a equivalence relation on S.

Theorem

Let group G acts on a non-empty set S. Define a relation on S as

$s \sim t \quad \Leftrightarrow \quad s = g.t$ for some $g \in G$.

Then, '$\sim$' is an equivalence relation on S.

Further, for every $s \in S$, the number of elements in equivalence class of 's' is equal to the index of the stabilizer of 's' in G.

Proof. (Reflexivity) As G acts on S. Therefore

$$\begin{aligned} &e.s = s \quad \text{for all} \quad s \in S \\ \Rightarrow\ &s \sim s \quad \text{for all} \quad s \in S. \end{aligned}$$

(Symmetry) Let $s \sim t$. Then we have

$$s = g.t \quad \text{for some} \quad g \in G$$
$$\Rightarrow g^{-1}.s = g^{-1}.(g.t)$$
$$\Rightarrow g^{-1}.s = (g^{-1}g).t$$
$$\Rightarrow g^{-1}.s = e.t = t, \text{ where } g^{-1} \in G$$
$$\Rightarrow t \sim s.$$

(Transitivity) Let $s \sim t$ and $t \sim u$. Then we have

$$s = g_1.t \quad \text{and} \quad t = g_2.u \quad \text{for some} \quad g_1, g_2 \in G$$
$$\Rightarrow s = g_1.(g_2.u)$$
$$\Rightarrow s = (g_1 g_2).u, \text{ where } g_1 g_2 \in G$$
$$\Rightarrow s \sim u.$$

Thus, '$\sim$' is an equivalence relation on S.

Further, for every $s \in S$, let c_s be equivalence class of s in S, i.e,

$$c_s = \{\, g.s : g \in G \,\}.$$

Let G_s be the stabilizer of s in G, $i_G(G_s)$ be the index of G_s in G and $\left(\frac{G}{G_s}\right)_{left}$ be the set of all left cosets of G_s in G. Then, in order to show that $O(c_s) = i_G(G_s)$ it suffices to show that there exists a bijection between c_s and $\left(\frac{G}{G_s}\right)_{left}$.

Define a map $\psi: c_s \to \left(\frac{G}{G_s}\right)_{left}$ as

$$\psi(g.s) = gG_s, \quad g \in G.$$

Let $g_1, g_2 \in G$ such that

$$g_1.s = g_2.s$$
$$\Leftrightarrow g_2^{-1}.(g_1.s) = g_2^{-1}(g_2.s)$$
$$\Leftrightarrow (g_2^{-1}g_1).s = s$$
$$\Leftrightarrow g_2^{-1}g_1 \in G_s$$
$$\Leftrightarrow g_1 G_s = g_2 G_s$$
$$\Leftrightarrow \psi(g_1.s) = \psi(g_2.s).$$

Therefore, ψ is well-defined and injective. Also, for each $gG_s \in \left(\frac{G}{G_s}\right)_{left}$, there exist $g.s \in c_s$ such that

$$\psi(g.s) = gG_s.$$

Thus, ψ is surjective. Hence

$$O(c_s) = O\left(\left(\frac{G}{G_s}\right)_{left}\right)$$
$$= i_G(G_s).$$

Definition

Let group G acts on a non-empty set S. Define a relation on S as $s \sim t \Leftrightarrow s = g.t$ for some $g \in G$.

Then, '$\sim$' is an equivalence relation on S. The equivalence class of s in S

$$c_s = \{g.s : g \in G\}$$

is called the ***orbit*** *of* G containing s.

Definition

Let group G acts on a non-empty set S. Then the action of group G on S is said to be ***transitive*** if G has exactly one orbit.

Problem

Let G be a group, S be a non-empty set and suppose that G acts on S. Let $a, b \in S$ such that $b = g.a$ for some $g \in G$, then $G_b = g\,G_a g^{-1}$, where G_a and G_b are stabilizers of a and b respectively.

Solution. Let $a, b \in S$ such that $b = g.a$ for some $g \in G$ and $x \in G_b$. Then

$$\begin{aligned}(g^{-1}xg).a &= (g^{-1}x).(g.a)\\ &= g^{-1}(x.b)\\ &= g^{-1}.b\\ &= a.\end{aligned}$$

Therefore

$$\begin{aligned}&g^{-1}xg \in G_a \text{ for all } x \in G_b\\ \Rightarrow\ &x \in gG_a g^{-1} \text{ for all } x \in G_b\\ \Rightarrow\ &G_b \subseteq gG_a g^{-1}.\end{aligned}$$

Conversely, let $x \in gG_a g^{-1}$

$$\begin{aligned}&\Rightarrow (g^{-1}xg).a = a\\ &\Rightarrow (g^{-1}x).b = a\\ &\Rightarrow g.\big((g^{-1}x).b\big) = g.a\\ &\Rightarrow x.b = g.a\\ &\Rightarrow x.b = b\end{aligned}$$

