DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTERS OF SCIENCE-MATHEMATICS

SEMESTER -I

ABSTRACT ALGEBRA

DEMATH-1 CORE-1

BLOCK-1

UNIVERSITY OF NORTH BENGAL

Postal Address:

The Registrar,

University of North Bengal,

Raja Rammohunpur,

P.O.-N.B.U.,Dist-Darjeeling,

West Bengal, Pin-734013,

India.

Phone: (O) +91 0353-2776331/2699008

Fax:(0353) 2776313, 2699001

Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in

Wesbsite: www.nbu.ac.in

First Published in 2019

FOREWORD

The Self-Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

ABSTRACT ALGEBRA

BLOCK-1

BLOCK-2

BLOCK-1: ABSTRACT ALGEBRA

In this block we will go through

Unit I :In this unit we will discuss about Homomorphisms, Isomorphisms, Group Isomorphism various properties of those functions between groups which preserve the algebraic structure of their domain groups.

Unit II: In this unit we will discuss about Fundamental Theorem of Homomorphism, Automorphisms After understanding the concept of isomorphisms & result about the relationship between homomorphism's and quotient groups is the Fundamental Theorem of Homomorphism for groups

Unit III: In this unit we will discuss about Groups, Symmetric Group, Cyclic Decomposition, Alternating Group, Cayley's Theorem, symmetric groups and their subgroups are called permutation groups The study of permutation groups and groups of transformations that gave the foundation to group theory a result by the mathematician Cayley, which says that every group is isomorphic to permutations group, This result is what makes permutation groups

Unit IV: In this unit we will discuss about Direct Product of Groups, External Direct Product, Internal Direct Product, Introduction To Sylow Theorems, Groups of Order, Finite Abelian Groups All cyclic groups are finite abelian but a finite abelian group is not necessarily cyclic & All subgroups of a finite abelian group are normal.

Unit V: In this unit we will discuss about algebra be attached in group actions In this unit getting the information related to conjugate elements

Unit VI: In this unit we will discuss about Cauchy-Riemann equations which under certain conditions provide the necessary and sufficient condition for the differentiability of a function of a complex variable at a point A very important concept of analytic functions which is useful in many application of the complex variable theory & discuss the concept of Cauchy's theorem

Unit VI: In this unit we will discuss about the Sylow Theorems provide a partial converse for Lagrange's Theorem: in certain cases they guarantee us subgroups of specific orders. These theorems yield a powerful set of tools for the classification of all finite non-abelian groups.

UNIT – 1: HOMOMORPHISM OF GROUPS

STRUCTURE

1.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of homomorphism
- Describe Isomorphism

1.1 INTRODUCTION

In this unit, we will discuss various properties of those functions between groups which preserve the algebraic structure of their domain groups. These functions are called group Homomorphisms. This term was introduced by the mathematician Klein in 1983

In this unit, you will also get an idea about a very important mathematical ideaisomorphism

1.2 HOMOMORPHISMS

Let us start our study of functions from one group to another with an example.

Consider the groups (Z, f) and ({ 1, - 1 } ,).If we define

$f : Z \to \{1, -1\}$ by $f(n) = \begin{cases} 1, \text{if } n \text{ is even} \\ -1, \text{if } n \text{ is odd,} \end{cases}$

then you can see that $f(a + b) = f(a).f(b)$ $\forall$ a, b $\square$ Z. What we have just seen is an example of a homomorphism, a function that preserves the algebraic structure of its domain.

Definition: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. A mapping $f : G_1 — G_2$ is said to be a group homomorphism (or just a homomorphism) , if

$f(x *_1 y) = f(x) *_2 f(y)$ $\forall x, \psi \in G_1$.

Note that a homomorphism f from G_1 to G_2 carries the product $x *_1 y$ in G_1 to the product

$f(x) *_2 f(y)$ in G_2.

Note: The word 'homomorphism' is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

Let us define two sets related to a given homomorphism.

Definition: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups and $f : G_1 \in G_2$ be a homomorphism. Then we define

(i) the image of f to be the set

Im $f = \{ f(x)\ 1\ x \in G_1 \}$.

(ii) the kernel of f to be the set

Ker $f = \{ x \in G_1 \mid f(x) = e_2 \}$, where e_2 is the identity of G_2.

Note that Im $f \subseteq G_2$, and Ker $f = f^{-1}(\{ e_2 \}) \in G_1$.

Example: Consider the two groups $(R, +)$ and $(R^*, .)$. Show that the map exp : $(R, +) \to (R^*, .)$: $\exp(r) = e^r$ is a group homomorphism. Also find Im exp and Ker exp.

Solution: For any $r_1, r_2 \in R$, we know that

:. $\exp(r_1 + r_2) = \exp(r_1).\exp(r_2)$.`

Hence, exp is a homomorphism from the additive group of real numbers to the multiplicative group of non-zero real numbers.

Now, Im exp = { exp (r) | r ∈ R } = { e^r | r ∈ R } ,

Also, Ker exp = { ρ ∈ R | e^r = l } = { 0 } .

Note that examples takes the identity 0 of R to the identity 1 of R*. example also carries the additive inverse – r of r. to the multiplicative inverse of exp (r) .

Example: Consider the groups (R, +) and (C, +) and define f : (C, +) → (R, +) by f (x + iy) = x, the real part of x + iy. Show that f is a homomorphism. What are Im f and Ker f?

Solution: Take any two elements a + ib and c + id in C. Then,

f ((a + ib) + (c + id)) = f ((a + c) + i (b + d)) = a + c = f (a + ib) + f (c + id)

Therefore, f is a group homomorphism.

Imf = { f (x + iy) | x, y ∈ R } = { x | x ∈ R) = R.

So, f is a surjective function

Ker f = { x + iy ∈ C | f (x + iy) = 0 } = { x + iy ∈ C | x = 0 }

= { iy | y E R } , the set of purely imaginary numbers.

Note that f carries the additive identity of C to the additive identity of R and (– z) to – f (z) , for any z ∈ C.

In Examples 1 and 2 we observed that the homomorphism's carried the identity to the identity and the inverse to the inverse. In fact, these observations can be proved for any group homomorphism.

Theorem: Let f ; (G_1, $*_1$) ∈ (G_2, $*_2$) be a group homomorphism.

Then

(a) f (e_l) = e_2, where e_1 is the identity of G_1 and e_2 is the identity of G_2.

(b) f (x^{-1}) = [f (x)]$^{-1}$ for all x in G_1.

Proof: (a) Let x ∈ G_1. Then we have e_1 * 1x = x. Hence,

f (x) = f (e_l $*_1$ x) = f (e_1) $*_2$ f (x) , since f is a homomorphism.

But

$f(x) = e_2 *_2 f(x)$ in G_2.

Thus, $f(e_1) *_2 f(x) = e_2 *_2 f(x)$.

So, by the right cancellation law in G_2, $f(e_1) = e_2$.

(b) Now, for any $x \in G_1$, $f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2$.

Similarly, $f(x^{-1}) *_2 f(x) = e_2$.

Hence, $f(x^{-1}) = [f(x)]^{-1} \ \forall \ x \ E \ G_1$.

Note that the converse of Theorem 1 is false. That is, if $f : G_1 \to G_2$ is a function such that $f(e_1) = e_2$ and $[f(x)]^{-1} = f(x^{-l}) = f(x^{-1}) \ \forall x \in G_1$, then f need not be a homomorphism.

For example, consider $f : Z \to Z : f(0) = 0$ and ,

$$f(n) = \begin{cases} n+1 \ \forall \ n > 0 \\ n-1 \ \forall \ n < 0 \end{cases}$$

Since $f(l + 1) \in f(1) + f(l)$, f is not a homomorphism. But $f(e_1) = e_2$ and $f(n) = - f(- n) \ \forall n \in Z$.

Let us look at a few more examples of homomorphism's now. We can get one important class of homomorphism's from quotient groups.

Example: Let $H \triangleq G$. Consider the map $p : G \to G/H : p(x) = Hx$. Show that p is **a** homomorphism. Also show that p is onto. What is Ker p?

Solution: For $x, y \in G$, $p(xy) = Hxy = Hx \ Hy = p(x) \ p(y)$. Therefore, p is a homomorphism.

Now, Im $p = \{ \ p(x) \ (\ x \in G \} = (\ Hx \mid x \in G \ \} = G/H$. Therefore, p is onto.

Ker $p = \{ \ x \in G \mid p(x) = H \ )$. (Remember, H is the identity of G/H.)

$= (\ x \in G \mid H x = H \ \}$

$= \{ \ x \in G \mid x \in \in H \ )$, by theorem.

= H.

In this example you can see that Ker p $\triangleq$ G. You can also check that Theorem 1 is true here.

Example*:* Let H be a subgroup of a group G. Show that the map i : H $\rightarrow$ G, i (h) = h is a homomorphism. This function is called the inclusion map.

Solution: Since i (h_1 h_2) = h_1 h_2 = i (h_1) i (h_2) $\forall$ h_1, h_2 $\in$ H. i is a group homomorphism.

Let us briefly look at the inclusion map in the context of symmetric groups. Consider two natural numbers m and n, where m I n.

Then, we can consider $S_m \leq S_n$, where any $\sigma \in$ Sm, written as

$\begin{pmatrix} 1 & 2 & .... & m \\ \sigma(1) & \sigma(2) & .... & \sigma(m) \end{pmatrix}$, is considered to be the same as

$\begin{pmatrix} 1 & 2 & .... & m & m+1 & .... & n \\ \sigma(1) & \sigma(2) & .... & \sigma(m) & m+1 & .... & n \end{pmatrix}$ $\in S_n$, i.e., σ (k) = k for m + 1 □ k □ n.

Then we can define an inclusion map i : $S_m \rightarrow S_r$.

For example, under i : $S_3 \rightarrow S_4$, (1 2) goes to $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 4 \end{pmatrix}$.

We will now prove some results about homomorphisms .Henceforth, for convenience, we shall drop the notation for the binary operation, and write a * b as ab.

Now let us look at the composition of two homomorphisms. Is it a homomorphism? Let us see.'

Theorem: If f : $G_1 \rightarrow G_2$ and g : $G_2 \rightarrow G_3$ are two group homomorphisms, then the composite map g . f : $G_1 \rightarrow G_3$ is also a group homomorphism.

Proof: Let x. y $\in$ G_1. Then

g o f (xy) = g (f (x : y))

= g (f (x) f (y) , since f is a homomorphism.

$= g (f (x))\ g (f (g))$, since g is a homomorphism.

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

Thus g, f is a homomorphism.

Theorem: Let $f : G_1 \to G_2$ be a group homomorphism. Then

(a) Ker f is a normal subgroup of G_1.

(b) Im f is a subgroup of G_2.

Proof: (a) Since $[(e_1) = e_2, e_1 \in$ Ker f. $\therefore$ Ker $f \neq \phi$.

Now, if $x, y \in$ Ker f, then $f (x) = e_2$ and $f (y) = e_2$.

$\therefore f (xy^{-1}) = f (x)\ f (y^{-1}) = f (x)\ [f (y)]^{-1} = e_2$.

$xy^{-1} \in$ Ker f.

Therefore, by Theorem 1, Ker $f \leq G_1$. Now, for any $y \in G_1$ and x E Ker f,

$f (y^{-1}xy) = f (y^{-1})\ f (x) f (y)$

$= [f (y)]^{-1} e_2 f (y)$, since $f (x) = e_2$ and by Theorem 1

$= e_2$.

$\therefore$ Ker f $\triangleq G_1$.

(b) Im $f \neq \phi$, since $f (e_l)$ E Im f.

Now, let $x_2, y_2 \in$ Im f. Then $\exists x_1, y_1 \in G_1$ such that $f (x_1) = x_2$ and $f (y_1) = y_2$.

$\therefore \quad x_2 y_2^{-1} = f (x_1)\ f (y_1^{-1}) = f (x_1 y_1^{-1}) \in$ Imf.

$\therefore$ Im $f \leq G_2$.

Using this result, we can immediately see that the set of purely imaginary numbers is a normal subgroup of C.

Consider $\phi : (R, +) \to (C^*, .)$ $\phi (x) = \cos x + i \sin x$. We have seen that $\phi (x + y) = \phi (x) \phi (y)$, that is, ϕ is a group homomorphism. Now $\phi (x) = 1$ iff $x = 2\pi n$ for some $n \in Z$. Thus, by Theorem 3, Ker

$\phi = (2 \pi n \mid n \in Z)$ is a normal subgroup of $(R. +)$. Note that this is cyclic, and 2n is a generator.

Similarly, Im ϕ is a subgroup of C*. This consists of all the complex numbers with absolute value 1, i.e., the complex numbers on the circle with radius 1 unit and centre $(0, 0)$.

You may have noticed that sometimes the kernel of a homomorphism is $\{ e \}$ and sometimes it is a large subgroup. Does the size of the kernel indicate anything? We will prove that a homomorphism is 1 – 1 iff its kernel is $\{ e \}$.

Theorem: Let $f : G_1 \to G_2$ be a group homomorphism. Then f is injective iff Ker f = $\{ e_1 \}$, where e_1 is the identity element of the group G_1.

Proof: Firstly, assume that f is injective. Let $x \in$ Ker f. Then $f (x) = e_2$, i.e., $f (x) = f (e_1)$. But f is 1 – 1. $\therefore x = e_1$.

Thus, Kerf = $\{ e_1 \}$.

Conversely, suppose Ker f = $\{ e_1]$. Let $x, y \in G_1$ such that

$f (x) = f (y)$. Then $f (xy^{-1}) = f (x) \ f (y^{-1})$

$= f (x) \ [f (y)]^{-1} = e_2$.

$\therefore \quad xy^{-1} \in$ Ker f = $\{ e1 \}$. $\quad \therefore xy^{-1} = e_1$ and x = y.

This shows that f is injective.

So, by using Theorem 4, we can immediately say that any inclusion i : B $\to$ G is 1-1, since
Ker i = $\{ e \}$.

Let us consider another example.

Example: Consider the group T of translations of R^2. We define a map $\phi : (R^2 +) \to (T, o) \ldots . (a, b) = f_{a, b}$. Show that ϕ is an onto homomorphism, which is also 1-1.

Solution: For (a, b), (c, d) in R*, we have seen that

$f_{a+c,h+d} = f_{a,b} \ o \ f_{c.d}$

$\therefore \quad \phi ((a, b) + (c, d)) = \phi (a, b) \text{ o } \phi (c, d)$.

Thus, ϕ, is a homomorphism of groups.

Now, any element of T is -f (a, b) . Therefore, ϕ is surjective. We now show that ϕ is also injective.

Let (R, b) $\in$ Ker ϕ. Then $ (a, b) = $f_{0, 0}$

i.e., $f_{a, b} = f_{0,0}$

$\therefore$ $f_{a,b} (0, 0) = f_{0, 0} (0, 0)$,

i.e., (a, b) = (0, 0)

$\therefore$ Ker ϕ = { 1 (0, 0) }

$\therefore$ ϕ is 1-1.

So we have proved that f is a homomorphism, which is bijective.

And now let us look at a very useful property of a homomorphism that is surjective.

Theorem: Iff : $G_1 \rightarrow G_2$ is an onto group homomorphism and S is a subset that generates G_1, then f (S) generates G_2.

Proof: We know that

$G_1 = < S > = \{ \mid m \in N, x_1 \in S, r_1 \in Z$ for all i) . We will show that

$G_2 = < f (S) >$

Let $x \in G_2$, Since f is surjective, there exists $y \in G_1$ such that f (y) = x. Since $y \in G_1$, y = for some m $\in$ N, where xi $\in$ S and ri $\in$ Z, $\leq 1 \leq$ i $\leq$ m.

Thus,x = f (y) = = since f is a homomorphism.

$\Rightarrow$ x $\in$ < f (S) >. since f (x_1) $\in$ f (S) for every i = 1, 2, ..., r.

Thus $G_2 = < f (S) >$.

So far you have seen examples of various kinds of homomorphisms-injective, surjective and bijective. Let us now look at bijective homomorphism in particular.

Check Your progress-1

1. Let H be a subgroup of a Group G. Then $H \to G, i(h) = h$ is a homomorphism. This function is called the .....

(a) inclusion map (b) normal function

(c) cyclic (d) abelian

2. gof (x, y) is equal to:

(a) gof (x) . gof (y) (b) gof (x) + gof (y)

(c) gof (x^{-1}) .gof (y^{-1}) (d) gof (x) . gof (y^{-1})

1.3 ISOMORPHISMS

Definition: Let G_1 and G_2 be two groups. A homomorphism $f : G_1 \to G_2$ is called an isomorphism if f is 1-1 and onto.

In this case we say that the group G_1 is isomorphic to the group G_2 or G_1 and G_2 are isomorphic. We denote this fact by $G_1 \approx G_2$.

An isomorphism of a group G onto itself is called an automorphism of G. For example, the identity' function $IG : G \to G : I_G(x) = x$ is an automorphism.

Note: The word 'isomorphisms' is derived from the Greek word 'ISOS' meaning 'equal'.

Let us look at another example of an isomorphism.

Example*:* Consider the set $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in R \right\}$.

Then G is a group with respect to matrix addition.

Show that $f : G \to C : f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$ is an isomorphism.

Solution: Let us first verify that f is a homomorphism. Now, for any two elements

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ in G,

$$r\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}+\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)=f\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}=(a+c)+i(b+d)$$

$= (a + ib) + (c + id)$

$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right)+f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$

Therefore, f is a homomorphism.

Now, Ker f = $f=\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\middle| a+ib=0\right\}=\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\middle| a+0, b=0\right\}=\left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right\}$

Therefore, by Theorem 4, f is 1-1.

Finally, since Im f = C. f is surjective

Therefore, f is an isomorphism.

We would like to make an important remark now.

Remark: If G_1 and G_2 are isomorphic groups, they must have the same algebraic structure and satisfy the same algebraic properties. For example, any group isomorphic to a finite group must be finite and of the same order. Thus, two isomorphic groups are algebraically indistinguishable systems.

The following result is one of the consequences of isomorphic groups being algebraically alike

Theorem: If $f : G \to H$ is a group isomorphism and $Y \in G$, then $< x >$; $< f (x) >$,

Therefore.