Therefore

$$\begin{aligned}&\Rightarrow x \in G_b \text{ for all } x \in gG_a g^{-1}\\ &\Rightarrow gG_a g^{-1} \subseteq G_b.\end{aligned}$$

Thus

$$gG_a g^{-1} \subseteq G_b.$$

Hence

$$G_b = gG_a g^{-1}.$$

Theorem

(Cycle Decomposition) *Every element of the symmetric group S_n has a unique cycle decomposition.*

Proof. Let $\sigma \in S_n$, $G = \langle \sigma \rangle$ and suppose that G acts on $S = \{1, 2, \cdots, n\}$. S can be partitioned into unique set of disjoint orbits. Let $\mathcal{O}$ be any orbit and $s \in \mathcal{O}$. Let $\left(\frac{G}{G_s}\right)_{left}$ be the set of left cosets of G_s in G. Then define a map ψ: $\mathcal{O} \to \left(\frac{G}{G_s}\right)_{left}$ as

$$\psi(\sigma^i.s) = \sigma^i G_s, \quad \sigma^i \in G = \langle \sigma \rangle, \quad s \in S.$$

Then, for $\sigma^i.s$, $\sigma^j.s \in \mathcal{O}$, we have

$$\begin{aligned} & \psi(\sigma^i.s) = \psi(\sigma^j.s) \\ \Rightarrow\ & \sigma^i G_s = \sigma^j G_s \\ \Rightarrow\ & \sigma^{i-j} \in G_s \\ \Rightarrow\ & \sigma^{i-j}.s = s \\ \Rightarrow\ & \sigma^i.s = \sigma^j.s \ . \end{aligned}$$

So, ψ is an injective map. Also for each $\sigma^r G_s \in \left(\frac{G}{G_s}\right)_{left}$, there exist $\sigma^r.s \in \mathcal{O}$ such that

$$\psi(\sigma^r.s) = \sigma^r G_s.$$

Therefore ψ is surjective and so it is a bijection. Thus

$$0(\mathcal{O}) = 0\left(\left(\frac{G}{G_s}\right)_{left}\right).$$

Now, as G is cyclic therefore $G_s \lhd G$ and so in view of Lemma 6.1, $\left(\frac{G}{G_s}\right)_{left}$ is also cyclic group of order `d', where d is the smallest positive integer for which $\sigma^d \in G_s$. Further

$$\begin{aligned} i_G(G_s) &= \frac{O(G)}{O(G_s)} \\ &= 0\left(\left(\frac{G}{G_s}\right)_{left}\right) \\ &= d \\ &= O(\mathcal{O}). \end{aligned}$$

Thus the distinct cosets of G_s in G are

$$eG_s, \quad \sigma G_s, \quad \sigma^2 G_s, \quad \cdots, \quad \sigma^{(d-1)} G_s.$$

Therefore, in view of above defined bijection ψ distinct elements of $\mathcal{O}$ are

$$s, \quad \sigma(s), \quad \sigma^2(s), \quad \cdots, \quad \sigma^{(d-1)}(s).$$

Fixing the elements of $\mathcal{O}$ in above order shows σ cycles the elements of $\mathcal{O}$ i.e. on orbit of order d, σ acts as a d-cycle.

Further, the orbits of $G = \langle\sigma\rangle$ are uniquely determined by σ. As within each orbit, we can start with any element. Suppose we choose to start with $\sigma^i(x)$ instead of x, then we have

$$\sigma^i(x), \quad \sigma^{i+1}(x), \cdots, \quad \sigma^{d-1}(x), \quad x, \quad \sigma(x), \quad \cdots, \quad \sigma^{i-1}(x)$$

which is a cyclic permutation. This shows cycle decomposition is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers with in each cycle.

Generalized Cayley Theorem

Let G be a group, H be a subgroup of G and let A be the set of left cosets of H in G. Then G acts on A by left multiplication and if π_H denotes the permutation representation afforded by this action then

1. G acts transitively on A.
2. The stabilizer in G of $eH \in A$ is the subgroup H.
3. The kernel of π_H is equal to $\cap_{x\in G} xHx^{-1}$ and it si the largest normal subgroup of G that is contained in H.

Proof. The action of G on A is by left multiplication that is for any $x \in G$ and for any coset $aH \in A$,

$$x.aH = (xa)H.$$

To prove (i), we need to show that for any two left cosets aH and bH of H, there is some element $x \in G$ such that $x.aH = bH$. We may choose $x = ba^{-1}$ so that $x.aH = (xa)H = bH$.

Next, by definition, the stabilizer of eH under the action of G is the set $\{x \in G: x.eH = eH\}$. Now,

$$\{x \in G: x.eH = eH\} = \{x \in G: xH = H\}$$
$$= H,$$

which establishes (ii).

Finally we prove (iii). We have

$$\begin{aligned}\text{Ker } \pi_H &= \{g \in G: g.xH = xH \ \forall \ x \in G\}\\ &= \{g \in G: (x^{-1}gx)H = H \ \forall \ x \in G\}\\ &= \{g \in G: x^{-1}gx \in H \ \forall \ x \in G\}\\ &= \{g \in G: g \in xHx^{-1} \ \forall \ x \in G\}\\ &= \bigcap_{x\in G} \{g \in G: g \in xHx^{-1}\}\\ &= \bigcap_{x\in G} xHx^{-1}.\end{aligned}$$

Since kernel of any homomorphism is always a normal subgroup, Ker π_H is normal in G.

Also, Ker $\pi_H \subseteq xHx^{-1}$ for each $x \in G$, and in particular, for $x = e$, Ker $\pi_H \subseteq H$.

Now let N be any normal subgroup of G that is contained in H.

For any $x \in G$, $N = xNx^{-1} \subseteq xHx^{-1}$.

Thus $N \subseteq \bigcap_{x\in G} xHx^{-1} =$ Ker π_H.

This proves that Ker π_H is the largest normal subgroup of G that is contained in H.

Index Theorem

If G is a finite group and $H < G$ such that $i_G(H) = p$, where p is the smallest prime such that $p|O(G)$, then H normal in G.

Proof. Let H be a subgroup of G such that $i_G(H) = p$ and $\left(\frac{G}{H}\right)_{left}$ be the set of all left cosets of H in G. Suppose G acts on $\left(\frac{G}{H}\right)_{left}$ by left multiplication and $\pi_H: G \to Sym\left(\left(\frac{G}{H}\right)_{left}\right)$ be the associated permutation representation induced by action. Let $K =$ ker π_H and $i_H(K) = k$. So we have

$$\begin{aligned}i_G(K) &= \frac{O(G)}{O(K)}\\ &= \frac{O(G)}{O(H)}.\frac{O(H)}{O(K)}\\ &= pk.\end{aligned}$$

Also, H has p left cosets in G. Therefore

$$\pi_H: G \to Sym\left(\left(\frac{G}{H}\right)_{left}\right) \approx S_p$$

So, by I st- isomorphism theorem,

$$\frac{G}{K} \approx \pi_H(G) < S_p.$$

Thus , by Lagrange's Theorem

$$O(\pi_H(G)) | O(S_p)$$

$\Rightarrow kp \mid p!$

$\Rightarrow k \mid (p-1)!$

$\Rightarrow$ prime divisors of k are less than p.

$\Rightarrow O(G)$ has a prime divisor less than p.

Also, by minimality of p, every prime divisor of k is greater than or equal to p. This gives $k = 1$. Hence

$$H = K \lhd G.$$

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Define stabilizer.
2. Define Orbit.
3. Define permutation groups.
4. Define Kernel of action.
5. Define faithful action.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Let be a group action on the nonempty set A. The relation on A defined by a∼b iff a=g.b for some g ∈ G then prove that '∼' is an equivalence relation on A.
2. Let G be a group, S be a set and suppose G acts on S, then prove that kernel of action is a subgroup of G.
3. Let G be a group and S be a set. Suppose that G acts on S, then prove that any two elements of G induce same permutation iff they are in the same coset of kernel of action.
4. Let G be a group, S be a set and suppose G acts on S. Let a, b∈S such that b = g.a for some g ∈ G, then prove that $G_b = gG_ag^{-1}$, where G_a and G_b are stabilizers of a and b respectively.
5. If G is a group such that $O(G)=p^n$ for some prime p and positive integer a. Then show that subgroup of index p is normal in G. Deduce that group of order p^2 has normal subgroup of order p.
6. Let G be a group and S be a set. Suppose that G acts on S, then prove that for each s∈ S, the stabilizer $G_s$of in g is a subgroup of G.
7. Prove that every element of the symmetric group S_n has a unique cycle decomposition.
8. State and prove the Generelized Cayley's theorem.
9. State and prove Index theorem.
10. If g is a finite group and H<G such that $i_G(H) = p$, where p is the smallest prime such that p\O(G), then prove that H normal in G.

UNIT-V

SYLLABUS

Groups acting on themselves by conjugation, class equation and consequences, conjugacy in Sn, p-groups, Sylow's theorems and consequences, Cauchy's theorem, Simplicity of An for n ≥ 5, non-simplicity tests.