(i) if s is of finite order, then $o (x) = o (f (s))$.

(ii) if x is of infinite order, so is $f (x)$.

Proof: If we restrict f to any subgroup K of G, we have the function $f | K ; K \to f (K)$, Since f is bijective, sc is its restriction $f | k ; k ; f (K)$ for any subgroup K of G. In particular, for any $x \in G$,

$< x > ; f (< x >) = < f (x) >$,

Now if x has finite order, then o (x) = o (< x >) = o (< f (x) >) = o (f (x)) , proving (i)

To prove (ii) assume hat x is of infinite order. Then < x > is an infinite group.

Therefore, < f (x) > is an infinite group, and hence, f (x) is of infinite order. So, we have proved (ii) .

Example: Show that (R*,.) is not isomorphic to (C*,.) .

Solution: Suppose they are isomorphic, and f : C* — R* is an isomorphism. Then

o (i) = o (f (i)) , by Theorem 6, Now o (i) = 4. ∴ o (f (i)) = 4.

However, the order of any real number different from ±1 is infinite: and o (1) = 1, o (–1) = 2.

So we reach a contradiction. Therefore, our supposition must be wrong. That is, R* and C* are not isomorphic.

You must have noticed that the definition of an isomorphism just says that the map is bijective, i.e., the inverse map exists. It does not tell us any properties of the inverse. The next result does so.

Theorem: If $f : G_1 \to G_2$ is an isomorphism of groups, then $f^{-1} : G_2 \to G_1$ is also an isomorphism.

Proof: You know that f^{-1} is bijective. So, we only need to show that f^{-1} is a homomorphism. Let a', b' $\in G_2$ and a = f^{-1} (a') , b = f^{-1} (b') . Then f (a) = a' and f (b) = b'.

Therefore, f (ab) = f (a) f (b) = a'b'. On applying f^{-1}, we get

f^{-1} (a'b') = ab = f^{-1} (a') f^{-1} (b') , Thus,

f^{-1} (a'b') = f^{-1} (a') f^{-1} (b') for all a', b' $\in G_2$.

Hence, f^{-1} is an isomorphism.

From Theorem 7 we can immediately say that

$\phi^{-1} : T \to R^2 : \phi^{-1} (f_{a,b,}) = (a, b)$ is an isomorphism.

Theorem says that if G_I ; G_2, then G_2 ; G_1. We will be using this result quite often.

Check Your progress-2

3. An isomorphism of a group G onto itself is called an _____of G.

a. automorphism

b. isomorphic

c. homomorphism

d. Non of the above

4. If $f : G_1 \rightarrow G_2$ is an isomorphism of groups, then $f^{-1} : G_2 \rightarrow G_1$ is also an _____.

a. automorphism

b. isomorphic

c. homomorphism

d. Non of the above

1.4 GROUP ISOMORPHISM

In abstract algebra, a group isomorphism is a function between two groups that sets up a one-to-one correspondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are called isomorphic. From the standpoint of group theory, isomorphic groups have the same properties and need not be distinguished.

Definition and Notation

Given two groups (G, *) and (H,) , a group isomorphism from (G, *) to (H,) is a bijective group homomorphism from G to H. Spelled out, this means that a group isomorphism is a bijective function $f : G \rightarrow H$ such that for all u and v in G it holds that

f (u * v) = f (u) f (v) .

The two groups (G, *) and (H,) are isomorphic if an isomorphism exists. This is written:

(G, *) ≅ (H,)

Often shorter and more simple notations can be used. Often there is no ambiguity about the group operation, and it can be omitted:

G ≅ H

Sometimes one can even simply write G = H. Whether such a notation is possible without confusion or ambiguity depends on context. For example, the equals sign is not very suitable when the groups are both subgroups of the same group.

Conversely, given a group (G, *) , a set H, and a bijection f : G → H, we can make H a group
(H,) by defining

f (u) f (v) = f (u * v) .

If H = G and = * then the bijection is an automorphism (q.v.)

Intuitively, group theorists view two isomorphic groups as follows: For every element g of a group G, there exists an element h of H such that h 'behaves in the same way' as g (operates with other elements of the group in the same way as g) . For instance, if g generates G, then so does h. This implies in particular that G and H are in bijective correspondence. So the definition of an isomorphism is quite natural.

An isomorphism of groups may equivalently be defined as an invertible morphism in the category of groups, where invertible here means has a two-sided inverse.

Examples:

1. The group of all real numbers with addition, (ϒ, +) , is isomorphic to the group of all positive real numbers with multiplication (ϒ+, ×) :

(ϒ, +) (ϒ+, ×)

via the isomorphism

f (x) = e^x

(see exponential function) .

2. The group ′ of integers (with addition) is a subgroup of □, and the factor group ϒ/′ is isomorphic to the group S^1 of complex numbers of absolute value 1 (with multiplication) :

ϒ/′ ≅ S^1

An isomorphism is given by

f (x + ′) = $e^{2\pi x1}$

for every x in ϒ.

3. The Klein four-group is isomorphic to the direct product of two copies of $'_2$ = ′/2′

(see modular arithmetic) , and can therefore be written $'_2 \cdot '_2$. Another notation is Dih_2, because it is a dihedral group.

4. Generalizing this, for all odd n, Dih_{2n} is isomorphic with the direct product of Dih_n and Z_2.

5. If (G, *) is an infinite cyclic group, then (G, *) is isomorphic to the integers (with the addition operation) . From an algebraic point of view, this means that the set of all integers (with the addition operation) is the 'only' infinite cyclic group.

Some groups can be proven to be isomorphic, relying on the axiom of choice, but the proof does not indicate how to construct a concrete isomorphism.

1. The group (ϒ, +) is isomorphic to the group (≤, +) of all complex numbers with addition.

2. The group ($\leq^*$, ·) of non-zero complex numbers with multiplication as operation is isomorphic to the group S^1 mentioned above.

Properties

The kernel of an isomorphism from (G, *) to (H,) , is always { e_G } where e_G is the identity of the group (G, *)

If (G, *) is isomorphic to (H,) , and if G is abelian then so is H.

If (G, *) is a group that is isomorphic to (H,) [where f is the isomorphism], then if a belongs to G and has order n, then so does f (a) .

If (G, *) is a locally finite group that is isomorphic to (H,) , then (H,) is also locally finite.

We also go through that 'group properties' are always preserved by isomorphisms.

Cyclic Groups

All cyclic groups of a given order are isomorphic to $(\mathbb{Z}_n, +_n)$.

Let G be a cyclic group and n be the order of G. G is then the group generated by $< x > = \{ e, x, ..., x^{n-1} \}$. We will show that

$$G \cong (\mathbb{Z}_n, +_n)$$

Define

$\phi : G \to \mathbb{Z}_n = \{ 0, 1, ..., n-1 \}$, so that $\phi (x^a) = a$. Clearly, ϕ is bijective.

Then

$\phi (x^a . x^b) = \phi (x^{a+b}) = a + b = \phi (x^a) +_n \phi (x^b)$ which proves that $G \cong \mathbb{Z}_n, +n$.

Consequences

From the definition, it follows that any isomorphism $f : G \to H$ will map the identity element of G to the identity element of H,

$$f (e_G) = e_H$$

that it will map inverses to inverses,

$$f (u^{-1}) = [f (u)]^{-1}$$

and more generally, nth powers to nth powers,

$$f (u^n) = [f (u)]^n$$

for all u in G, and that the inverse map $f^{-1} : H \to G$ is also a group isomorphism.

The relation "being isomorphic" satisfies all the axioms of an equivalence relation. If f is an isomorphism between two groups G and H, then everything that is true about G that is only related to the group structure can be translated via f into a true ditto statement about H, and vice versa.

Check Your progress-3

5. Let $f : G_1 \to G_2$ be a group homomorphism thus her f is a ..... of G.

(a) subgroup (b) normal

(c) cyclic (d) abelian

6. If (G, *) is isomorphic to (H,) , and if G is abelian then so is.

(a) H (b) G

(c) Both H & G (d) Non of the above

1.5 LET US SUM UP

In this unit we have discussed the definition and example of a group homomorphism. Let $f : G_1 \to G_2$ be a group homomorphism. Then $f (e_1) = e_2$, $[f (x)]^{-1} = f (x^{-1})$, Im $f \leq G_2$, Ker f G_1.

We have also discussed a homomorphism is 1-1 iff its kernel is the trivial subgroup. The definition and examples of a group isomorphism. Two groups are isomorphic if they have exactly the same algebraic structure.

Lastly we have discussed the composition of group homomorphisms (isomorphisms) is a group homomorphism (isomorphism) .

1.6 KEYWORDS

1. **Homomorphism:** Homomorphism is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

2. Inclusion map: Let H be a subgroup of a group G. Show that the map i: H $\rightarrow$ G, i (h) = h is a homomorphism. This function is called the **inclusion map.**

1.7 QUESTIONS FOR REVIEW

1. Show that f : (R*,.) $\rightarrow$ (R, 4) : f (x) = inx, the natural logarithm of x, is a group homomorphism. Find Ker f and Im f also.
2. Is f : (GL_3 (R) 3,) $\rightarrow$ (w*,.) : f (A) = det (A) a homomorphism? If so, obtain Ker f and Im f.
3. Define the natural homomorphism p from S_3 to S_3/A_3. Does (1 2) E Ker p? Does (1 2) E Im p?
4. Let S = [z $\in$ C| |z| = 1 } .

   Define f : (R, +) $\rightarrow$ (S,.) L f (x) = e^{Inx}, where n is a fixed positive integer. Is f a homomorphism? If so find Ker f.
5. Define Inclusion map by giving a suitable example.

1.8 SUGGESTED READINGS AND REFERENCES

1. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
2. Paul B. Garrett (2007) . *Abstract Algebra*. Chapman and Hall/CRC.
3. Vijay K Khanna (2017) .*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
4. LALJI PRASAD (2016) . *Modern Abstract Algebra*. Paramount Publication
5. Stephen Lovett (2016) . *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

1.9 ANSWERS TO CHECK YOUR PROGRESS

1. (a) (answer for Check your Progress-1 Q.1)
2. (a) (answer for Check your Progress-1 Q.2)
3. (a) (answer for Check your Progress-2 Q.3)
4. (b) (answer for Check your Progress-2 Q.4)
5. (b) (answer for Check your Progress-3 Q.5)
6. (a) (answer for Check your Progress-3 Q.6)

UNIT - 2: HOMOMORPHISM THEOREM

STRUCTURE

2.0 OBJECTIVES

After studying this unit, you should be able to:

- Discuss fundamental theorem of homomorphism
- Explain the concept of automorphism

2.1 INTRODUCTION

After understanding the concept of isomorphisms. Let us prove some result about the relationship between homomorphisms and quotient groups. The first result is the Fundamental Theorem of Homomorphism for groups. It is called 'fundamental' because a lot of group theory depends upon this result. This result is also called the first isomorphism theorem.

2.2 FUNDAMENTAL THEOREM OF HOMOMORPHISM

Theorem 1 (Fundamental Theorem of Homomorphism) : Let G_1 and G_2 be two groups and $f : G_1 \to G_2$ be a group homomorphism. Then

$G_1/\text{Ker } f$; Im f.

In particular, if f is onto, then $G_1/\text{Ker } f$; G_2.

Proof: Let Ker f = H. Note that $H \triangleq G_1$. Let us define the function

$\psi : G_1/H \to \text{Im } f : \psi\ (Hx) = f(x)$.

At first glance it seems that the definition of ψ depends on the coset representative. But we
will show that if $x, y \in G_1$ such that Hx = Hy, then $\psi\ (Hx) = \psi\ (Hy)$. This will prove that ψ is a
well-defined function.

Now, $Hx = Hy \Rightarrow xy^{-1} \in H = \text{Ker } f \Rightarrow f(xy^{-1}) = e_2$, the identity of G_2.

$\Rightarrow f(x)\,[f(y)]^{-1} = e^2 \Rightarrow f(x) = f(y)$.

$\Rightarrow \psi(Hx) = \psi(HY)$.

Therefore, y is a well-defined function,

Now, let us check that ψ is a homomorphism. For Hx, Hy □ G_1/H,

$\psi(Hx)\ (Hy)\ ) = \psi(Hxy)$

$= f(xy)$

$= f(x)\ f(y)$, since f is a homomorphism.

$= \psi(H)\ \psi(HY)$

Therefore, ψ is a group homomorphism.

Next, let us see whether ψ is bijective or not.

Now, $\psi(Hx) = \psi(Hy)$ for Hx, HY in G_1/H

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

$\Rightarrow f(x)\ [f(y)\,l^{-1} = e_2$

$\Rightarrow f(xy1) = e_2$

$\Rightarrow xy^{-1} \in \text{Ker } f = H.$

$\Rightarrow Hx = Hy$

Thus, ψ, is 1-1.

Also, any element of Im f is $f(x) = \psi(Hx)$, where $x \in G_1$.

$\therefore$ Im ψ = Im f.

So, we have proved that ψ is bijective, and hence, an isomorphism. Thus, G1/Ker f = Im f.

Now, if f is surjective, Im f = G_2. Thus, in this case G_1/Ker f ; G_2.

The situation in Theorem can be shown in the following Figure 2.1

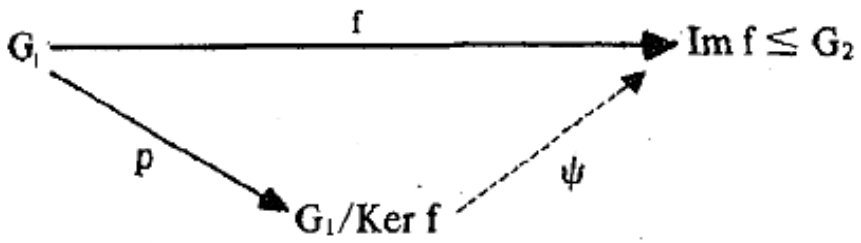


Figure : The situation of Fundamental Theorem of Homomorphism

Here, p is the natural homomorphism.

The diagram says that if you first apply p, and then ψ, to the elements of G_1, it is the same as applying f to them. That is,

$\psi \circ p = f$.

Also, note that Theorem says that two elements of G_1 have the same image under f iff they belong to the same coset of Ker f.

Let us look at a few examples.

One of the simplest situations we can consider is $I_G : G \to G$. On applying Theorem here, we see that G/ { e } ; G. We will be using this identification of G/ { e) and G quite often.

Example: Prove that C/R ; R.

Solution: Define $f : C \to R : f(a + ib) = b$. Then f is a homomorphism, Ker f = R and Im f = R. Therefore, on applying Theorem 1 we see that C/R ; R.

Example: Consider $f : Z \to (\{ 1, - 1) ,.)$: $f(n) = \begin{cases} 1, \text{if n is even} \\ -1, \text{if n is odd.} \end{cases}$

At the beginning, you saw that f is a homomorphism. Obtain Ker f and Im f. What does Theorem 1 say in this case?

Solution: Let Z_e and Z_o denote the set of even and odd integers, respectively. Then

Ker f = $\{ n \in Z \mid f (n) = 1 \} = Z$,

Im f = $\{ f (n) \mid n \in Z) = \{ l , – 1 \}$

Thus, by Theorem 1, Z/Z, ; $\{ 1, - 1 \}$.

This also tells us that o (Z/Z_e) = 2. The two cosets of Z_e in Z are Z_e and *.

$\therefore$ $\{ Z_e, Z_o \}$; $\{ 1, -1 \}$.

Example: Show that $GL_2 (R) /SL_2 (R)$; R*, where $SL_2 (R) = \{ A \in GL_2 (R) \mid \det (A) = 1 \}$.,

Solution: We know that the function

f : $GL_2 (R) \to R^*$: f (A) = der (A) is a homomorphism. Now, Ker f = $SL_2 (R)$.

Also, Im f = R*, since any r $\in$ R* can be written as det $\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)$.

Thus, using Theorem 1, $GL_2 (R) /SL_2 (R)$; R*.

Now-we will use the Fundamental Theorem of Homomorphism to prove a very important result which classifies all cyclic groups.

Theorem: Any cyclic group is isomorphic to (Z, +) or (Z_n, +) .

Proof: Let G = < x > be a cyclic group. Define

f : $Z \to G$: f (n) =x^n.

f is a homomorphism because

f (n + m) = $x^{n+m} = x^n . x^m$ = f (n) f (m) .

Also note that Im f = G.

Now, we have two possibilities for Ker I → Ker f = { 0) or Ker f ≠ { 0 } .

Case 1 (Ker f = { 0)) : In this case f is 1-1. Therefore, f is an isomorphism. Therefore, by Theorem 7 of unit 6, f-1 is an isomorphism. That is, G ; (Z, +) .

Case 2 (Ker f # { 0)) : Since Ker f ≤ Z, we know that Ker f = nZ, for some n ∈ N. Therefore, by the Fundamental Theorem of Homomorphism, Z/nZ ; G.

∴ G = Z/nZ = (Z_n, +) .

Over here note that since < x > = Z_n, o (x) = n. So, a finite cyclic group is isomorphic to Z_n, where n is the order of the group.

Theorem : If H and K are subgroups of a group G, with K normal in G, then H/ (H I K) ;
(HK) /K.

Proof: We must first verify that the quotient groups H/ (H I K) and (HK) /K are well defined. You know that H I K H. You know that HK ≤ G. Again, you know that KHK. Thus, the given quotient groups are meaningful.

Now, what we want to do is to find an onto homomorphism f : H — (HK) /K with kernel H □ K. Then we can apply the Fundamental Theorem of Homomorphism and get the result. We define f : H → (HK) /K : f (h) = hK.

Now, for x, y ∈ H,

f (xy) = xyK = (xK) (yK) = f (x) f (y) .

Therefore, f is a homomorphism.

We will show that Im f = (HK) /K. Now, take any element hK ∈ Im f. Since h ∈ H, h ∈ HK

∴ hK ∈ (HK) /K. ∴ Im f ⊆ (HK) /K. On the other hand, any element of (HK) /K is

hkK = hK, since k ∈ K.

$\therefore$ hkK $\in$ Im f. (HK) /K $\subseteq$ Im f.