GROUPS ACTING ON THEMSELVES BY CONJUGATION —THE CLASS EQUATION

In this section G is any group and we first consider G *acting on itself* (i.e., $A = G$) *by conjugation*:

$$g \cdot a = gag^{-1} \qquad \text{for all } g \in G,\ a \in G$$

where gag^{-1} is computed in the group G as usual. This definition satisfies the two axioms for a group action because

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1 g_2)a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

and

$$1 \cdot a = 1a1^{-1} = a$$

for all $g_1, g_2 \in G$ and all $a \in G$.

Definition. Two elements a and b of G are said to be *conjugate in* G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classes of* G.

Examples

(1) If G is an abelian group then the action of G on itself by conjugation is the trivial action: $g \cdot a = a$, for all $g, a \in G$, and for each $a \in G$ the conjugacy class of a is $\{a\}$.

(2) If $|G| > 1$ then, unlike the action by left multiplication, G does *not* act transitively on itself by conjugation because $\{1\}$ is always a conjugacy class (i.e., an orbit for this action). More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$ for all $g \in G$ if and only if a is in the center of G.

(3) In S_3 one can compute directly that the conjugacy classes are $\{1\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{(1\ 2\ 3), (1\ 3\ 2)\}$. We shall shortly develop techniques for computing conjugacy classes more easily, particularly in symmetric groups.

As in the case of a group acting on itself by left multiplication, the action by conjugation can be generalized. If S is any subset of G, define

$gSg^{-1} = \{gsg^{-1} \mid s \in S\}$.

A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g \cdot S = gSg^{-1}$ for any $g \in G$ and $S \in \mathcal{P}(G)$. As above, this defines a group action of G on $\mathcal{P}(G)$. Note that if S is the one element set $\{s\}$ then $g \cdot S$ is the one element set $\{gsg^{-1}\}$ and so this action of G on all subsets of G may be considered as an extension of the action of G on itself by conjugation.

Definition. Two subsets S and T of G are said to be *conjugate in* G if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

Class Equation

Definition

Then above equation where $o(G)$ can be represented in terms of cardinality of $Z(G)$ and conjugacy classes of a_i not in $Z(G)$ is called **class equation** of G.

Example

If G is an abelian group of order n then class equation of G is

$n = 1 + 1 + 1 + \ldots + 1$ (n times).

Since G is an abelian group, conjugacy class of every element in the group is a singleton set.

Theorem

If G is a group of order p^n for some prime number p and $n \geq 1$, then G has a non- trivial center.

Proof: Consider the class equation of G

$$O(G) = 1 + 1 + \ldots + 1 \ (O(Z(G)) \text{ times}) + \sum_{a \notin Z(G)} |G : C_G(a)|,$$

where the summation runs over exactly one element from every conjugacy class.
If $G=Z(G)$ then clearly $Z(G)$ is non- trivial.
So assume $G \neq Z(G)$.

Consider $a \notin Z(G)$.

Then by the choice of a, there exists $x \in G$ satisfying $xa \neq ax$.

This shows $C_G(a) \neq G$.

Since $C_G(a)$ is a subgroup of G, by the application of Lagrange's theorem $o(C_G(a)) \mid o(G)$.

Thus order of $C_G(a)$ is of the form of p^m $(0 \leq m < n)$ and therefore,

$|G : C_G(a)| = p^{n-m}$ where $n - m \geq 1$.

Thus p divides $|G : C_G(a)|$ for all $a \notin Z(G)$ and we get

p divides $\sum_{a \notin Z(G)} |G : C_G(a)|$. This give p divides $o(G) - \sum_{a \notin Z(G)} |G : C_G(a)|$ which

shows p divides $o(Z(G))$.

Hence $Z(G)$ is non-trivial.

In order to prove next theorem we prove a lemma.

Lemma

If $a \notin Z(G)$ then $Z(G) \not\subset C_G(a) \not\subset G$

Proof: It can be easily verified that $Z(G) \subseteq C_G(a)$. Also as $a \in C_G(a)$ and given $a \notin Z(G)$, we have $Z(G) \not\subset C_G(a)$. Since $a \notin Z(G)$, therefore there exists $x \in G$ such that $x \notin C_G(a)$ and $C_G(a) \not\subset G$ proving the desired result.

Theorem

Every group of order p^2 is abelian where p is a prime.

Proof: Let G be a group of order p^2 where p is a prime.

Consider the class equation of G

$o(G) = 1 + 1 + \ldots + 1 \ (o(Z(G)) \text{ times}) + \sum_{a \notin Z(G)} |G : C_G(a)|$.

we have $o(Z(G)) \neq 1$.

By the application of Lagrange's theorem the possibility of order of $Z(G)$ is p or p^2.

If $o(Z(G)) = p^2$ then we are done.

If $o(Z(G)) = p$, then there exists $a \in G$ such that $a \notin Z(G)$ and we get $Z(G) \not\subset C_G(a) \not\subset G$.

Also $C_G(a)$ is a subgroup of G, therefore $o(C_G(a))$ divides p^2.