$\therefore$ Im f = (HK) /K.

Finally, Ker f = { h $\in$ H | f (h) = K } = { h $\in$ H hK = K }

= { h $\in$ H | h $\in$ K }

= H I K .

Thus, on applying the Fundamental Theorem, we get H / (H I K) ; (HK) / K

We would like to make a remark here.

Remark: If H and K are subgroups of (G.+) , then Theorem 3 says that

(H + K) / K ; H/H I K.

Theorem: Let H and K be normal subgroups of a group G such that K □ H. Then (G/K) / (H/K) ; G/H.

Proof: We will define a homomorphism from G/K onto G/H, whose kernel will turn out to be H/K.

Consider f : G/K $\rightarrow$ G/H : f (Kx) = Hx. f is well-defined because Kx = Ky tor x, y $\in$ G

$\Rightarrow xy^{-1} \in K \subseteq H \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy \Rightarrow$ (Kx) = f (Ky) .

Check your progress-1

1. An isomorphism of a group G itself is called as an ..... of G.

   (a) Homomorphism (b) automorphism

   (c) Herf (d) one-to-one function

2. The word isomorphisms is derived from Greek word ISOS meaning .....

   (a) equal (b) unequal

   (c) bijective (d) subjective

2.3 AUTOMORPHISMS

Let us start discussing the concept of automorphism

Let G be a group. Consider

Aut G = { f : G $\rightarrow$ G | f is an isomorphism } .

You have already seen that the identity map $I_G \in$ Aut G. You know that Aut G is closed under the binary operation of composition. Iff E Aut G, then $f^{-1} \in$ Aut G. We summarise this discussion in the following theorem.

An isomorphism from a group (G,*) to itself is called an Automorphisms of this group. Thus it is a bijection f : G $\rightarrow$ G such that

f (u) * f (v) = f (u * v) .

An automorphism always maps the identity to itself. The image under an automorphism of a conjugacy class is always a conjugacy class (the same or another) . The image of an element has the same order as that element.

The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group G, denoted by Aut (G) , forms itself a group, the automorphism group of G.

For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse this is the trivial automorphism, e.g. in the Klein four-group. For that group all permutations of the three non-identity elements are automorphisms, so the automorphism group is isomorphic to S_3 and Dih_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with corresponding changes in the other elements. The Automorphisms group is isomorphic to
Z_{p-1}. For example, for n = 7, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 = 1$ (modulo 7) , while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with

this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely.

The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these.

The automorphism group of $Z_2 \times Z_2 \times Z_2 = Dih_2 \times Z_2$ has order 168, as can be found as follows.

All 7 non-identity elements play the same role, so we can choose which plays the role of $(1,0,0)$. Any of the remaining 6 can be chosen to play the role of $(0, 1, 0)$. This determines which corresponds to $(1, 1, 0)$. For $(0, 0, 1)$ we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphisms. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements. The lines connecting three points correspond to the group operation: a, b, and c on one line means a + b = c, a + c = b, and b + c = a. See also general linear group over finite fields.

For Abelian groups all automorphisms except the trivial one are called outer automorphisms.

Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer Automorphisms.

Theorem: Let G be a group. Then Aut G, the set of automorphisms of G, is a group.

Let us look at an example of Aut G.

Example: Show that Aut Z ; Z_1.

Solution: Let $f : Z \to Z$ be an automorphism. Let $f(1) = n$. We will show that n = 1

or – 1. Since f is onto and $1 \in Z$, $\exists\ m \in Z$such that $f(m) = l$, i.e., $mf(l) = l$, ie., m=l.

$\therefore$ n = 1 or n = –1.

Thus, there are only two elements in Aut Z, I and –I.

So Aut Z = < – I > ; Z_2.

Now given an element of a group G. We will define an automorphism of G corresponding to it.

Consider a fixed element g ∈ G. Define

$f_g : G \to G : f_g (x) = gxg^{-1}$.

We will show that f_g is an automorphism of G.

(i) f, is a homomorphism : If x, y ∈ G, then

$f_g (xy) = g (xy) g^{-1}$

$= gx (e) yg^{-1}$, where e is the identity of G.

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

$= (gxg^{-1}) (gyg^{-1})$

$= f_g (x) f_g (dy)$.

(ii) f_g is 1-1 : For x, y ∈ G, $f_g (x) = f_g (y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x$ = y, by the cancellation laws in G.

(iii) f_g is onto : If y ∈ G, then

$Y = (gg^{-1}) y (gg^{-1})$

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

$= f_g (g^{-1}yg) \in$ lm f_g.

Thus, f, is an automorphism of G.

Definition: f_g is called an inner automorphism of G induced by the element g in G. The subset of Aut G consisting of all inner automorphism of G is denoted by Inn G.

For example, Let us compute $f_g (1)$. $f_g (l 3)$ and $f_g (1 2 3)$, where g = (1 2) . Note that g^{-1} = (1 2) = g.

Now, f_g (1) = g a I o g^{-1} = I,

$f_g (l 3) = (1 2) (1 3) (1 2) = (2 3)$.

$f_g (1\,2\,3) = (1\,2)\,(1\,2\,3)\,(1\,2) = (1\,3\,2)$.

Theorem: Let G be a group. Then Inn G is a normal subgroup of Aut G. i

Proof: Inn G is non-empty, because $I_G = f_e \in$ Inn G, where e is the identity in G.

Now, let us see if f, o fh $\in$ Inn G for g, h $\in$ G.

For any x $\in$ G, $f_g \cdot f_n (x) = fg (hxh^{-1})$

$= g (hxh^{-1})\ g^{-1}$

$= (gh)\ x\ (gh)^{-1}$

$= fgh (x)$

Thus, $f_{gh} = f_g$ o f_h, i.e., Inn G is closed under composition. Also $f_e = I_G$ belongs to Inn G.

Now, for $f_g \in$ Inn G, 3 $fg^{-1} \in$ Inn G such that

f_g o $f_g^{-1} = f_{gg^{-1}} = f_e = I_G$. Similarly, f_{g-1}o $f_g = I_G$.

Thus, $f_g^{-1} = (f_g)^{-1}$. That is every element of Inn G has an inverse in Inn G.

This proves that Inn G is a subgroup of Aut G.

Now, to prove that Inn Aut G, let $\phi \in$ Aut G and $f_g \in$ Inn G. Then, for any x $\in$ G

$\phi^{-1} \times f_g \times \phi (x) = \phi^{-1} \times f_g (\phi (x))$

$= \phi^{-1} (g\phi (x)\, g^{-1})$

$= \phi^{-1} (g)\ \phi^{-1} (\phi (x))\ \phi^{-1} (g^{-1})$

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

= (Note that ϕ-1 (g) ϕ G.)

$\therefore\ \phi^{-1}$ o f_g o $\phi = f_{\phi^{-1}(g)} \in$ Inn G $\forall\ \phi \in$ Aut G and $f_g \in$ Inn G.

$\therefore$ Inn G $\triangleq$ Aut G.

Now we will prove an interesting result which relates the cosets of the centre of a group G to

lnn G. Recall that the centre of G, Z (G) = { x ∈ G | xg = gx ∀ g ∈ G } .

Theorem: Let G be a group. Then G/Z (G) ; Inn G.

Proof: As usual, we will use the powerful Fundamental Theorem of Homomorphism to prove this result.

We define f : G → Aut G : f (g) = f_g.

Firstly, f is a homomorphism because for g, h ∈ G,

f (gh) = f_{gh}

= I, o f_h (sec proof of Theorem 13)

= [(g) o f (h) .

Next, Im F = (f_g, 1 g ∈ G) = Inn G.

Finally, Kerf = (g ∈ G | f, = I_G }

= { g ∈ G [f_g (x) = x ∀ x ∈ G }

= { g ∈ G | gxg^{-1} = x ∀ x ∈ G }

= { g ∈ G | gx = xg ∀ x ∈ G }

= Z (G) .

Therefore, by the Fundamental Theorem,

G/Z (G) ; Inn G.

Check your progress-2

3. The subset of Aut G consisting of all inner automorphism of G is denoted by _____.

a. G Inn

b. Inn G

4. For Abelian groups all automorphisms except the trivial one are called _____.

a. Outer automorphisms

b. Inner automorphisms

2.4 LET US SUM UP

Here we have studied the proof of the Fundamental Theorem of Homomorphism, which says that if $f : G_1 \to G_2$ is a group homomorphism, then G_1/Ker f ; Im f. Any infinite cyclic group is isomorphic to (Z, +) . Any finite cyclic group of order n is isomorphic to (Z , +) . Let G be a group, $H \leq G$, $K \triangleq G$. Then H/ (H I K) ; HK) /K. Let G be a group, $H \triangleq G$, $K \triangleq G$, $K \subseteq H$, Then (G/K) / (H/K) ; G/H.

The set of automorphism of a group G, Aut G, is a group with respect to the composition of functions. Inn G $\triangleq$ Aut G, for any group G. G/Z (G) ; Inn G, for any group G.

2.5 KEYWORDS

1. Group homomorphism: Iff : G1 $\to$ G2 and g : G2 G3 are two group homomorphisms, then the composite map g . f : G1 $\to$ G3 is also a group homomorphism.
2. Isomorphisms: Let G1 and G2 be two groups. A homomorphism f : G1 $\to$ G2 is called an isomorphism if f is 1-1 and onto.

2.6 QUESTIONS FOR REVIEW

1. Let G be a group and $H \Delta G$. Show that there exists a group G1 and a homomorphism
   f : G $\to$ G1 such that Ker f = H.
2. Show that the homomorphic image of a cyclic group is cyclic i.e., if G is a cyclic group and f : G $\to$ G' is a homomorphism, then f (G) is cyclic.
3. Show that Z = nZ, for a fixed integer n,

(Hint: Consider f : (Z, +) $\rightarrow$ (nZ, +) : f (k) = nk)

4. Is f : Z $\rightarrow$ Z : f (x) = 0 a homomorphism?
5. Describe outer automorphisms.

2.7 SUGGESTED READINGS AND REFERENCES

1. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
2. Paul B. Garrett (2007) . *Abstract Algebra*. Chapman and Hall/CRC.
3. Vijay K Khanna (2017) .*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
4. LALJI PRASAD (2016) . *Modern Abstract Algebra*. Paramount Publication
5. Stephen Lovett (2016) . *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

2.8 ANSWERS TO CHECK YOUR PROGRESS

1. (b) (answer for Check your Progress-1 Q.1)
2. (a) (answer for Check your Progress-1 Q.2)
3. (b) (answer for Check your Progress-2 Q.3)
4. (a) (answer for Check your Progress-2 Q.4)

UNIT - 3: PERMUTATION GROUPS

STRUCTURE

3.0 OBJECTIVES

After studying this unit, you should be able to:

- Discuss the concept of permutation group
- Explain the symmetric group
- Describe the cyclic decomposition
- Prove and use Cayley's Theorem

3.1 INTRODUCTION

In earlier classes, you have studied about the symmetric group. As you have often seen in previous units, the symmetric groups S, as well as its subgroups, have provided us a lot of examples. The symmetric groups and their subgroups are called permutation groups. It was the study of permutation groups and groups of transformations that gave the foundation to group theory. In this unit, we will prove a result by the mathematician Cayley, which says that every group is isomorphic to

permutations group. This result is what makes permutation groups so important.

3.2 GROUPS

In earlier units, you have studied that a permutation on n non-empty set X is a bijective function from X onto X. We denote the set of all permutations on X by S (X) .

3.3.1 Symmetric Group

Suppose X is a finite set having n elements. For simplicity, we take these elements to be
1, 2, . . . , n. Then, we denote the set of all permutations on these n symbols by S_n.

We represent any $f \in S_n$ in n 2-line form as

$$f = \begin{pmatrix} 1 & 2 & .... & n \\ f(1) & f(2) & .... & f(n) \end{pmatrix}.$$

Now, there are n possibilities for f (l) , namely, 1, 2, . . . , n. Once f (1) has been specified, there are (n – 1) possibilities for f (2) , namely, { 1, 2, . . . , n } \ { f (1) } . This is because f is 1-1. Thus, there are n (n – 1) choices for f (1) and f (2) . Continuing in this manner, we see that there are n! different ways in which f can be defined. Therefore, S, has n! element.

Now, let us discuss at the algebraic structure of S (X) , for any set X. The composition of permutations is a binary operation on S (X) . To help you regain practice in computing the composition of permutations, consider an example.

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ be in S_4.

Then, to get fog we first apply g and then apply f.

$\therefore$ f o g (1) = f (g (1)) = f (4) = 3.

f o g (2) = f (g (2)) f (1) = 2.

f o g (3) = f (g (3)) = f (3) = 1.

$f \circ g\ (4) = f(g(4)) = f(2) = 4.$

$\therefore \qquad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

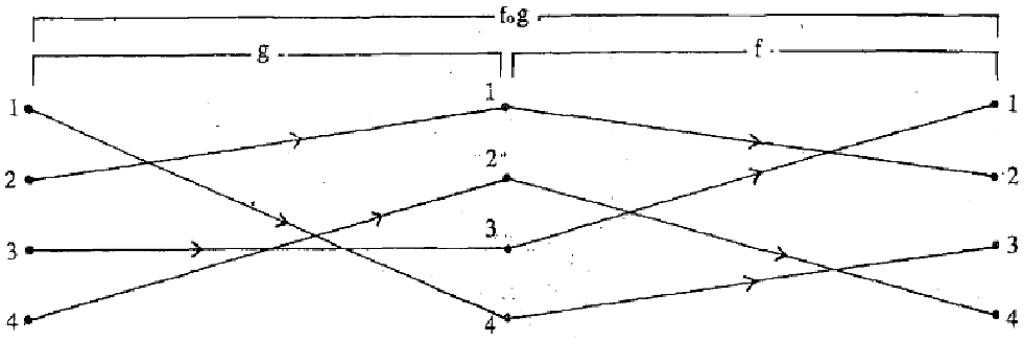


Figure: Example Showing Symmetric Group

Now, let us go back to S (X) , for any set k.

Theorem: Let X be a non-empty set. Then the system (S (X) , 0) forms a group, called the symmetric group of X.

Thus, S_n is a group of order n!. We call S_n, the symmetric group of degree n. Note that if $f \in S_n$, then $f^{-1} = \begin{pmatrix} f(1) & f(2) & .... & f(n) \\ 1 & 2 & .... & n \end{pmatrix}$.

Remark: From now we will refer to the composition of permutations as multiplication of permutations. We will also drop the composition sign. Thus, we will write f o g as fg. The two-line notation that we have used for a permutation is rather cumbersome. In the next section we will see how to use a shorter notation.

3. 3 .2 Cyclic Decomposition

Let us first discuss what a cycle is.

Consider the permutation f = . Choose any one of the symbols say 1.

Now, we write down a left hand bracket followed by I : (1

Since f maps 1 to 3, we write 3 after 1 : (1 3

Since f maps 3 to 4, we write 4 after 3 : (1 3 4

Since f maps 4 to 2, we write 2 after 4 : (l 3 4 2

Since f maps 2 to 1 (the symbol we started with) ,
we close the brackets after the symbol (1 3 4 2)

Thus, we write f = (1 3 4 2) . This means that f maps each symbol to the symbol on its right, except for the final symbol in the brackets, which is mapped to the first.

If we had chosen 3 as our starting symbol we would have obtained the expression (3 4 2 1) for f. However, this means exactly the same as (1 3 4 2) , because both denote the permutation which we have represented diagrammatically in Figure 8.2.

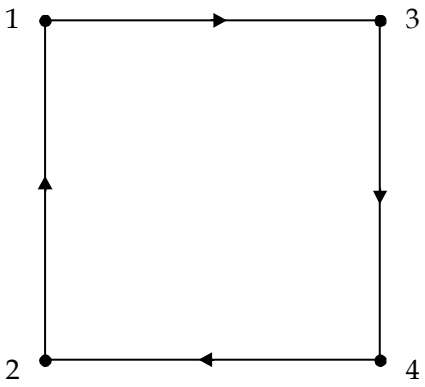


Figure: (1 3 4 2)

Such a permutation is called a 4-cycle, or a cycle of length 4. Figure 8.2 can give you an indication as to why we give this name.

Let us give a definition now.

Definition: A permutation $f \in S_n$, is called an r-cycle (or cycle of length r) if there are r distinct integers $i_1, i_2, i_3, \ldots, i_r$ lying between 1 and n such that

$f(i_1) = i_2, f(i_2) = i_3, \ldots\ldots, f(i_{,-1}) = i_r, f(i_r) = i_1.$

and $f(k) = k \;\; k \notin \{ i_1, i_2, \ldots, i_r \}$.

Then, we write $f = (i_1\, i_2 \ldots\ldots i_r)$.

In particular, 2-cycles are called transpositions. For example, the permutation f = (2 3) $\in S_3$ is a transposition. Here f (1) = 1, f (2) = 3 and f (3) = 2.

Later you will see that transpositions play a very important role in the theory of permutations.

Now consider any 1-cycle (i) in S,. It is simply the identity permutation $I = \begin{pmatrix} 1 & 2 & .... & n \\ 1 & 2 & .... & n \end{pmatrix}$, since it maps i to i and the other $(n - 1)$ symbols to themselves.

Let us see some examples of cycles in S_3 $(1\ 2\ 3)$ is the 3-cycle that takes 1 to 2, 2 to 3 and 3 to 1. There are also 3 transpositions in S_3, namely, $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$.

Now, can we express any permutation as a cycle? No. Consider the following example from S_5. Let g be the permutation defined by

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

If we start with the symbol 1 and apply the procedure for obtaining a cycle to g, we obtain
$(1\ 3\ 4)$ after three steps, Because, g maps 4 to 1, we close the brackets, even though we have not yet written down all the symbols. Now we simply choose another symbol that has not appeared so far, say 2, and start the procedure of writing a cycle again. Thus, we obtain another cycle $(2\ 5)$. Now, all the symbols are exhausted.

$\therefore \quad g = (1\ 3\ 4)\ (2\ 5)$.

We call this expression for g a product of a 3-cycle and a transposition. In Figure 8.3 we represent g by a diagram which shows the 3-cycle and the 2-cycle clearly.

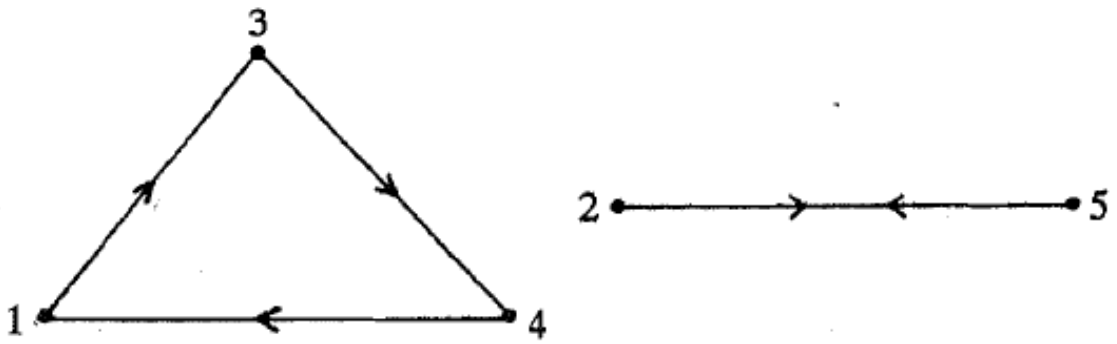


Figure: (1 3 4) (2 5)

Because of the arbitrary choice of symbol at the beginning of each cycle, there are many ways of expressing g. For example,

g = (4 1 3) (2 5) = (2 5) (1 3 4) = (5 2) (3 4 1) .

That is, we can write the product of the separate cycles in any order, and the choice of the starting element within each cycle is arbitrary.

So, you see that g can't be written as a cycle; it is a product of disjoint cycles.

Definition: We call two cycle disjoint if they have no symbol in common. Thus, disjoint cycles move disjoint sets of elements, (Note that f Î S,, moves a symbol i if f (i) ≠ i. We say that f fixes i if f (i) = i.)

So, for example, the cycles (1 2) and (3 4) in S_4 are disjoint. But (1 2) and (1 4) are not disjoint, since they both move 1.

Note that if f and g are disjoint, then fg=-gf, since f and g move disjoint sets of symbols.

Now let us examine one more example. Let h be the permutation in S_5 defined by

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

Following our previous rules, we obtain

h = (1 4 5) (2) (3) ,

because each of the symbols 2 and 3 is left unchanged by h. By convention, we don't include the 1-cycles (2) and (3) in the expression for h unless we wish to emphasize them, since they just represent the identity permutation. Thus, we simply write h = (1 4 5) .

The same process that we have just used is true for any cycle. That is, any r-cycle (i_1 i_2 . . . . . i_r) can be written as (i_1 i_r) (i_1 i_1) . . . . . (i_1 i_2) , a product of transpositions.

Now we will use Theorem 2 to state a result which shows why transpositions are so important in the theory of permutations.

Theorem: Every permutation in S_n $(n \geq 2)$ can be written as a product of transpositions.

Proof: The proof is really very simple. By Theorem 1 every permutation, apart from I, is a product of disjoint cycles. Also, you have just seen that every cycle is a product of transpositions. Hence, every permutation, apart from I, is a product of transpositions.

Also, I = (1 2) (1 2). Thus, I is also a product of transpositions. So, the theorem is proved.

Let us see how Theorem 3 works in practice. This is the same as (1 4) (1 2) (1 3) (1 5).

Similarly, the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$

= (1 3 4) (2 6 5) = (1 4) (1 3) (2 5) (2 6).

The decomposition given in Theorem 3 leads us to a subgroup of S_n that we will now discuss.

3.3.3 Alternating Group

You have seen that a permutation in S_n can be written as a product of transpositions. But all such representations have one thing in common – if a permutation in S_n is the product of an odd number of transpositions in one such representation, then it will be a product of an odd number of transpositions in any such representation. Similarly, if $f \in S_n$ is a product of an even number of transpositions in one representation, then f is a product of an even number of transpositions in any such representation. To see this fact we need the concept of the signature or sign function.

Definition: The signature of $f \in S_n$, $(n \geq 2)$ is defined to be

$$\text{sign } f = \prod_{i,j=1} \frac{f(i) - f(i)}{j - i}$$

For example, for f = (1 2 3) $\in S_3$,

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

Similarly, iff = (1 2) $\in S_3$, then

$$\text{sign f} = \frac{f(2)-f(1)}{2-1}\cdot\frac{f(3)-f(1)}{3-1}\cdot\frac{f(3)-f(2)}{3-2}$$

$$= \left(\frac{1-2}{1}\right)\left(\frac{3-2}{2}\right)\left(\frac{3-1}{1}\right) = -1.$$

Henceforth, whenever we talk of sign f, we shall assume that f $\in S_n$ for some $n \geq 2$.

Theorem: Let f, g $\in$ S,. Then sign (f o g) = (sign f) (sign g) .

Proof: By definition,

$$\text{sign fog} = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{f(g(j))-f(g(i))}{j-i}$$

$$= \prod_{i,j}\frac{f(g(j))-f(g(i))}{g(j)-g(i)}\cdot\prod_{i,j}\frac{g(j)-g(i)}{j-i}$$

Now, as i and j take all possible pairs of distinct values from 1 to n, so do g (i) and g (j) , since g is a bijection.

$$\therefore \quad \prod_{i<j}\frac{f(g(j))-f(g(i))}{g(j)-g(i)} = \text{sign f.}$$

$\therefore$ sign (fog) = (sign f) (sign g) .

Now we will show that Im (sign) = (1, – 1 } .

Theorem: (a) If t $\in$ S, is a transposition, then sign t = – 1.

(b) sign f = 1 or - 1 f $\in$ S,.

(c) Im (sign) = (1, –1) .

Proof: (a) Let t = (p q) , where p < q.

Now, only one factor of sign t involves both p and q, namely,

$$\frac{t(q)-t}{q-p} = \frac{p-1}{q-p} = 1.$$

Every factor of sign t that doesn't contain p or q equals 1, since

$$\frac{t(i)-t(j)}{i-j} = \frac{i-j}{i-j} = 1, \text{ if } i, j \neq p, q.$$

The remaining factors contain either p or q, but not both. These can be paired together to form one of the following products.

$$\frac{t(i)-t(p)}{i-p}\cdot\frac{t(i)-t(q)}{i-q}=\frac{i-q}{i-p}\cdot\frac{i-p}{i-q}=1, \text{ if } i>q,$$

$$\frac{t(p)-t(i)}{p-i}\,\frac{t(q)-t(i)}{q-i}=\frac{q-i}{p-i}\cdot\frac{p-i}{q-i}=1, \text{ if } i>p,$$

Taking the values of all the factors of sign t, we see that sign t = –1.

(b) Let $f \in S$,. By Theorem 3 we know that $f = t_1,t_2 \ldots t$, for some transpositions $t_1, \ldots t_r$ in S_n.

$\therefore$ sign f = sign ($t_1\ t_2 \ldots t$,)

= (sign t_1) (sign t_2) . . . . . sign (t_r) , by Theorem 3.

= (-1) ^{r}, by (a) above.

$\therefore$ sign f = 1 or –1.

(c) We know that Im (sign) $\subseteq$ { 1, – 1 } .

We also know that sign t = –1, for any transposition t; and sign I = 1.

$\therefore$ { 1, – 1 } $\subseteq$ Im { sign }

$\therefore$ Im (sign) = { 1, –1 } .

Now, we are in a position to prove what we said at the beginning of this section.

Theorem: Let $\phi \in S$, and let

$f = t_1t_2 \ldots t_r = t_1' t_2' \ldots t_4'$

be two factorisations off into a product of transpositions. Then either both r and s are even integers, or both are odd integers.

Proof: We apply the function sign: S_n □ { 1, –1 } to $f = t_1t_2 \ldots t_r$.

By Theorem 4 we see that

sign f = (sign t_1) (sign t_2) ..... (sign t_r) = (- 1) '.

$\therefore$ sign ($t_1' t_2' \ldots t_s'$) = (–1) substituting $t_1' t_2' \ldots ts'$ for f.

that is, (-1) ^{s} = (–1) ^{r}.

This can only happen if both s and rare even, or both are odd.

So, we have shown that for $f \in S$, the number of factors occurring in any factorisation of into transposition is always even or always odd.
Therefore, the following definition is meaningful.

Definition: A permutation $f \in S_n$, is called even if it can be written as a product of an even sign number of transposition. f is called odd if it can be represented as a product of an odd number of transpositions.

For example, $(1\ 2) \in S_3$ is an odd permutation. In fact, any transposition is an odd permutation. On the other hand, any 3-cycle is an even permutation, since

$(i\ j\ k) = (i\ k)\ (i\ j)$

Now, we define an important subset of S_n, namely,

A, = (f ∈ Sn, | f is even) .

We'll show that A,, Δ S_n, and that o (A_n) = $\frac{n!}{2}$, for n ≥ 2.

Theorem: The set A,, of even permutations in S,, forms a normal subgroup of S_n, of order $\frac{n!}{2}$.

Proof: Consider the signature function,

sign : $S_n \rightarrow (1, -1)$.

Note that $(1, -1)$ is a group with respect to multiplication. Now, Im (sign) = $(1, -1)$. Let us obtain Ker (sign) .

Ker (sign) = { $f \in S_n$ | sign f = 1 }

= ($f \in S_n$ | f is even)

= A.

$\therefore$ $A \triangleq S_n$.

Further, by the Fundamental Theorem of Homomorphism

S_n/A_n ; $(1, -1)$.

$\therefore$ o (S_n/A_n) = 2, that is, $\frac{o(S_n)}{o(A_n)} = 2.$

$\therefore$ o (An) = $\frac{o(S_n)}{2} = \frac{n!}{2}.$

Note that this theorem says that the number of even permutations in S, equals the number of odd permutations in S,.

Theorem leads us to the following definition.

Definition: A,, the group of even permutations in S_n, is called the alternating group of degree n.

Let us look at an example that you have already seen in previous units,

A_3. Now, Theorem says that o (A_3) = $\frac{3!}{2} = 3.$ Since (1 2 3) = (1 3) (1 2) , (1 2 3) $\in A_3$. Similarly,

(1 3 2) $\in A_3$. Of course, I $\in A_3$.

$\therefore A_3$ = { I, (1 2 3) , (1 3 2)) .

A fact that we have used in the example above is that an r-cycle is odd if r is even, and even if r is odd. This is because ($i_1 i_2$ .... i_r,) = (i_1 i,) (i_1 i_{r-1}) . . . . . (i_1 i_2) , a product of (r – 1) transpositions.

Now, for a moment, Lagrange's theorem says that the order of the subgroup of a finite group divides the order of the group. We also said that if
n |o (G) , then G need not have a subgroup of order n. Now that you know what A_4 looks like, we are in a position to illustrate this statement.

We will show that A_4 has no subgroup of order 6, even though 6 | o (A_4) . Suppose such a subgroup H exists. Then o (H) = 6, o (A_4) = 12.
$\therefore$ (A_4 : H | = 2. $\therefore$ H A4 (see Theorem 3, Unit 1) . Now, A_4/H is a group of order 2.

(Hg) ^{2} = H $^\forall$ g $\in A_4$. (Remember H is the identity of A_4/H.)

$\therefore$ $g^2 \in$ H $^\forall$ g $\in A_4$.

Now, (1 2 3) E A_4. $\therefore$ (1 2 3) * = (1 3 2) $\in$ H.

Similarly, $(1\,3\,2)^2 = (1\,2\,3) \in H$. By the same reasoning $(1\,4\,2)$, $(1\,2\,4)$, $(1\,4\,3)$, $(1\,3\,4)$, $(2\,3\,4)$, $(2\,4\,3)$ are also distinct element of H. Of course, $I \in H$.

Thus, H contains at least 9 elements.

$\therefore o(H) \geq 9$. This contradicts our assumption that $o(H) = 6$.

Therefore, A_4 has no subgroup of order 6.

We use A_4 to provide another example too. (See how useful A_4 is!) In earlier unit we'd said that if $H \triangleq N$ and $N \triangleq G$, then H need not be normal in 6**.** Well, here's the example.'

Consider the subset $V_4 = \{ I, (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4) \}$ of A_4.

Now, let $H = \{ I, (1\,2)(3\,4) \}$. Then H is a subgroup of index 2 in V_4. $\therefore H \text{ A } V_4$.

So, $H \triangleq V_4$, $V_4 \triangleq A_4$. But $H \not\triangleq A_4$. Why? Well, $(1\,2\,3) \in A_4$ is such that

$(1\,2\,3)^{-1}(1\,2)(3\,4)(1\,2\,3) = (1\,3)(2\,4) \notin H$.

And now let us see why permutation groups are so important in group theory.

Check Your Progress-1

1. If ..... is a group of order n!. Then we call S, the symmetric group of define n.

   (a) S^n (b) S_n

   (c) Sn^1 (d) Sn^{-1}

2. Every permutation is S_n ($n \geq$ .....) can be written as produce of transposition

   (a) $n \geq 2$ (b) $n \geq 3$

   (c) $n \geq 4$ (d) $n \geq 5$

3. If $t \in S$, is a transposition then sight = ...

(a) –1 (b) 1

(c) 0 (d) 2

3.3 CAYLEY'S THEOREM

Most finite groups that first appeared in mathematics were groups of permutations. It was the English mathematician Clayley who first realised that every group has the algebraic structure of a subgroup of **S (X) ,** for some set X. In this section we will discuss Cayley's result and some of its applications.

Theorem (Cayley) : Any group G is isomorphic to a subgroup of the symmetric group S (G) .

Proof: For a $\in$ G, we define the left multiplication function

$f_a : G \to G : f_4 (x) = ax.$

f_a is 1-1, since

fa (x) = fa (y) $\Rightarrow$ ax = ay $\Rightarrow$ x = y x, y E G.

fa is onto, since any x E G is **f,** (a – 'x) .

:. $f_a \in S (G) \ \forall \ a \in G.$

(Note that S (G) is the symmetric group on the set G.)

Now we define a function f : G $\to$ S (G) : f (a) = fa.

We will show that f is an injective homomorphism. For this we note that

$(f_{ao}, f_b) \ (x) = f_a (bx) = abx = f_{ab} \ (x) \ \forall \ a, b \in G.$

$\therefore$ f (ab) = $f_{ab} = f_a$ o f_b = f (a) of (b) $\forall$ a, b $\in$ G.

That is, f is a homomorphism.

Now, Ker f = (a $\in$ G | fa = I_G)

= (a $\in$ G | f_a (x) =x $\forall$ x $\in$ G }

= (a $\in$ G |a x = x $\forall$ x $\in$ G }

= { e } .

Thus, by the Fundamental Theorem of Homomorphism,

G/Ker f ; Im f ≤ S (G) ,

that is, G is isomorphic to a subgroup of S (G) .

As an example of Cayley's theorem, we will show you that the Klein 4-group K_4 is isomorphic to the subgroup V_4 of S_4. The multiplication table for K_4 is

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Check your Progress-2

4. Any group G is ..... to a subgroup of the symmetric group S (G)

   (a) isomorphic (b) homomorphic

   (c) automorphic (d) surjective

5. Any group is isomorphic to a ..... group.

   (a) normal group (b) subgroup

   (c) cyclic group (d) permutation group

.

3.4 LET US SUM UP

The symmetric group S (X) , for any set X, and the group S,, in particular. The definitions and some properties of cycles and transpositions. Any non-identity permutation in S_n can be expressed as a disjoint product of cycles.

Any permutation in S_n (n ≥ 2) can be written as a product of transpositions. The homomorphism sign : S_n — { 1, – 1 } , n ≥ 2. Odd and even permutations. A,, the set of even permutations in S,, is a normal subgroup of S_n of order $\frac{n!}{2}$, for. Any group is isomorphic to a permutation group.

3.5 KEYWORDS

1. ***Symmetric Group:*** Let X be a non-empty set. Then the system (S (Xj, 0) forms a group, called the symmetric group of X.

2. ***Permutation:*** A permutation f ∈ S, is called an r-cycle (or cycle of length r) if there are r distinct integers $i_1, i_2, i_3, \ldots, i_r$ lying between 1 and n.

3.6 QUESTIONS FOR REVIEW

1. Show that (S,, °) is a non-commutative group for n ≥ 3.

(Hint: Check the $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ don't commute.)

2. Write down 2 transpositions, 2 3-cycles and a 5-cycle in S_5.

3. Show that every permutation in S_n is a cyclic iff n < 4.

4. Iff = (i_2 i_2 , ...i) S,, then show that f^{-1} = (i_r i_{r-1} .... $i_2 i_1$) .

5. Iff is an r-cycle, then show that o (f) = r, i.e., $f^r = I$ and $f^5 \neq I$, if s < r.

(Hint: If f = (i_1, i_2 ....i) , then f (i_1) = i_2, r^2 (i_1) = i_3,....,f^{r-1} (i_1) = i_m)

6. Express the following cycles as products of transpositions.

(a) (1 3 5) (b) (5 3 1)

(c) (2 4 5 3)

7. Write the permutation in E3 (b) as a product of transpositions.

8. Show that (1 2 .... 10) = (1 2) (2 3) . . . (9 10) .

9. Check that (V_4, °) is a normal subgroup of A_4.

3.5 SUGGESTED READINGS AND REFERENCES

6. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.

7. Lalji Prasad (2016) . *Modern Abstract Algebra*. Paramount Publication

8. Dan Saracino (2008) .*Abstract Algebra; A First Course*. Waveland Press, Inc.; 2 edition

9. Mitchell and Mitchell (2007) . *An Introduction to Abstract Algebra*. Wadsworth Publishing

10. John B. Fraleigh (2003) . *An Introduction to Abstract Algebra* (Relevant Portion) .Pearson Education

3.6 ANSWERS TO CHECK YOUR PROGRESS

5. (b) (answer for Check your Progress-1 Q.1)
6. (a) (answer for Check your Progress-1 Q.2)
7. (a) (answer for Check your Progress-1 Q.3)
8. (a) (answer for Check your Progress-2 Q.4)
9. (d) (answer for Check your Progress-2 Q.5)

UNIT – 4: GROUP ACTIONS

STRUCTURE

4.0 OBJECTIVES

After studying this unit, you should be able to:

- Discuss direct product of groups
- State Sylow theorem
- Explain groups of order 1 to 10.
- Define finite abelian group

4.1 INTRODUCTION

In the last unit, we have studied about permutation group. This unit will provide you the information related to 15 finite groups and direct products. Let us understand all these one by one.