Thus $o(C_G(a)) = 1$, p or p^2.

Since $Z(G) \not\subset C_G(a) \not\subset G$, we have $p < o(C_G(a)) < p^2$ which is impossible.

Thus we get $o(Z(G)) \neq p$. This proves the result.

The above result can also be proved from the following more generalized result

Theorem

If G is a finite group of order p^n, then $o(Z(G)) \neq p^{n-1}$.

Proof: Suppose $o(Z(G)) = p^{n-1}$, then $o\left(\frac{G}{Z(G)}\right) = p$.

Since every group of prime order is cyclic, we get $\frac{G}{Z(G)}$ is cyclic.

This implies G is abelian and $o(Z(G)) = o(G) = p^n$, which is contradiction to our assumption and therefore we get $o(Z(G)) \neq p^{n-1}$.

Conjugacy in S_n

If G is a permutation group then we have a simple rule to find conjugacy classes. We now introduce various definitions and concepts required to obtain class equation of S_n.

Definition

(Partition of a positive integer): Let n be a positive integer. A sequence of positive integers $n_1, n_2, \ldots n_k$ is said to be a partition of n if

1) $n_1 \leq n_2 \leq \ldots\ldots \leq n_k$
2) $n_1 + n_2 + \ldots\ldots + n_k = n$.

We denote the partition of n by $\{n_1, n_2, \ldots n_k\}$. For example $\{1,2,3\}$, $\{3, 3\}$, $\{2, 2, 2\}$ are partitions of 6.

It can easily be seen that a positive integer n can have several partition.

Let $p(n)$ denote the number of partitions of n.

It can be computed that

$p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ and $p(6) = 11$.

Relation between conjugacy and similarity

Now we prove a result which will be used to prove an important theorem which relates conjugacy and similarity.

Result

Let $f \in S_n$ be a permutation which can be represented as product of disjoint cycles as $(a_1\, a_2 \ldots a_{n_1})(b_1\, b_2 \ldots b_{n_2}) \ldots (c_1\, c_2 \ldots c_{n_3})$ then for any $g \in S_n$, gfg^{-1} is

$$\left(g(a_1)\, g(a_2) \ldots g(a_{n_1})\right)\left(g(b_1)\, g(b_2) \ldots g(b_{n_2})\right) \ldots \left(g(c_1)\, g(c_2) \ldots g(c_{n_3})\right).$$

That is, all conjugates of an element have same cycle decomposition type.

Proof: Let f be any permutation in S_n and $a, b \in \{1, 2, \ldots, n\}$ such that $f(a) = b$. Now consider $gfg^{-1}(g(a)) = gf(a) = g(b)$. Therefore, gfg^{-1} maps $g(a)$ to $g(b)$ which shows gfg^{-1} has same cycle decomposition type as f.

p-Group

Definition

*A group whose order is p^n for some prime p and a positive integer n is called a **p-group**.*

Remark

It is a straight application of the Lagrange's theorem that any subgroup of a p-group is again of the order p^α for some $\alpha \geq 0$.

Definition

*If G is a group of order n and p is a prime that divides n then a subgorup of G of order p^α where $p^\alpha | n$ but $p^{\alpha+1} \nmid n$ is called a **Sylow p-subgorup** of G.*

Notation

The set of all Sylow p-subgroups of a group G will be denoted by $\mathbf{Syl}_p(G)$ and

the number of Sylow p-subgroups of G will be denoted by $\boldsymbol{n_p(G)}$.

Sylow's First Theorem

Theorem

If G is a finite gorup and p is a prime that divides $|G|$ then G has a Sylow p-subgorup. In other words, if $p||G|$ then $Syl_p(G)$ is non-empty.

Example

Let G be a group of order 180.

We may factorize $|G|$ as $5 \times 3^2 \times 2^2$.

The Sylow's first theorem guarantees that G will have subgroups of order 5, 9 and 4. Any group of order 5 will be called a Sylow 5-subgorup of G, any subgorup of order 9 will be called a Sylow 3-subgorup and any subgorup of order 4 will be called a Sylow 2-subgorup of G.

Before entering the proof of the theorem, we build some background in form of lemmas.

Lemma

If H and K of subgroups of G and $HK = H$, then $K \subseteq H$.

Lemma

If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $H \leq G$ and $K(G$ then $HK \leq G$.

Lemma

If H and K are finite subgroups of G, then

$|HK| = \frac{|H||K|}{|H \cap K|}$

Proof. By definition, $HK = \{hk : h \in H, k \in K\}$.

We may, therefore write HK as the union of left cosets of K by the elements of H $i.e.$

$$HK = \bigcup_{h \in H} hK.$$

Since two such cosets are either the same or disjoint, we have

$$|HK| = \sum |hK|,$$

where the sum runs over disjoint cosets of type hK.