A group for which the elements commute (i.e., AB = BA for all elements A and B) is called a finite abelian group. All cyclic groups are finite abelian, but a finite abelian group is not necessarily cyclic. All subgroups of a finite abelian group are normal. In a finite abelian group, each element is in a conjugacy class by itself, and the character table involves powers of a single element known as a group generator.

4.2 DIRECT PRODUCT OF GROUPS

In this section, we will discuss a very important method of constructing new groups. We will first see how two groups can be combined to form a third group. Then we will see how two subgroups of a group can be combined to form another subgroup.

4 .2 .1 External Direct Product

In this sub-section we will construct a new group from two or more groups that we already have.

Let $(G_1, *_1)$ and $((G_2, *_2)$ be two groups. Consider their Cartesian product $G = G_1 \times G_2 = \{ (x, y) |$

$x \in G_1, y \in G_2 \}$.

Can we define a binary operation on G by using the operations on G_1 and G_2? Let us try the method, namely, component-wise multiplication. That is, we define the operation * on G by $(a,b) * (c, d) = (a*_1 c,$ $b*_2 d) \ \forall \ a, c \in G_1, b, d \in G_2$.

So, you have proved that $G = G_1 \times G_2$ is a group with respect to *. We call G the external direct product of $(G_1, *_1)$ and $(G_2, *_2)$.

For example, R^2 is the external direct product of R with itself.

Another example is the direct product $(Z, +) \times (R^*, .)$ in which the operation is given by $(m, X) * (n, y) = (m + n, xy)$.

We can also define the external direct product of 3, 4 or more groups on the same lines.

Definition: Let $(G_1, *_1), (G_2, *_2), \ldots\ldots, (G,, *_n)$ be n groups. Their external direct product is the group $(G, *)$, where

$G = G_1 \times G_2 \ldots\ldots \times G_n$ and

Thus, R^n is the external direct product of n copies of R,

We would like to make a remark about notation now.

Remark: Henceforth, we will assume that all the operations $*, *_1, \ldots, *_n$ are multiplication, unless mentioned otherwise. Thus, the operation on $G = G_1 \times G_2 \times \ldots\ldots \times G_n$ will be given by

$(a_1, \ldots\ldots, a) \cdot (b_1, \ldots\ldots, b)$

$= (a_1b_1, a_2b_2, \ldots\ldots, a_aba,)$ $a_i, b_i \in G_i$.

Now, let G be the external direct product $G_1 \times G_2$. Consider the projection map

$T_1 : G_1 \times G_2 \to G_1 : p_1 : (x, y) = x$.

Then π_1 is a group homomorphism, since

$\pi_1 ((a, b)(c, d)) = \pi_1 (ac, bd)$

$= ac$

$= \pi_1 (a, b) \pi_1 (c, d)$

π_1 is also onto, because any $x \in G_1$ is $p_1 (x, e_2)$

Now, let us look at Ker π_1.

Ker $\pi_1 = \{ (x, y) \in G_1 \times G_2 \mid \pi_1 (x, y) = e_1 \}$

$= \{ (e_1, y) \mid y \in Gz \} = \{ e_1 \} \times G_2$.

$\therefore \{ e \} \times G_2 \; G_1 \times G_2$.

Also, by the Fundamental Theorem of Homomorphism $(G_1 \times G_2) / (\{ e_1 \} \times Gz) ; G_1$.

We can similarly prove that $G_1 \times \{ e_2 \} \; G_1 \times G_2$ and $(G_1 \times G_2) / (G_1 \times \{ e_2 \}) ; G_2$.

So, far we have seen the construction of $G_1 \times G_2$ from two groups G_1 and G_2. Now we will see under what conditions we can express a group as a direct product of its subgroups.

4 .2 .2 Internal Direct Product

Let us begin by recalling from previous unit that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. We are interested in the case when HK is the whole of G. We have the following definition.

Definition: Let H and K be normal subgroups of a group G. We call G the internal direct product of H and K if

G = HK and H I K = { e } .

We write this fact as G = H × K.

For example, let us consider the familiar Klein 4-group

K_4 = { e, a, b, ab } , where a^2 = e, b^2 = e and ab = ba.

Let H = <a> and K = <b>. Then H I K = { e) . Also, K_4 = HK.

∴ K_4 = H × K.

Note that H ; Z_2 and K ; Z_2 ∴ K_4 ; $Z_2 \times Z_2$.

For another example, consider Z_{10}. It is the internal direct product of its subgroups H = $\{\bar{0}, \bar{5}\}$ and K = $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$. This is because

(i) Z_{10}= H + K, since any element of Z_{10} is the sum of an element of H and an element of K, and

(ii) H I K= $\{\bar{0}\}$

Now, can an external direct product also be an internal direct product? What does it say? It says that the external product of $G_1 \times G_2$ is the internal product ($G_1 \times \{ e_2 \}$) × ($\{ e_1 \} \times G_2$) .

We would like to make a remark here.

Remark: Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is isomorphic to the external direct

product of H and K. Therefore, when we talk of an internal direct product of subgroups we can drop the word internal, and just say 'direct product of subgroups'.

Let us now extend the definition of the internal direct product of two subgroups to that of several subgroups.

Definition: A group G is the internal direct product of its normal subgroups $H_1, H_2, ... ,H_n$ if

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

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

For example, look at the group G generated by { a, b, c } , where $a^2 = e = b^2 = c^2$ and ab = ba, ac = ca, bc = cb. This is the internal direct product of < a >, < b > and < c >. That is G ; $Z_2 \times Z_2 \times Z_2$.

Now, can every group be written as an internal direct product of two or more of its proper normal subgroups? Consider Z. Suppose $Z = H \times K$, where H, K are subgroups of Z.

You know that H = < m > and K = < n > for some m, n ∈ Z. Then mn ∈ H ∩ K. But if $H \times K$ is a direct product, H ∩ K = { 0 } . So, we reach a contradiction. Therefore, Z can't be written as an internal direct product of two subgroups.

By the same reasoning we can say that Z can't be expressed as $H_1 \times H_2 \times ..... \times H_n$, where $H_i \leq Z \quad i = 1, 2, ... , n.$

When a group is an internal direct product of its subgroups, it satisfies the following theorem.

Theorem : Let a group G be the internal direct product of its subgroups H and K. Then

(a) each x ∈ G can be uniquely expressed as x = hk, where h ∈ H, k ∈ K; and

(b) $hk = kh \quad \forall \; h \in H , k \in K .$

Proof: (a) We know that G = HK. Therefore, if $x \in G$, then x = hk, for some $h \in H$, $k \in K$. Now suppose $x = h_1k_1$ also, where $h_1 \in H$ and $k_1 \in K$. Then $hk = h_1k_1$.

$\therefore h_1^{-1} h = k_1k^{-1}$. Now $h_1^{-1} h \in H$.

Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1} h \in K$. $\therefore h_1^{-1} h \in H \cap K = \{ e \}$.

$\therefore \quad h_1^{-1}h = e$, which implies that $h = h_1$.

Similarly, $k_1 k^{-1} = e$, So that $k_1 = k$.

Thus, the representation of x as the product of an element of H and an element of K is unique.

(b) The best way to show that two elements x and y commute is to show that their commutator $x^{-1}y^{-1} xy$ is identity. So, let $h \in H$ and $k \in K$ and consider h-'k-'hk. Since $K \triangleq G$, $h^{-1}k^{-1} h \in K$.

$\therefore h^{-1}k^{-1}hk \in K$.

By similar reasoning, $h^{-1}k^{-1}hk \in H$. $\therefore h^{-1}k^{-1}hk \in H \cap K = \{ e \}$.

$\therefore \quad h^{-1} k^{-1}hk = e$, that is, hk = kh.

Now let us look at the relationship between internal direct products and quotient groups.

Theorem: Let H and K be normal subgroups of a group G such that $G = H \times K$. Then G/H ; K and G/K ; H.

Proof: We will use Theorem 8 of Unit 1 to prove this result.

Now G = HK and $H \cap K = \{ e \}$. Therefore,

G/H = HK/H ; K/H I K = K/ { e) ; K.

We can similarly prove that G/K ; H.

Theorem: Let G be a finite group and H and K be its subgroups such that G = H X K.

Then o (G) = o (H) o (K) .

Check Your progress-1

1. Let a group G be the ..... product of its subgroups H and k. Then hk = kh $h \in H, k \in K$.

   (a) external (b) internal

   (c) finite (d) infinite

2. Let H and k be normal subgroups of a group G such that $G = H \times k$. Then G/H ..... and G/k H

   (a) k (b) H

   (c) H^{-1} (d) $k^{-1'}$

4.3 INTRODUCTION TO SYLOW THEOREMS

In Lagrange's theorem, which says that the order of a subgroup of a finite group divides the order of the group. We also said that if G is a finite cyclic group and m | o (G) , then G has a subgroup of order. But if G is not cyclic, this statement need not be true, as you have seen in the previous unit. In this context, in 1845 the mathematician Cauchy proved the following useful result.

Theorem : If a prime p divides the order of a finite group G, then G contains an element of order p.

The proof of this result involves a knowledge of group theory that is beyond the scope of this course. Therefore, we omit it.

Theorem : If a prime p divides the order of a finite group G, then G contains a subgroup of order p.

Proof: Just take the cyclic subgroup generated by an element of order p. This element exists because of Theorem.

So, by Theorem we know that any group of order 30 will have a subgroup of order 2, a subgroup of order 3 and a subgroup of order 5. In 1872 Ludwig Sylow, a Norwegian mathematician, proved a remarkable extension of Cauchy's result. This result, called the first Sylow theorem, has turned out to be the basis of finite group theory. Using this result we

can say, for example, that any group of order 100 has subgroups of order 2, 4, 5 and 25.

Theorem: Let G be a finite group such that o (G) = $p^n m$, where p is a prime, $n \geq 1$ and (p, m) = 1. Then G contains a subgroup of order pk k = 1, . . . , n.

We shall not prove this result or the next two Sylow theorems either. But, after stating all these results we shall show how useful they are.

The next theorem involves the concepts of conjugacy and Sylow p-subgroups which we now define.

Definition: Two subgroups H and K of a group G are conjugate in G if $\exists$ $g \in G$ such that $K = g^{-1}Hg$ and then K is called a conjugate of H in G.

Now we define Sylow p-subgroups.

Definition: Let G be a finite group and p be a prime such that $p^n \mid o(G)$ but p^{n+1} o (G) , for some $n \geq 1$. Then a subgroup of G of order pn is called a Sylow p-subgroup of G.

So, if o (G) = $p^n m$, (p, m) = I, then a subgroup of G of order p" is a Sylow p-subgroup. Theorem 6 says that this subgroup always exists. But, a group may have more than one Sylow p-subgroup. The next result tells us how two Sylow p-subgroups of a group are related.

Theorem : Let G be a group such that o (G) = $p^n m$, (p, m) = 1, p a prime. Then any two Sylow p-subgroups of G are conjugate in G.

And now let us see how many Sylow p-subgroups a group can have.

Theorem : Let G be a group of order $p^n m$, where (p, m) = 1 and p is a prime. Then n_p, the number of distinct Sylow p-subgroups of G, is given by $n_p = 1 + kp$ for some $k \geq 0$. And further, $n_p \mid o(G)$.

We would like to make a remark about the actual use of Theorem 8.

Remark: Theorem 8 says that $n_p, \equiv 1 \pmod p$. (n_p, pn) = 1. Also, since np | o (G) , using Theorem we find that $n_p \mid m$. This fact helps us to cut down the possibilities for n,, as you will see in the following examples.

Example: Show that any group of order 15 is cyclic.

Solution: Let G be a group of order 15 = 3 × 5. Theorem 6 says that G has a Sylow 3-subgroup. Theorem 8 says that the number of such subgroups must divide 15 and must be congruent to l (mod 3) . In fact, by Remark 3 the number of such subgroups must divide 5 and must be congruent to l (mod 3) . Thus, the only possibility is 1. Therefore, G has a unique Sylow 3-subgroup, say H. Hence, by Theorem 7 we know that $H \triangleq G$. Since H is of prime order, it is cyclic.

Similarly, we know that G has a subgroup of order 5. The total number of such subgroups is 1,6 or 11 and must divide 3. Thus, the only possibility is 1. So G has a unique subgroup of order 5, say K. Then $K \triangleq G$ and K is cyclic.

Now, let us look at H I K. Let $x \in H \cap K$. Then $x \in H$ and $x \in K$.

$\therefore$ $o(x) \mid o(H)$ and $o(x) \mid o(K)$ i.e., $o(x) \mid 3$ and $o(x) \mid 5$.

$\therefore$ $o(x) = 1$. $\therefore x = e$. That is, $H \cap K = \{e\}$. Also,

$\therefore$ $G = HK$.

So, $G = H \times K$; $Z_3 \times Z_5 = Z_{15}$,

Example: Show that a group *G* of order 30 either has a normal subgroup of order 5 or a normal subgroup of order 3, i.e. G is not simple. A group G is called simple if its only normal subgroups.

Solution: Since 30 = 2 × 3 × 5, G has a Sylow 2-subgroup, a Sylow 3-subgroup and a Sylow 5-subgroup. The number of Sylow 5-subgroups is of the form 1 + 5k and divides 6. Therefore, it can be 1 or ***6.*** If it is 1, then the Sylow 5-subgroup is normal in G.

On the other hand, suppose the number of Sylow 5-subgroups is 6. Each of these subgroups are distinct cyclic groups of order 5, the only common element being e. Thus, together they contain 24 + 1 = 25 elements of the group. So, we are left with 5 elements of the group which are of order 2 or 3. Now, the number of Sylow 3-subgroups can be 1 or 10. We can't have 10 Sylow
3-subgroups, because we only have at most 5 elements of the group

which are of order 3. So, if the group has 6 Sylow 5-groups then it has only 1 Sylow 3-subgroup.

Now let us use the powerful Sylow theorems to classify groups of order 1 to 10. In the process we will show you the algebraic structure of several types of finite groups.

Check your progress-2

3. Let G ..... be and H and k be its subgroup such that G = H × k. Thus O (G) = O (H) o (k) .

   (a) external (b) internal

   (c) finite (d) infinite

4. If a prime p divides the order of a finite group G, then G contains an element of .....

   (a) P (b) G

   (c) Q (d) R

4.4 GROUPS OF ORDER 1 TO 10

Here, we will apply the results of the above discussion to study some finite groups. In particular, we will list all the groups of order 1 to 10, up to isomorphism.

We start with proving a very useful result.

Theorem : Let G be a group such that o (G) = pq, where p, q are primes such that p > q and $q \nmid p - 1$. Then G is cyclic.

Proof: Let P be a Sylow p-subgroup and Q be a Sylow q-subgroup of G. Then o (P) = p and
o (Q) = q. Now, any group of prime order is cyclic, so P = < x > and Q = < y > for some x, y $\in$ G.
By the third Sylow theorem, the number n_p of subgroups of order p can be 1 , 1+ p, 1 + 2p, . . . , and it must divide q. But p > q. Therefore, the only possibility for n_p is 1. Thus, there exists only one Sylow p-subgroup, i.e., P. Further, by Sylow's second theorem P $\triangleq$ G.

Again, the number of distinct Sylow q-subgroups of G is n_q, = 1 + kq for some k, and n, | p. Since p is a prime, its only factors are 1 and p. ∴ n, = 1 or n_q = p. Now if 1 + kq = p, then q | p – 1. But we started by assuming that 9 $\not|$ p - 1. So we reach a contradiction. Thus, n_q = 1 is the only possibility. Thus, the Sylow q-subgroup Q is normal in G.

Now we want to show that G = P × Q. For this, let us consider P I Q. The order of any element of P I Q must divide up as well as q, and hence it must divide (p, q) = 1.

P I Q = { e } . ∴ o (PQ) = o (P) o (Q) = pq = o (G) . ∴ G = PQ.

So we find that G = P × Q ; $Z_p \times Z_p$; Z_{pq},

Therefore, G is cyclic of order pq.

Using Theorem, we can immediately say that any group of order 15 is cyclic. Similarly, if
o (G) = 35, then G'is cyclic.

Now if q | p – 1, then does o (G) = pq imply that G is cyclic? Well, consider S_3. You know that o (S_3) = 6 = 2.3, but S_3 is not cyclic. In fact, we have the following result.

Theorem: Let G be a group such that o (G) = 2p, where p is an odd prime, Then either G is cyclic or G is isomorphic to the dihedral group D_{2p} of order 2p.

(Recall that D_{2p} = < (x, y | x^P = e = Y^2 and yx = x^{-l}y } > .)

Proof: As in the proof of Theorem 9, there exists a subgroup P = < x > of order p with

P $\triangleq$ G and a subgroup Q = < y > of order 2, since p > 2. Since (2, p) = 1,

P I Q = { e } . ∴ o (PQ) = o (G) .

∴ G = PQ.

Now, two cases arise, namely, when Q $\triangleq$ G and when QG.

If Q $\triangleq$ G, then G = P × Q. And then G = <xy>.

If Q is not normal in G, then G must be non-abelian.

(Remember that every subgroup of an abelian group is normal.)

$\therefore xy \neq yx.$ $\therefore y^{-1}xy \neq x.$

Now, since P = < x > $\triangleq$ G, $y^{-1}xy \in P. \therefore y^{-1}xy = x'$, for some r = 2 ,... . , p - 1.

Therefore, $y^{-2}xy^2 = y^{-1}$ ($y^{-1}xy$) = $y^{-1}x^ry$ = ($y^{-1}xy$) ^{r} = (x^r) ^{r} =

$\Rightarrow$ x = since o (y) = 2.

$\Rightarrow$.

But o (x) = p. Therefore, by Theorem 4, p | $r^2 - 1$, i.e., p | (r – 1) (r + 1)

$\Rightarrow$ p | (r – 1) or p | (r + 1) . But $2 \leq r \leq p - 1.$ $\therefore$ p = r + l,

i.e., r = p – 1. So we see that

y^{-1} xy = x^r =' $x^{p-1} = x^{-1}$

So, G = PQ = < { x, y | x^p = e, y^2 = e, $y^{-1}xy = x^{-1}$ > , which is exactly the same algebraic structure as that of D_{2p}.

$\therefore$ G = D_{2p} = { e, x, x^2, ... , x^{p-1}, y, xy, x^2 y, ... , x^{p-1}y]

Example: What are the possible algebraic structures of a group of order 6?

Solution: Let G be a group of order 6. Then, by theorem 10, G ; Z_6 or G ; Ds. You must have already noted that S_3 ; D_6. So, if G is not cyclic, then G ; S_3.

Now, we know that if o (G) is a prime, then G is cyclic. Thus, groups of orders 2, 3, 5 and 7 are cyclic. This fact allows us to classify all groups whose orders are 1, 2, 3, 5, 6, 7 or 10. What about the structure of groups of order 4 = 22 and 9 = 3^2? Such groups are covered by the following result.

Theorem: If G is a group of order p^2, p a prime, then G is abelian.

We will not prove this result, since its proof is beyond the scope of this course. But, using this theorem, we, can easily classify groups of order p^2.

Theorem: Let G be a group such that o (G) = p^2, where p is a prime. Then either G is cyclic or G = $Z_p \times Z_p$, a direct product of two cyclic groups of order p.

Proof: Suppose G has an element a of order p^2. Then G = < a > .

On the other hand, suppose G has no element of order. Then, for any x E G, o (x) = I or o (x) = p.

Let $x \in G$, $x \neq e$ and H = < x > . Since $x \neq e$, o (H) $\neq 1$

$\therefore$ o (H) = p.

Therefore, $\exists\ y \in G$ such that $y \notin H$. Then, by the same reasoning, K = < y > is of order p. Both H and K are normal in G, since G is abelian.

We want to show that G = H × K. For this, consider H I K. Now H I K ≤ H.

$\therefore$ o (H I K) | o (H) = p. o (H I K) = 1 or o (H I K) = p.

If o (H I K) = p, then H I K = H, and by similar reasoning, H I K = K. But then,

H = K. $\therefore\ y \in H$, a contradiction.

o (H I K) = 1, i.e., H I K = { e } .

So, H G, KG, H I K = { e } and o (HK) = p^2 = o (6) .

$\therefore$ G = H × K ; $Z_p \times Z_p$.

So far we have shown the algebraic structure of all groups of order 1 to 10, except groups of order 8. Now we will list the classification of groups of order 8.

If G is an abelian group of order 8, then

(i) G ; Z_8, the cyclic group or order 8, or

(ii) G ; $Z_4 \times Z_2$, or

(iii) G ; $Z_2 \times Z_2 \times Z_2$.

If G is a non-abelian group of order 8, then

(i) G ; Q_8, the quaternion group, or

(ii) G ; D_8, the dihedral group.

So, we have seen what the algebraic structure of any group of order 1, 2, ... , 10 must be. We have said that this classification is up to isomorphism. So, for example, any group of order 10 is isomorphic to Z_{10} or D_{10}. It need not be equal to either of them.

Check Your progress- 3

5. If a prime P divides the order of a finite group G, then G contains a ..... of order P.

(a) subgroup (b) normal

(c) cycle (d) permutation

6. A ..... is a set, A together with an operations ".". That combines any two elements a and b to form another element denoted a.b.

(a) cyclic (b) permutation

(c) abelian (d) normal

4.5 FINITE ABELIAN GROUPS

In Mathematica, the function finite abelian group [{ n_1, n_2 ... }] represents the direct product of the cyclic groups of degrees n_1 n_2 ...

4.5.1 Definition

A finite abelian group is a set, A, together with an operation "•" that combines any two elements a and b to form another element denoted a • b. The symbol "•" is a general placeholder for a concretely given operation. To qualify as a finite abelian group, the set and operation,

$(A, \bullet)$, must satisfy five requirements known as the *finite abelian group axioms*:

Closure

For all a, b in A, the result of the operation a • b is also in A.

Associatively

For all *a*, *b* and *c* in *A*, the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity Element

There exists an element *e* in *A*, such that for all elements *a* in *A*, the equation $e \bullet a = a \bullet e = a$ holds.

Inverse Element

For each *a* in *A*, there exists an element *b* in *A* such that $a \bullet b = b \bullet a = e$, where *e* is the identity element.

Commutatively

For all *a*, *b* in *A*, $a \bullet b = b \bullet a$.

More compactly, a finite abelian group is a commutative group. A group in which the group operation is not commutative is called a “non-finite abelian group” or “non-commutative group”.

You should notice that any field is a finite abelian group under addition. Furthermore, under multiplication, the set of non-zero elements of any field must also form a finite abelian group. Of course, in this case the two operations are not independent–they are connected by the distributive laws.

The definition of a finite abelian group is also useful in discussing vector spaces and modules. In fact, we can define a vector space to be a finite abelian group together with a scalar multiplication satisfying the relevant axioms. Using this definition of a vector space as a model, we can state the definition of a module in the following way.

4.5.2 Properties

Let us assume that, If n is a natural number and x is an element of a finite abelian group G written additively, then nx can be defined as x + x + ... + x (n summands) and (–n) x = – (nx) . In this way, G becomes a module over the ring Z of integers. In fact, the modules over Z can be identified with the finite abelian groups.

Theorems about finite abelian groups can often be generalized to theorems about modules over an arbitrary principal ideal domain. A typical example is the classification of finitely generated finite abelian groups which is a specialization of the structure theorem for finitely generated modules over a principal ideal domain. In the case of finitely generated finite abelian groups, this theorem guarantees that a finite abelian group splits as a direct sum of a torsion group and a free finite abelian group. The former may be written as a direct sum of finitely many groups of the form Z/p^kZ for p prime, and the latter is a direct sum of finitely many copies of Z.

If f, g : G $\rightarrow$ H are two group homomorphisms between finite abelian groups, then their sum
f + g, defined by (f + g) (x) = f (x) + g (x) , is again a homomorphism. (This is not true if H is a non-finite abelian group.) The set Hom (G, H) of all group homomorphisms from G to H thus turns into a finite abelian group in its own right.

Somewhat kind to the dimension of vector spaces, every finite abelian group has a rank. It is defined as the cardinality of the largest set of linearly independent elements of the group. The integers and the rational numbers have rank one, as well as every subgroup of the rationals.

4.5.3 Notation

There are two main notational conventions for finite abelian groups: '+' additive and '.' multiplicative.

Convention	Operation	Identity	Powers	Inverse
Addition	$x + y$	0	nx	$-x$
Multiplication	$x * y$ or xy	e or 1	x^n	x^{-1}

Figure: Notational Conventions

Generally, the multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules. The additive notation may also be used to emphasize that a particular group is abelian, whenever both abelian and non-finite abelian groups are considered.

Multiplication Table

To verify that a finite group is abelian, a table (matrix) - known as a Cayley table - can be constructed in a similar fashion to a multiplication table. If the group is $G = \{ g_1 = e, g_2, ..., g_n \}$ under the operation ", the (i, j) 'th entry of this table contains the product $g_i . g_j$. The group is abelian if and only if this table is symmetric about the main diagonal.

This is true since if the group is abelian, then $g_i . g_j = g_j . g_i$. This implies that the (i, j) 'th entry of the table equals the (j, i) 'th entry, thus the table is symmetric about the main diagonal.

Examples:

1. For the integers and the operation addition "+", denoted (**Z**,+) , the operation + combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer n has an additive inverse, $-n$, and the addition operation is commutative since $m + n = n + m$ for any two integers m and n.
2. Every cyclic group G is abelian, because if x, y are in G, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Thus the integers, **Z**, form a finite abelian group under addition, as do the integers modulo n, $\mathbf{Z}/n\mathbf{Z}$.

3. Every ring is a finite abelian group with respect to its addition operation. In a commutative ring the invertible elements, or units, form an abelian multiplicative group. In particular, the real numbers are a finite abelian group under addition, and the non-zero real numbers are a finite abelian group under multiplication.
4. Every subgroup of a finite abelian group is normal, so each subgroup gives rise to a quotient group. Subgroups, quotients, and direct sums of finite abelian groups are again abelian.

In general, matrices, even invertible matrices, do not form a finite abelian group under multiplication because matrix multiplication is generally not commutative. However, some groups of matrices are finite abelian groups under matrix multiplication - one example is the group of 2 x 2 rotation matrices.

Example*:* Find all finite abelian groups of order 108 (up to isomorphism) .

Solution: The prime factorization is $108 = 2^2 \cdot 3^3$. There are two possible groups of order 4: $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$. There are three possible groups of order 27: $\mathbf{Z}_{27}$, $\mathbf{Z}_9 \times \mathbf{Z}_3$, and $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$. This gives us the following possible groups:

$\mathbf{Z}_4 \times \mathbf{Z}_{27}$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{27}$

$\mathbf{Z}_4 \times \mathbf{Z}_9 \times \mathbf{Z}_3$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 \times \mathbf{Z}_3$

$\mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

Example: Let G and H be finite abelian groups, and assume that G × G is isomorphic to H × H. Prove that G is isomorphic to H.

Solution: Let p be a prime divisor of |G|, and let $q = p^m$ be the order of a cyclic component of G. If G has k such components, then G × G has 2k components of order q. An isomorphism between G × G and H × H must preserve these components, so it follows that H also has k cyclic

components of order q. Since this is true for every such q, it follows that $G \cong H$

Example: Let G be a finite abelian group which has 8 elements of order 3, 18 elements of order 9, and no other elements besides the identity. Find (with proof) the decomposition of Gas a direct product of cyclic groups.

Solution: We have $|G| = 27$. First, G is not cyclic since there is no element of order 27. Since there are elements of order 9, G must have Z_9 as a factor. To give a total of 27 elements, the only possibility is $G \cong Z_9 \times Z_3$.

Check: The elements 3 and 6 have order 3 in Z_9, while 1 and 2 have order 3 in Z_3. Thus, the following 8 elements have order 3 in the direct product: $(3, 0)$, $(6, 0)$, $(3, 1)$, $(6, 1)$, $(3, 2)$, $(6, 2)$, $(0, 1)$, and $(0, 2)$.

Example: Let G be a finite abelian group such that $|G| = 216$. If $|6G| = 6$, determine G up to isomorphism.

Solution: We have $216 = 2^3 \cdot 3^3$, and $6G \cong Z_2 \times Z_3$ since it has order 6. Let H be the Sylow 2-subgroup of G, which must have 8 elements. Then multiplication by 3 defines an automorphism of H, so we only need to consider 2H. Since $2H \cong Z_2$, we know that there are elements not of order 2, and that H is not cyclic, since $2Z_8 \cong Z_4$. We conclude that $H \cong Z_4 \times Z_2$.

A similar argument shows that the Sylow 3-subgroup K of G, which has 27 elements, must be isomorphic to $Z_9 \times Z_3$.

Using the decomposition, we see that

$G \cong Z_4 \times Z_2 \times Z_9 \times Z_3$.

(If you prefer the form of the decomposition, you can also give the answer in the form $G \cong Z_{36} \times Z_6$.)

Example: Apply both structure theorems to give the two decompositions of the finite abelian group $Z_{216}^{\times}$

Solution: $Z_{216}^{\times} \cong Z_8^{\times} \times Z_{27}^{\times} \cong Z_2 \times Z_2 \times Z_{27}^{\times}$

Since 27 is a power of an odd prime, it follows that $Z_{27}^{\times}$ is cyclic. This can also be shown directly by guessing that 2 is a generator.

Since $Z_{27}^{\times}$ has order $3^3 - 3^2 = 18$, an element can only have order 1, 2, 3, 6, 9 or 18. We have

$2^2 = 4$,

$2^3 = 8$,

$2^6 \equiv 8^2 \equiv 10$, and

$2^9 \equiv 2^3 \cdot 2^6 \equiv 8 \cdot 10 \equiv -1$,

so it follows that 2 must be a generator.

We conclude that $Z_{216}^{\times} \cong Z_2 \times Z_2 \times Z_{18}$.

To give the first decomposition, states that any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. In this decomposition we need to split Z_{18} up into cyclic subgrops of prime power order, so we finally get the decomposition

$Z_{216}^{\times} \equiv Z_2 \times Z_2 \times Z_2 \times Z_9$.

On the other hand, the second decomposition, where any finite finite abelian group is written as a direct product of cyclic groups in which the orders any component is a divisor of the previous one. To do this we need to group together the largest prime powers that we can. In the first decomposition, we can combine Z_2 and Z_9 to get Z_{18} as the first component. We end up with

$Z_{216}^{\times} \equiv Z_{18} \times Z_2 \times Z_2$

as the second way of breaking $Z_{216}^{\times}$ up into a direct product of cyclic subgroups.

Example*:* Let G and H be finite abelian groups, and assume that they have the following property. For each positive integer m, G and H have

the same number of elements of order m. Prove that G and H are isomorphic.

Solution: We give a proof by induction on the order of |G|. The statement is clearly true for groups of order 2 and 3, so suppose that G and H are given, and the statement holds for all groups of lower order. Let p be a prime divisor of |G|, and let G_p and H_p be the Sylowp-subgroups of G and H, respectively. Since the Sylow subgroups contain all elements of order a power of p, the induction hypothesis applies to G_p and H_p. If we can show that G_p H_p for all p, then it will follow that G H, since G and H are direct products of their Sylow subgroups.

Let x be an element of G_p with maximal order $q = p^m$. Then $< x >$ is a direct factor of G_p, so there is a subgroup G' with $G_p = < x > \times G'$. By the same argument we can write $H_p = < y > \times H'$, where y has the same order as x.

Now consider $< x^p > \times G'$ and $< y^p > \times H'$. To construct each of these subgroups we have removed elements of the form (x^k, g'), where x^k has order q and g' is any element of G'. Because x has maximal order in a p-group, in each case the order of g' is a divisor of q, and so (x^k, g') has order q since the order of an element in a direct product is the least common multiple of the orders of the components. Thus to construct each of these subgroups we have removed $(p^m – p^{m-1}) \cdot |G'|$ elements, each having order q. It follows from the hypothesis that we are left with the same number of elements of each order, and so the induction hypothesis implies that $< x^p > \times G'$ and $< y^p > \times H'$ are isomorphic. But then G' ; H', and so G_p ; H_p, completing the proof.

Proposition: Every finite abelian group has a natural structure as a module over the ring Z.

As with vector spaces, one goal is to be able to express a finite abelian group in terms of simpler building blocks. For vector spaces we can use one-dimensional spaces as the building blocks; for finite abelian groups, it seems natural to use the simple finite abelian groups.

Recall that in an arbitrary group G, a subgroup $N \subseteq G$ is called a normal subgroup if $gxg^{-1} \in N$, for all $x \in N$ and all $g \in G$. Then G is said to be a simple group if its only normal subgroups are $\{ 1 \}$ and G. If the group A is abelian, then all subgroups are normal, and so A is simple iff its only subgroups are the trivial subgroup (0) and the improper subgroup A. The same definition is given for modules: a nonzero module M is a simple module if its only submodules are (0) and M. When you view a finite abelian group as a Z-module, then, of course, the two definitions coincide.

Any cyclic finite abelian group is isomorphic to Z or Z_n, for some n.

Outline of the Proof: Let A be a cyclic finite abelian group that is generated by the single element a. Define the group homomorphism $f : Z \to A$ by setting $f (n) = na$, for all $n \in Z$. Note that f maps Z onto A since $f (Z) = Za = A$. If f is one-to-one, then A is isomorphic to Z. If f is not

one-to-one, we need to use the fundamental homomorphism theorem and the fact that every subgroup of Z is cyclic to show that A is isomorphic to Z_n, where n is the smallest positive integer such that $na = 0$.

Proposition: A finite abelian group is simple iff it is isomorphic to Z_p, for some prime number p.

Proof: First, let A be a finite abelian group isomorphic to Z_p, where p is a prime number. The isomorphism preserves the subgroup structure, so we only need to know that Z_p has no proper nontrivial subgroups. This follows from the general correspondence between subgroups of Z_n and divisors of n, since p is prime precisely when its only divisors are ±1 and ±p, which correspond to the subgroups Z_p and (0), respectively.

Conversely, suppose that A is a simple finite abelian group. Since A is nonzero, pick any nonzero element $a \in A$. Then the set $Za = \{ na \mid n \in Z \}$ is a nonzero subgroup of A, so by assumption it must be equal to A. This shows that A is a cyclic group. Furthermore, A can't be infinite, since then it would be isomorphic to Z and would have infinitely many subgroups. We conclude that A is finite, and hence isomorphic to Z_n, for

some n. Once again, the correspondence between subgroups of Z_n and divisors of n shows that if Z_n is simple, then n must be a prime number.

A module M is said to be semisimple if it can be expressed as a sum (possibly infinite) of simple submodules. Although the situation for finite abelian groups is more complicated than for vector spaces, it is natural to ask whether all finite abelian groups are semisimple.

Example: The group Z_4 is not a semisimple Z-module. First, Z_4 is not a simple group. Secondly, it cannot be written non-trivially as a direct sum of any subgroups, since its subgroups lie in a chain $Z_4 \supset 2Z_4 \supset (0)$, and no two proper nonzero subgroups intersect in (0).

Example: The group Z_6 is a semisimple Z-module. To see this, define $f : Z_6 \to Z_2 \oplus Z_3$ by setting $f(0) = (0, 0)$, $f(1) = (1, 1)$, $f(2) = (0, 2)$, $f(3) = (1, 0)$, $f(4) = (0, 1)$, $f(5) = (1, 2)$. You can check that this defines an isomorphism, showing that Z_6 is isomorphic to a direct sum of simple finite abelian groups.

The function defined in the example is a special case of a more general result that is usually referred to as the Chinese remainder theorem (this result is given more generally for rings. The proof of the next proposition makes use of the same function.

Proposition: If k = mn, where m and n are relatively prime integers, then Z_k is isomorphic to $Z_m \oplus Z_n$.