Since we know that $|hK| = |K|$ for each $h \in H$, our task reduces to find the number of distinct left cosets of type hK with $h \in H$.

We have

$h_1K = h_2K$

$\Leftrightarrow h_2^{-1}h_1K = K$

$\Leftrightarrow h_2^{-1}h_1 \in K.$

But since both h_1 and h_2 belong to H, $h_2^{-1}h_1 \in H$.

Therefore $h_2^{-1}h_1 \in H \cap K$.

We thus conclude that $h_1K = h_2K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$.

Clearly, the number of distinct left cosets of the type hK is same as the number of distinct left cosets of the subgroup $H \cap K$ in H.

By Lagrange's theorem, the number of distinct left cosets of $H \cap K$ in H is $\frac{|H|}{|H \cap K|}$.

This completes the proof.

Sylow's Second and Third Theorems

Theorem

Let G be a finite group and p be a prime that divides $|G|$. Then

1. If P is a Sylow p-subgorup of G and Q is any subgorup of G then Q is contained in some conjugate of P, that is there is some $g \in G$ such that $Q \leq gPg^{-1}$.
2. The number n_p of distinct Sylow p-subgroups of G is of the form $1 + kp$, $k = 0,1,2,\ldots$ and $n_p||G|$.

Proof. Let P be a Sylow p-subgorup of G of order p^α

Since G is a finite group, P has finitely many conjugates.

We list all the distinct conjugates of P in the set $\mathcal{S} = \{P_1, P_2, \ldots, P_r\}$.

Let Q be a p-subgorup of G.

We define an action of the group Q n the set $\mathcal{S}$ as follows.

For any $x \in Q$, define a map σ_x on $\mathcal{S}$ as $\sigma_x(P_i) = xP_ix^{-1}$ for any $P_i \in \mathcal{S}$.

Since $\mathcal{S}$ contains all the conjugates of P, $\sigma_x(P_i) \in \mathcal{S}$ $\forall$ $x \in Q$, $1 \leq i \leq r$.

Also, since conjugation is an invertibel operation, σ_x is a bijection of $\mathcal{S}$ for any $x \in Q$.

The set $\mathcal{S}$, therefore can be written as a disjoint union of orbits under this action.

Let these orbits be $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_s$ so that

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \ldots \cup \mathcal{O}_s \qquad (3)$$

Since the orbits are disjoint, $r = |\mathcal{S}| = |\mathcal{O}_1| + |\mathcal{O}_2| + \cdots + |\mathcal{O}_s|$.

Since each of the orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_s$ are equivalence classes in $\mathcal{S}$, we may choose one representatives from each of these classes.

Let $\tilde{P}_i$ denote the chosen representative of $\mathcal{O}_i$ for $1 \leq i \leq s$.

We also denote the remaining $r-s$ elements of $\mathcal{S}$ as $\tilde{P}_j, s \le j \le r$.

Then $\mathcal{S} = \{\tilde{P}_1, \tilde{P}_2, \ldots \tilde{P}_r\}$.

From the orbit stabilizer theorem, for each $1 \le i \le r$ $|\mathcal{O}_i| = |Q : Q_{\tilde{P}_i}|$ where $Q_{\tilde{P}_i}$ is the stabilizer of $\tilde{P}_i$ in Q.

By the definition

$$Q_{\tilde{P}_i} = \{x \in Q : x\tilde{P}_i x^{-1} = \tilde{P}_i\}$$
$$= \{x \in G : x\tilde{P}_i x^{-1} = \tilde{P}_i\} \cap Q$$
$$= N_G(\tilde{P}_i) \cap Q,$$

and by Lemma

$N_G(\tilde{P}_i) \cap Q = \tilde{P}_i \cap Q$.

Thus we have

$$|\mathcal{O}_i| = |Q : \tilde{P}_i \cap Q|, \quad 1 \le i \le s. \tag{4}$$

Since each $\tilde{P}_i$ is a conjugate of P and conjugacy preserves order, we have

$$|\tilde{P}_i| = |P| = p^{\alpha}.$$

The equation (4) is true for any p-subgorup Q of G, we may replace Q by $\tilde{P}_1$ to obtain

$$|\mathcal{O}_i| = |\tilde{P}_1 : \tilde{P}_i \cap \tilde{P}_1|.$$

For $i \neq 1$, $\tilde{P}_1 \cap \tilde{P}_i$ is a proper subgorup of $\tilde{P}_1$ so the index $|\tilde{P}_1 : \tilde{P}_i \cap \tilde{P}_1|$ is greater than 1. Also,

$$|\tilde{P}_1 : \tilde{P}_i \cap \tilde{P}_1| = \frac{|\tilde{P}_1|}{|\tilde{P}_i \cap \tilde{P}_1|}.$$

Since $|\tilde{P}_1|$ is a power of p, so is $|\tilde{P}_1 : \tilde{P}_i \cap \tilde{P}_1|$.

And for $i = 1$, this index is obviously 1. Coming back to the expression

$$r = |\mathcal{S}| = |\mathcal{O}_1| + |\mathcal{O}_2| + \cdots + |\mathcal{O}_s|$$

Clearly, $|\mathcal{O}_1| = 1$ and for $i > 1$, $|\mathcal{O}_i|$ is a multiple of p.

We conclude that $r = 1 + kp$ for some $k = 0,1,\ldots$.

Now we prove the first part of the theorem.

Suppose Q is any p-subgorup of G.

Suppose, if possible, Q is not contained in any of the conjugates of P.

Then $Q \cap \tilde{P}_i$ is a proper subgorup of Q.

Again, $|\mathcal{O}_i| = |Q : Q \cap \tilde{P}_i|$ and this number, for each i is greater than 1 and a multiple of p.

This forces $r = |\mathcal{S}| = |orb_1| + \cdots + |\mathcal{O}_s|$ to be a multiple of p.

But the number r can not depend on the choice of the p-subgroup Q.

We have already determined that r is of the form $1 + kp$ so it can never be a multiple of p. We are arriving at this contradiction due to the assumtion that Q was not contained in any of $\tilde{P}_i$.

Thus Q must be contained in some P_i. This proves part 1.

If we take Q as another Sylow p-subgorup of G then $|Q| = p^{\alpha} = |P|$ and we have just proven that there is some $g \in G$ such that $Q \subseteq gPg^{-1}$.

But $|gPg^{-1}| = |P| = |Q|$ therefore $Q = gPg^{-1}$.

Hence any two Sylow p-subgroups of G are conjugate to each other.

This immediately implies that the set $\mathcal{S}$ is precisely the set of all Sylow p-subgroups of G and the number of Sylow p-subgroups is r.

We have already shown that $r = 1 + kp$, forsome $k = 0,1, \ldots$.

This completes the proof of part 2.

Cauchy's Theorem for abelian groups

Lemma

If G is a finite abelian group and p is a prime dividing $|G|$, then G must have an element of order p.

Proof. The proof is by induction on $|G|$. Since $p||G|$, $|G| \geq p$.

So we start our induction with $|G| = p$.

If $|G| = p$, a prime, then it has at least one non-identity element, say x.

By Lagrange's theorem, $|x|$ divides $|G|(= p)$.

Since p has only two divisors 1 and p itself, and $|x| \neq 1$, we get x as the required element of order p.

Now assume that $|G| > p$ and the result is true for all groups whose order is less than that of G and divisible by p.

We again pick $x \neq e$ from G.

If $p||x|$ say $|x| = np$ then $|x^n| = p$ and we are done in this case too. So we take up the case where p does not divide $|x|$.

Let N denote the subgroup $\langle x \rangle$ of G generated by x.

Since G is abelian, N is normal.

By Lagrange's theorem, $|G/N| = \frac{|G|}{|N|}$.

Also, $|N| = |x|$ which, by our assumption, is not divisible by p.

Therefore $|G/N|$ is divisible by p.

Since $|N| > 1$, $|G/N| < |G|$.

The group G/N thus fits into our induction hypothesis and it must have an element, say yN of order p.

Saying that yN has order p in G/N is equivalent to $y^p \in N$ but $y \notin N$.

Clearly $\langle y^p \rangle \subseteq \langle y \rangle$ with $\langle y^p \rangle \neq \langle y \rangle$. For if $\langle y^p \rangle = \langle y \rangle$, then $y \in \langle y^p \rangle \subseteq N$ which is a contradiction.

If $|y| = n$ then n and p can not be co-prime for then y^p will generate the cyclic subgroup $\langle y \rangle$.

So p must divide $|y|$ and we ave already seen that if G has an element whose order is a multiple of p then G has an element of order p.

This completes the proof.

The Simplicity of A5

Once 120 has been disposed of, we will have shown that the only integers between 1 and 200 that can be the orders of non-Abelian simple groups are 60 and 168. For completeness, we will now prove that A_5, which has order 60, is a simple group. A similar argument can be used to show that the factor group $SL(2, Z_7)/Z(SL(2, Z_7))$ is a simple group of order 168. [This group is denoted by $PSL(2, Z_7)$.]