Outline of the Proof: Define $f : Z_k \to Z_m \oplus Z_n$ by $f([x]_k) = ([x]_m, [x]_n)$, for all $x \in Z$. Here I have been a bit more careful, by using $[x]_k$ to denote the congruence class of x, modulo k. It is not hard to show that f preserves addition. The sets Z_k and $Z_m \oplus Z_n$ are finite and have the same number of elements, so f is one-to-one iff it is onto, and therefore proving one of these conditions will give the other. (Actually, it isn't hard to see how to prove both conditions.) Showing that f is one-to-one depends on the fact that if x is an integer having both m and n as factors, then it must have mn as a factor since m and n are relatively prime. On the other hand, the usual statement of the Chinese remainder theorem is precisely the condition that f is an onto function.

Corollary: Any finite cyclic group is isomorphic to a direct sum of cyclic groups of prime power order.The corollary depends on an important result in Z: every positive integer can be factored into a product of prime numbers. Grouping the primes together, the proof of the corollary uses induction on the number of distinct primes in the factorization.

This basic result has implications for all finite groups. The cyclic group Z_n also has a ring structure, and the isomorphism that proves the corollary is actually an isomorphism of rings, not just of finite abelian groups. To use this observation, suppose that A is a finite finite abelian group. Let n be the smallest positive integer such that $na = 0$ for all $a \in A$. (This number might be familiar to you in reference to a multiplicative group G, where it is called the exponent of the group, and is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.)

You can check that because $na = 0$ for all $a \in A$, we can actually give A the structure of a Z_n-module.

Next we can apply a general result that if a ring R can be written as a direct sum $R = I_1 \oplus \ldots \oplus I_n$ of two-sided ideals, then each I_j is a ring in its own right, and every left R-module M splits up into a direct sum $M_1 \oplus \ldots \oplus M_n$, where M_j is a module over I_j . Applying this to Z_n, we can write Z_n as a direct sum of rings of the form $Z_p{}^k$, where p is a prime, and then the group A breaks up into $A_1 \oplus \ldots \oplus A_n$, where each A_j is a p-group, for some prime p. (Recall that a group G is a p-group if every element of G has order p.) This argument proves the next lemma. (You can also prove it using Sylow subgroups, if you know about them.)

Every finite abelian group can be written as a direct sum of p-groups.

The decomposition into p-groups occurs in one and only one way. Then it is possible to prove that each of the p-groups splits up into cyclic groups of prime power order, and so we have the following fundamental structure theorem for finite abelian groups.

Theorem: Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order.

A proof of the fundamental structure theorem, let us first discuss some of the directions it suggests for module theory. First of all, the hope was to construct finite abelian groups out of ones of prime order, not prime power order. The only way to do this is to stack them on top of each other, instead of having a direct sum in which the simple groups are lined up one beside the other. To see what I mean by "stacking" the groups, think of Z_4 and its subgroups $Z_4 \supset 2Z_4 \supset (0)$.

The subgroup $2Z_4 = \{0, 2\} \cong Z2$ is simple, and so is the factor module $Z_4/2Z_4 \cong Z_2$. This having Z_2 stacked on top of Z_2, and the group is structured so tightly that you can't even find an isomorphism to rearrange the factors.

A module M is said to have a composition series of length n if there is a chain of submodules $M = M_0 \supset M_1 \supset \ldots \supset M_n = (0)$ for which each factor module M_{i-1}/M_i is a simple module. Thus, we would say that Z_4 has a composition series of length 2. This gives a measurement that equals the dimension, in the case of a vector space. It is also true that the length of a cyclic group of order p^n is precisely n. It can be shown that if M has a composition series of length n, then every other composition series also has length n, so this is an invariant of the module. Furthermore, the same simple modules show up in both series, with the same multiplicity.

The idea of a composition series is related to two other conditions on modules. A module is said to satisfy the ascending chain condition, or ACC, if it has no infinite chain of ascending submodules; it is said to satisfy the descending chain condition, or DCC, if it has no infinite chain of descending submodules. Modules satisfying these conditions are called Noetherian or Artinian, respectively. A module has finite length iff it satisfies both the ACC and DCC. As an example to keep in mind, let's look at the ring of integers, which has ACC but not DCC. Since $mZ \subseteq nZ$ iff $n \mid m$, generators get smaller as you go up in Z, and larger as you go down. Any set of positive integers has a smallest element, so we can't have any infinite ascending chains, but, for example, we can construct the infinite descending chain $2Z \supset 4Z \supset 8Z \ldots$.

The cyclic groups of prime power order play a crucial role in the structure of finite abelian groups precisely because they cannot be split up any further. A module M can be expressed as a direct sum of two submodules M_1 and M_2 iff $M_1 \cap M_2 = (0)$ and $M_1 + M_2 = M$. In the case of a cyclic group of prime power order, the subgroups form a descending chain, and so any two nonzero subgroups have a nonzero intersection. A module is called indecomposable if it cannot be written as a direct sum of two nonzero submodules. With this terminology, the cyclic groups of prime power order are precisely the indecomposable finite abelian groups. The major results in this direction are (the Krull-Schmidt theorem), which show that any module with finite length can be written as a direct sum of indecomposable submodules, and this decomposition is unique up to isomorphism and the order of the summands.

After this rather lengthy preview, or review, as the case may be, it is time to move on to study general rings and modules. The next results present a proof of the structure theorem for finite abelian groups, but you should feel free to skip them.

Lemma: Let A be a finite abelian p-group.

(a) Let $a \in A$ be an element of maximal order, and let $b + Za$ be any coset of A/Za. Then there exists $d \in A$ such that $d + Za = b + Za$ and $Zd \cap Za = (0)$.

(b) Let $a \in A$ be an element of maximal order. Then there exists a subgroup B with $A \cong Za \oplus B$.

Proof: (a) The outline of part (a) is to let us be the smallest positive integer such that $sb \in Za$. Then we solve the equation $sb = sx$ for elements $x \in Za$ and let $d = b - x$.

Using $o(x)$ for the order of an element x, let us be the order of $b + Za$ in the factor group G/Za. Then $sb \in Za$, and we can write $sb = (qt)a$ for some exponent qt such that $t = p^{\beta}$ for some β and p $\nmid$ q. Then qa is a generator for Za, since q is relatively prime too (a). Since s is a divisor of the order of b, we have $o(b)/s = o(sb) = o((qt)a) = o(a)/t$, or simply, $o(b) \cdot t = o(a) \cdot s$. All of these are

powers of p, and so $o(b) \leq o(a)$ implies that s|t, say t = ms. Then x = (qm) a is a solution of the equation sb = sx. If d = b – x, then d + Za = b + Za and so sd = sb – sx = sb – sb = 0.

Therefore, $Zd \cap Za = (0)$, since $nd \in Za$ implies $n(b - x) = nb - nx \in Za$. Thus, $nb \in Za$ implies $n(b + Za) = Za$ in G/Za, so s|n and nd = 0.

(b) The outline of this part is to factor out Za and use induction to decompose A/Za into a direct sum of cyclic groups. Then part (a) can be used to choose the right preimages of the generators of A/Za to generate the complement B of Za.

We use induction on the order of A. If |A| is prime, then A is cyclic and there is nothing to prove. Consequently, we may assume that the statement of the lemma holds for all groups of order less than $|A| = p^{\alpha}$. If A is cyclic, then we are done. If not, let Za be a maximal cyclic subgroup, and use the induction hypothesis repeatedly to write A/Za as a direct sum $B_1 \oplus B_2 \oplus \ldots \oplus B_n$ of cyclic subgroups.

We next use part (a) to choose, for each i, a coset $a_i + Za$ that corresponds to a generator of A_i such that $Za_i \cap Za = (0)$. We claim that $A \cong Za \oplus B$ for the smallest subgroup $B = Za_1 + Za_2 + \cdots + Za_n$ that contains $a_1, a_2, \ldots, a_n$.

First, if $x \in Z_a \cap (Za_1 + \cdots + Za_n)$, then $x = m_1a_1 + \cdots + m_na_n \in Za$ for some coefficients $m_1, \ldots, m_n$. Thus $x + Za = (m_1a_1 + \cdots + m_na_n) + Za = Za$, and since A/Za is a direct sum, this implies that $m_ia_i + Za = Za$ for each i. But then $m_ia_i \in Za$, and so $m_ia_i = 0$ since $Za_i \cap Za = (0)$. Thus x = 0.

Next, given $x \in A$, express the coset x + Za as $(m_1a_1 + \cdots + m_na_n) + Za$ for coefficients $m_1, \ldots, m_n$. Then $x \in xZa$, and so $x = ma + m_1a_1 + \cdots + m_na_n$ for some m.

Thus, we have shown that $Za \cap B = (0)$ and A = Za + B, so $A \cong Za \oplus B$.

Theorem (Fundamental Theorem of Finite Abelian Groups) : Any finite abelian group is isomorphic to a direct sum of cyclic groups of

prime power order. Any two such decompositions have the same number of factors of each order.

Proof: We first decompose any finite abelian group A into a direct sum of p-groups, and then we can use the previous lemma to write each of these groups as a direct sum of cyclic subgroups.

Uniqueness is shown by induction on |A|. It is enough to prove the uniqueness for a given p-group. Suppose that

$Z_p\alpha_1 \oplus Z_p\alpha_2 \oplus \bullet\bullet\bullet \oplus Z_p\alpha_n = Z_p\beta_1 \oplus Z_p\beta_2 \oplus \bullet\bullet\bullet \oplus Z_p\beta_m$

where $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$ and $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_m$. Consider the subgroups in which each element has been multiplied by p. By induction, $\alpha_1 - 1 = \beta_1 - 1, \ldots$, which gives $\alpha_1 = \beta_1, \ldots$, with the possible exception of the α_i's and β_j's that equal 1. But the groups have the same order, and this determines that each has the same number of factors isomorphic to Z_p. This completes the proof.

Check Your progress-4

7. In a finite abelian group, each element is in a conjugacy class by itself and the character table involve powers of a single element known as a .....

   (a) group generator (b) group connector

   (c) group and subgroup (d) normal group element

8. In mathematics, the function finite abelian group { n_1, n_2, ... } represents ..... product of the cyclic group of degree in$_1$n$_2$ .....

   (a) direct (b) indirect

   (c) single (d) external

9. In commutative ring ..... the elements, or unit, from an abelian multiplication groups.

   (a) inversible (b) vertible

   (c) direct (d) finite

10. Every subgroup of a finite abelian group is normal, so each subgroup gives rest to a ..... group.

(a) cyclic (b) permutation

(c) quotient (d) multiplicative

4.6 LET US SUM UP

The definition and examples of external direct products of groups. The definition and examples of internal direct products of normal subgroups. If (m, n) = 1, then $Z_m \times Z_n$; Z_{mn}. o (H × K) = o (H) o (K) . The statement and application of Sylow's theorems, which state that: Let G be a finite group of order $p^n m$, where p is a prime and p m. Then G contains a subgroup of order p^k k = 1, ... , n; any two Sylow p-subgroups are conjugate in G; the number of distinct Sylow p-subgroups of G is congruent to 1 (mod p) and divides o (G) (in fact, it divides m) .

Let o (G) = pq, p a prime, p > q, q p – 1. Then G is cyclic. Let o (G) = p^2, p a prime. Then G is abelian. G is cyclic or G ; $Z_p \times Z_p$. The classification of groups of order 1 to 10, which we give in the following table:

O(G)	Algebraic Structure
1	{e}
2	Z_2
3	Z_3
4	Z_4 or $Z_2 \times Z_2$
5	Z_5
6	Z_6 or S_3
7	Z_7
8	Z_8 or $Z_4 \times Z_2$ or $Z_2 \times Z_2 \times Z_2$ (if G is abelian) Q_8 or D_8 (if G is non-abelian)
9	Z_9 or $Z_3 \times Z_3$
10	Z_{10} or D_{10}

A finite abelian group is a set, *A*, together with an operation "•" that combines any two elements *a* and *b* to form another element denoted *a* • *b*. The symbol "•" is a general placeholder for a concretely given operation. To qualify as a finite abelian group, the

set and operation, $(A, \bullet)$, must satisfy five requirements known as the *finite Abelian group axioms.* Generally, the multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules. The additive notation may also be used to emphasize that a particular group is abelian, whenever both abelian and non-finite abelian groups are considered.

For the integers and the operation addition "+", denoted $(\mathbf{Z}, +)$, the operation + combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer n has an additive inverse, "n, and the addition operation is commutative since $m + n = n + m$ for any two integers m and n. Every cyclic group G is abelian, because if x, y are in G, then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Thus the integers, $\mathbf{Z}$, form a finite abelian group under addition, as do the integers modulo n, $\mathbf{Z}/n\mathbf{Z}$.

4.7 KEYWORDS

External direct product*:* Let $(G_1, *_1), (G_2, *_2), \ldots\ldots, (G_n, *_n)$ be n groups. Their **external direct product** is the group $(G, *)$, where

$G = G_1 \times G_2 \ldots\ldots \times G_n$ and

Thus, R^n is the external direct product of n copies of R.

Internal direct product*:* Let H and K be normal subgroups of a group G. We call G the **internal direct product** of H and K if

$G = HK$ and $H \cap K = \{ e \}$.

We write this fact as $G = H \times K$.

Sylow p-subgroup: Let G be a finite group and p be a prime such that $p^n \mid o (G)$ but $p^{n+1} \nmid o (G)$, for some $n \geq 1$. Then a subgroup of G of order p^n is called a **Sylow p-subgroup of** G.

Finite abelian group: A finite abelian group is a set, *A*, together with an operation "•" that combines any two elements *a* and *b* to form another element denoted *a* • *b*.

Multiplication: The multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules.

Cyclic group: Every cyclic group *G* is abelian, because if *x*, *y* are in *G*, then $xy = a^m a^n = a^{m+n} =$

$a^{n+m} = a^n a^m = yx$.

4.8 QUESTIONS FOR REVIEW

1. Show that the binary operation * on G is associative. Find its identity element and the inverse of any element (x, y) in G.
2. Show that $G_1 \times G_2 = G_2 \times G_1$, for any two groups G_1 and G_2.
3. Show that $G_1 \times G_2$ is the product of its normal subgroup $H = G_1 \times \{ e_2 \}$ and $K = \{ e_1 \} \times G_2$. Also show that $(G_1 \times \{ e_2 \}) \cap (\{ e_1 \} \times G_2) = \{ (e_1, e_2) \}$.
4. Prove that $P (G_1 \times G_3) = Z (G_1) \times Z (G_2)$, where $Z (G_3)$ denotes the centre of G (see Theorem 2 of unit 3) .
5. Let A and B be cyclic groups of order m and n, respectively, where (m, n) = 1. Prove that
   A × B is cyclic of order mn.

   (Hint: Define $f : Z \to Z_m \times Z_n : f (r) = (r + mZ, r + nZ)$. Then apply the Fundamental theorem of Homomorphism to show that $Z_m \times Z_n \cong Z_{mn}$.
6. Let H and K be normal subgroups of G which satisfy (a) of Theorem 1. Then show that
   G = H × K.
7. Use Theorem 2 to prove Theorem 3.

8. Compute all possible finite abelian groups of order n. What is the largest n for which it will work?
9. Find all finite abelian group of order less than or equal to 40 up to isomorphism.
10. Find all finite abelian groups of order 200 to 720 up to isomorphism.
11. Show that the infinite direct product $G = Z_2 \times Z_2 \times \ldots$ is not finitely generated.
12. Let G be a finite abelian group of order m. If n divides m, prove that G has a subgroup of order n.

4.9 SUGGESTED READINGS AND REFERENCES

11. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
12. Paul B. Garrett (2007) . *Abstract Algebra*. Chapman and Hall/CRC.
13. Stephen Lovett (2016) . *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC
14. Dan Saracino (2008) .*Abstract Algebra; A First Course*. Waveland Press, Inc.; 2 edition
15. Mitchell and Mitchell (2007) . *An Introduction to Abstract Algebra*. Wadsworth Publishing

4.10 ANSWERS TO CHECK YOUR PROGRESS

1. (b) (answer for Check your Progress-1 Q.1)
2. (a) (answer for Check your Progress-1 Q.2)
3. (c) (answer for Check your Progress-2 Q.3)

4. (a) (answer for Check your Progress-2 Q.4)

5. (a) (answer for Check your Progress-3 Q.5)

6. (c) (answer for Check your Progress-3 Q.6)

7. (a) (answer for Check your Progress-4 Q.7)

8. (a) (answer for Check your Progress-4 Q.8)

9. (a) (answer for Check your Progress-4 Q.9)

10. (c) (answer for Check your Progress-4 Q.10)

UNIT - 5:CLASS EQUATION

STRUCTURE

5.0 OBJECTIVES

After studying this unit, you should be able to:

- Define conjugate subgroup
- Discuss conjugacy class of an element

5.1 INTRODUCTION

In the last unit, you have studied about finite abelian group. If G is a group and X is an arbitrary set, a group action of an element $g \in G$ and $x \in X$ is a product, g^x giving in x many problem in algebra may best be attached in group actions. In this unit, you will get the information related to conjugate elements.

5.2 CONJUGATE SUBGROUP

Definition: Let G be a group, and let x, y be elements of G. Then y is said to be a **conjugate** of x if there exists an element a in G such that $y = axa^{-1}$.

If H and K are subgroups of G, then K is said to be a **conjugate subgroup of H** if there exists an element a in G such that $K = aHa^{-1}$.

Proposition:

(a) Conjugacy of elements defines an equivalence relation on any group G.

(b) Conjugacy of subgroups defines an equivalence relation on the set of all subgroups of G.

Definition: Let G be a group. For any element x in G, the set

$\{ a \text{ in } G \mid axa^{-1} = x \}$

is called the **centralizer** of x in G, denoted by C (x) .

For any subgroup H of G, the set

$\{ a \text{ in } G \mid aHa^{-1} = H \}$

is called the **normalizer** of H in G, denoted by N (H) .

Proposition : Let G be a group and let x be an element of G. Then C (x) is a subgroup of G.