If A_5 had a nontrivial proper normal subgroup H, then $|H|$ would be equal to 2, 3, 4, 5, 6, 10, 12, 15, 20, or 30. By Exercise 61 in Chapter 5, A_5 has 24 elements of order 5, 20 elements of order 3, and no elements of order 15. Now, if $|H|$ is equal to 3, 6, 12, or 15, then $|A_5/H|$ is relatively prime to 3, and by Exercise 61 in Chapter 9, H would have to contain all 20 elements of order 3. If $|H|$ is equal to 5, 10, or 20, then $|A_5/H|$ is relatively prime to 5, and, therefore, H would have to contain the 24 elements of order 5. If $|H| = 30$, then $|A_5/H|$ is relatively prime to both 3 and 5, and so H would have to contain all the elements of orders 3 and 5. Finally, if $|H| = 2$ or $|H| = 4$, then $|A_5/H| = 30$ or $|A_5/H| = 15$. But we know from our results in Chapter 24 that any group of order 30 or 15 has an element of order 15. However, since A_5 contains no such element, neither does A_5/H. This proves that A_5 is simple.

The simplicity of A_5 was known to Galois in 1830, although the first formal proof was done by Jordan in 1870. A few years later, Felix Klein showed that the group of rotations of a regular icosahedron is simple and, therefore, isomorphic to A_5 (see Exercise 27). Since then it has frequently been called the *icosahedral group*. Klein was the first to prove that there is a simple group of order 168.

The problem of determining which integers in a certain interval are possible orders for finite simple groups goes back to 1892, when Hölder went up to 200. His arguments for the integers 144 and 180 alone used up 10 pages. By 1975, this investigation had been pushed to well beyond 1,000,000. See [3] for a detailed account of this endeavor. Of course, now that all finite simple groups have been classified, this problem is merely a historical curiosity.

Nonsimplicity Tests

Sylow Test

Theorem

Let G be a group of order n which is not a prime, and let p be a prime divisor of n. Suppose that there is no divisor of n other than 1 which can be written in the form $1+kp, k=0,1,\ldots$ then G is not simple.

Before we prove this theorem, lets recall the Sylow's theorems (without proof).

Sylow's Theorem

Theorem

Let G be a group and p is a prime that divides $|G|$, then

1. G must have a subgroup of order equal to the highest power of p that divides $|G|$. One such subgroup is called a Sylow p-subgroup of G.
2. If P is a Sylow p-subgroup of G then all the cojuagtes of P are Sylow p-subgroups and conversely, any Sylow p-subgroup of G is conjugate to P.
3. The number n_p of Sylow p-subgroups of G must be of the form $1+kp$ where k can be any non-negative integer and n_p must divide $|G|$.

Proof of Sylow Nonsimplicity Test. We first consider the case when $|G|=p^\alpha$.

We know that the centre of a group is always a normal subgroup.

If $Z(G)=G$ then G is abelian and from Proposition 2.1, G can not be simple.

It is an easy consequence of the Class Equation that the centre of a p-group can not be trivial.

Thus for a non-abelian group of order p^α, the centre $Z(G)$ is a proper normal subgroup.

Hence a group of order p^α with $\alpha \geq 2$ can not be simple.

We now assume that $|G|$ is not a power of p.

The first part of the Theorem 3.2 guarantees the existence of a subgroup P of order p^α, and since we have assumed that $|G|$ is not a prime, this subgroup P is a proper subgroup of G.

It is an easy consequence of the second part of Theorem 3.2 that when G has a unique Sylow p-subgroup, P must be equal to all its conjugates and therefore normal.

Finally, the third part of the Sylow's theorem helps determine the number of Sylow p-subgroups of G.

By our assumption, there is no number of the form $1+kp$ that divides $|G|$ other than 1. So n_p must be equal to 1, *i.e.* P is the unique Sylow p-subgroup of G.

We have thus proved that G has a proper normal subgroup P and hence G is not normal. □

POSSIBLE QUESTIONS

PART-B (5 x 2 =10 Marks)

Answer all the questions

1. Write about the conjugacy class of a.
2. Define Sylow p-subgroup.
3. Define cycle type.
4. State Cauchy's theorem.
5. Define conjugate subgroup.

PART-C (5 x 6 =30 Marks)

Answer all the questions

1. Let G be a finite group and let $g_1, g_2, \ldots\ldots g_r$ be representatives of the distinct conjugacy classes of G not contained in the centre Z(G) of G, then prove that $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$.
2. If p is a prime and P is a group of prime power order p^{α} for some $\alpha \geq 1$, then prove that p has a non trivial center.
3. Prove that A_5 is a simple group.
4. Prove that if an integer of the form 2n, where n is an odd number greater than 1, is not the order of a simple group.
5. State and prove Cauchy's theorem.
6. State and prove Sylow's first theorem.
7. State and prove Sylow's second theorem.
8. State and prove Sylow's third theorem.
9. If a finite non abelian simple group G has a subgroup of index n, then show that G is isomorphic to a subgroup of A_n.
10. Let G be a finite group and let p be a prime. If p^k divides $|G|$, then prove that G atleast one subgroup of order p^k.