Proposition : Let x be an element of the group G. Then the elements of the conjugacy class of x are in one-to-one correspondence with the left cosets of the centralizer C (x) of x in G.

Example: Two permutations are conjugate in S_n if and only if they have the same shape (i.e., the same number of disjoint cycles, of the same lengths) . Thus, in particular, cycles of the same length are always conjugate.

Theorem : [Conjugacy class Equation] Let G be a finite group. Then

$| G | = | Z (G) | + \Sigma[g : C (x)]$

where the sum ranges over one element x from each nontrivial conjugacy class.

Definition: A group of order p^n, with p a prime number and $n \geq 1$, is called a **p-group.**

Theorem : [Burnside] Let p be a prime number. The center of any p-group is nontrivial.

Corollary : Any group of order p^2 (where p is prime) is abelian.

Theorem : [Cauchy] If G is a finite group and p is a prime divisor of the order of G, then G contains an element of order p.

Example: Prove that if the center of the group G has index n, then every conjugacy class of G has at most n elements.

Solution: The conjugacy class of an element a in G has [G **:** C (a)] elements. Since the center Z (G) is contained in C (a) , we have [G **:** C (a)] ≤ [G **:** Z (G)] = n. (In fact, [G **:** C (a)] must be a divisor of n.)

Example: Find all finite groups that have exactly two conjugacy classes.

Solution: Suppose that |G| = n. The identity element forms one conjugacy class, so the second conjugacy class must have n-1 elements. But the number of elements in any conjugacy class is a divisor of |G|, so the only way that n-1 is a divisor of n is if n = 2.

Example: Let G = D_{12}, given by generators a, b with |a|=6, |b|=2, and ba=a^{-1}b. Let H = { 1, a^3, b, a^3b } . Find the normalizer of H in G and find the subgroups of G that are conjugate to H.

Solution: The normalizer of H is a subgroup containing H, so since H has index 3, either N_G (H) = H or N_G (H) = G. Choose any element not in H to do the first conjugation.

aHa^{-1} = { 1, a (a^3) a^5, aba^5, a (a^3b) a^5 } = { 1, a^3, a^2b, a^5b }

This computation shows that a is not in the normalizer, so N_G (H) = H. Conjugating by any element in the same left coset aH = { a, a^4, ab, a^4b } will give the same subgroup. Therefore, it makes sense to choose a^2 to do the next computation.

a^2Ha^{-2} = { 1, a^3, a^2ba^4, a^2 (a^3b) a^4 } = { 1, a^3, a^4b, ab }

Comment: It is interesting to note that an earlier problem shows that b, a^2b, and a^4b form one conjugacy class, while ab, a^3b, and a^5 b form a second conjugacy class. In the above computations, notice how the orbits of individual elements combine to give the orbit of a subgroup.

Example*:* Write out the class equation for the dihedral group D_n. Note that you will need two cases: when n is even, and when n is odd.

Solution: When n is odd the center is trivial and elements of the form $a^i b$ are all conjugate. Elements of the form a^i are conjugate in pairs; $a^m \neq a^{-m}$ since $a^{2m} \neq 1$. We can write the class equation in the following form:

$|G| = 1 + ((n-1) /2) \cdot 2 + n$

When n is even, the center has two elements. (The element $a^{n/2}$ is conjugate to itself since it is equal to $a^{-n/2}$. This shows that Z (G) = { 1, $a^{n/2}$ } .) Therefore, elements of the form $a^i b$ split into two conjugacy classes. In this case the class equation has the following form:

$|G| = 2 + ((n-2) /2) \cdot 2 + 2 \cdot (n/2)$

Example: Show that for all $n \geq 4$, the centralizer of the element (1,2) (3,4) in S_n has order $8 \cdot (n-4)$!. Determine the elements in the centralizer of ((1,2) (3,4)) .

Solution: The conjugates of a = (1,2) (3,4) in S_n are the permutations of the form (a,b) (c,d) . The number of ways to construct such a permutation is

$n (n-1) /2 \cdot (n-2) (n-3) /2 \cdot 1/2$,

and dividing this into n! gives the order $8 \cdot (n-4)$! of the centralizer.

We first compute the centralizer of a in S_4. The elements (1, 2) and (3, 4) clearly commute with
(1, 2) (3, 4) . Note that a is the square of b = (1, 3, 2, 4) ; it follows that the centralizer contains
< b >, so b^3 = (1, 4, 2, 3) also belongs. Computing products of these elements shows that we must include (1, 3) (2, 4) and (1, 4) (2, 3) , and this gives the required total of 8 elements.

To find the centralizer of a in S_n, any of the elements listed above can be multiplied by any permutation disjoint from (1, 2) (3, 4) . This produces the required total $|C (a)| = 8 \cdot (n-4)$!.

Check Your progress-1

1. Let G be a group and let x be an elements of the G. Then L (x) is a ..... of G.

(a) Normal subgroup (b) Cyclic subgroup

(c) Subgroup (d) Permutation group

2. Any group of order p^2 is .....

(a) permutation (b) abelian

(c) cyclic (d) finite

3. If G is a ..... group and P is a prime divisor of the order of G, then G contains an element of order P.

(a) direct (b) external

(c) internal (d) finite

4. Let P be a prime number. The center of any P-group is .....

(a) trivial (b) non-trivial

(c) finite (d) infinite

5. A group of order p^n, with P is a prime number and n ..... is called a p-group.

(a) a = 1 (b) b > 1

(c) c < 1 (d) d ≥ 1

.

5.3 LET US SUM UP

Let G be a group, and let x,y be elements of G. Then y is said to be a **conjugate** of x if there exists an element a in G such that $y = axa^{-1}$. If H and K are subgroups of G, then K is said to be a **conjugate subgroup of H** if there exists an element a in G such that $K = aHa^{-1}$. Conjugacy of elements defines an equivalence relation on any group G. Conjugacy of subgroups defines an equivalence relation on the set of all subgroups of G. Let G be a group. For any element x in G, the set { a in G | axa^{-1} = x } is called the **centralizer** of x in G, denoted by C (x) .

For any subgroup H of G, the set { a in G | $aHa^{-1} = H$ } is called the **normalizer** of H in G, denoted by N (H) . Let G be a group and let x be an element of G. Then C (x) is a subgroup of G. Let x be an element

of the group G. Then the elements of the conjugacy class of x are in one-to-one correspondence with the left cosets of the centralizer C (x) of x in G.

5.4 KEYWORDS

Conjugate element: If H and K are subgroups of G, then K is said to be a ***conjugate*** **subgroup** of H if there exists an element a in G such that $K = aHa^{-1}$.

Centralizer: Let G be a group. For any element x in G, the set

{ a in G | $axa^{-1} = x$ }

is called the ***centralizer*** of x in G, denoted by C (x) .

5.5 QUESTIONS FOR REVIEW

1. Compute the G-equivalence classes of X for each of the G-sets X = { 1, –2, 24, 5, 6 } and
   G = { (1) , (1, 2) (3, 4, 5) ; (1 2) (3 4 5) , (1 2) (3 8 4) } for each $x \in X$ verify $|G| = |O_X| |G_X|$.
2. Write the class equation for S5 and for $|G_X|$
3. Let P be prime. Show that the number of different abelian groups of order P^n is the same as the number of conjugacy class in S_n.
4. Let a □ G, show that for any $g \in G$, $gc (a) g^{-1} = c (gag^{-1})$.
5. Let $|G| = p^n$ and suppose that $|Z (G)| = p^{n-1}$ for p prime. Prove that G is abelian.
6. Let G be a group with order p^n, where p is prime and X a finite G-set. If $X_G = \{ x \in X : gx = x \text{ for all } g \in G \}$ is the set of elements in X fixed by the group actions, then prove that
   $|X| = |X_G| \pmod{p}$.

5.6 SUGGESTED READINGS AND REFERENCES

16. Lalji Prasad (2016) . *Modern Abstract Algebra*. Paramount Publication
17. Stephen Lovett (2016) . *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC
18. Dan Saracino (2008) .*Abstract Algebra; A First Course*. Waveland Press, Inc.; 2 edition
19. Mitchell and Mitchell (2007) . *An Introduction to Abstract Algebra*. Wadsworth Publishing
20. John B. Fraleigh (2003) . *An Introduction to Abstract Algebra* (Relevant Portion) .Pearson Education

5.7 ANSWERS TO CHECK YOUR PROGRESS

10. (c) (answer for Check your Progress-1 Q.1)
11. (b) (answer for Check your Progress-1 Q.2)
12. (d) (answer for Check your Progress-1 Q.3)
13. (b) (answer for Check your Progress-1 Q.4)
14. (d) (answer for Check your Progress-1 Q.5)

UNIT - 6: CAUCHY'S THEOREM

STRUCTURE

6.0 OBJECTIVES

After studying this unit, you should be able to:

- Define homotopy
- Discuss the Cauchy's theorem
- Describe examples of Cauchy's theorem

6.1 INTRODUCTION

Cauchy-Riemann equations which under certain conditions provide the necessary and sufficient condition for the differentiability of a function of a complex variable at a point. A very important concept of analytic functions which is useful in many application of the complex variable theory. Let's discuss the concept of Cauchy's theorem.

6.2 HOMOTOPY

Suppose D is a connected subset of the plane such that every point of D is an interior point—we call such a set a region—and let C_1 and C_2 be oriented closed curves in D. We say C_1 is **homotopic** to C_2 in D if there

is a continuous function $H : S \to D$, where S is the square $S = \{ (t, s) : 0 \le s, t \le 1 \}$, such that $H(t,0)$ describes C_1 and $H(t,1)$ describes C_2, and for each fixed s, the function $H(t, s)$ describes a closed curve C_s in D.

The function H is called a **homotopy** between C_1 and C_2. Note that if C_1 is homotopic to C_2 in D, then C_2 is homotopic to C_1 in D. Just observe that the function $K(t, s) = H(t,1 – s)$ is a homotopy.

It is convenient to consider a point to be a closed curve. The point c is a described by a constant function $\gamma(t) = c$. We thus speak of a closed curve C being homotopic to a constant—we sometimes say *C* is **contractible** to a point.

Emotionally, the fact that two closed curves are homotopic in D means that one can be continuously deformed into the other in D.

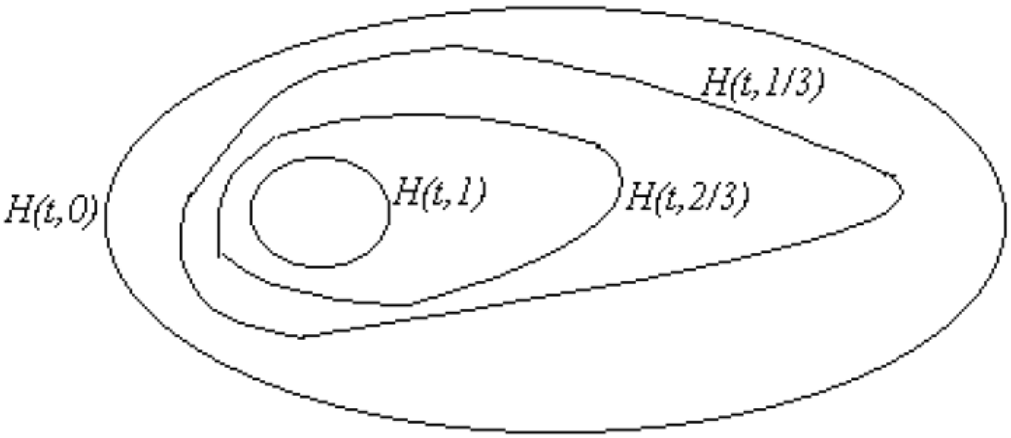
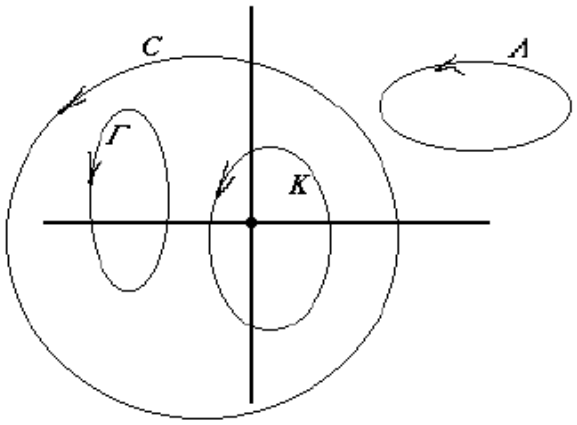


Figure : Diagram showing Homotopy

Example: Let D be the annular region $D = \{ z : 1 < |z| < 5 \}$. Suppose C_1 is the circle described by $\gamma_1(t) = 2e^{i2\pi t}$, $0 \le t \le 1$; and C_2 is the circle described by $\gamma_2(t) = 4e^{i2\pi t}$, $0 \le t \le 1$. Then $H(t, s) = (2 + 2s)\, e^{i2\pi t}$ is a homotopy in D between C_1 and C_2. Suppose C_3 is the same circle as C_2 but with the opposite orientation; that is, a description is given by $\gamma_3(t) = 4e^{-i2\pi t}$, $0 \le t \le 1$. A homotopy between C_1 and C_3 is not too easy to construct—in fact, it is not possible! The moral: orientation counts. From now on, the term “closed curve” will mean an oriented closed curve.

Another Example

Let D be the set obtained by removing the point z = 0 from the plane. Take a look at the picture. Meditate on it and convince yourself that C and K are homotopic in D, but Γ and Λ are homotopic in D, while K and Γ are not homotopic in D.



Check Your progress-1

1. Suppose D is a connected subset of the plane such that every point of D is an interior point—we call such a set a region—and let C_1 and C_2 be oriented closed .....

2. It is convenient to consider a point to be a closed curve. The point c is a described by a constant function $\gamma (t) = c$. We thus speak of a closed curve C being homotopic to a constant—we sometimes say C is ..... to a point.

6.3 CAUCHY'S THEOREM

Suppose C_1 and C_2 are closed curves in a region D that are homotopic in D, and suppose f is a function analytic on D. Let $H (t, s)$ be a homotopy between C_1 and C_2. For each s, the function $\gamma_s (t)$ describes a closed curve C_s in D. Let $I (s)$ be given by

$$I (s) = \int_{C_s} f(z)dz.$$

Then,

$$I(s) = \int_0^1 f(H(t,s)) \frac{\partial H(t,s)}{\partial t} dt.$$

Now, let's look at the derivative of I (s) . We assume everything is nice enough to allow us to differentiate under the integral:

$$I'(s) = \frac{d}{ds}\left[\int_0^1 f(H(t,s)) \frac{\partial H(t,s)}{\partial t} dt\right]$$

$$= \int_0^1 \left[f'(H(t,s)) \frac{\partial H(t,s)}{\partial t} \frac{\partial H(t,s)}{\partial t} + f(H(t,s)) \frac{\partial^2 H(t,s)}{\partial s \partial t} \right] dt$$

$$= \int_0^1 \left[f'(H(t,s)) \frac{\partial H(t,s)}{\partial t} \frac{\partial H(t,s)}{\partial t} + f(H(t,s)) \frac{\partial^2 H(t,s)}{\partial t \partial s} \right] dt$$

$$= \int_0^1 \frac{\partial}{\partial t}\left[f(H(t,s)) \frac{\partial H(t,s)}{\partial s} \right] dt$$

$$= f(H(1,s)) \frac{\partial H(1,s)}{\partial s} - f(H(0,s)) \frac{\partial H(0,s)}{\partial s}.$$

But we know each H (t, s) describes a closed curve, and so H (0, s) = H (1, s) for all s. Thus,

$$I'(s) = f(H(1,s)) \frac{\partial H(1,s)}{\partial s} - f(H(0,s)) \frac{\partial H(0,s)}{\partial s} = 0.$$

which means I (s) is constant! In particular, I (0) = I (1) , or

$$\int_{C_1} f(z)dz = \int_{C_2} f(z)dz$$

This is a big deal. We have shown that if C_1 and C_2 are closed curves in a region *D* that are homotopic in *D*, and *f* is analytic on *D*, then

$$\int_{C_1} f(z)dz = \int_{C_2} f(z)dz.$$

An easy corollary of this result is the celebrated Cauchy's Theorem, which says that if *f* is analytic on a simply connected region D, then for any closed curve C in D, $\int_C f(z)dz = 0.$

In court testimony, one is admonished to tell the truth, the whole truth, and nothing but the truth. Well, so far in this chapter, we have told the truth, but we have not quite told the whole truth. We assumed all sorts of continuousm derivatives in the preceding discussion. These are not

always necessary—specifically, the results can be proved true without all our smoothness assumptions—think about approximation.

Example:

Look at the picture below and convince yourself that the path C is homotopic to the closed path consisting of the two curves C_1 and C_2 together with the line L. We traverse the line twice, once from C_1 to C_2 and once from C_2 to C_1.

Observe then that an integral over this closed path is simply the sum of the integrals over C_1 and C_2, since the two integrals along L, being in opposite directions, would sum to zero. Thus, if f is analytic in the region bounded by these curves (the region with two holes in it) , then we know that

$$\int_C f(z)dz = \int_{C_1} f(z)dz + \int_{C_2} f(z)dz.$$

Check Your progress-2

3. Emotionally, the fact that two closed curves are ..... in D means that one can be continuously deformed into the other in D.
4. If f is analytic in the region bounded by these curves (the region with two holes in it) , then we know that .....

6.4 LET US SUM UP

Suppose D is a connected subset of the plane such that every point of D is an interior point—we call such a set a region—and let C_1 and C_2 be oriented closed curves in D. We say C_1 is **homotopic** to C_2 in D if there is a continuous function $H : S \to D$, where S is the square $S = \{ (t, s) : 0 \le s, t \le 1 \}$, such that $H(t,0)$ describes C_1 and $H(t,1)$ describes C_2, and for each fixed s, the function $H(t, s)$ describes a closed curve C_s in D. The function H is called a **homotopy** between C_1 and C_2. Note that if C_1 is homotopic to C_2 in D, then C_2 is homotopic to C_1 in D. Just observe that the function $K(t, s) = H(t,1 – s)$ is a homotopy.

It is convenient to consider a point to be a closed curve. The point c is a described by a constant function γ (t) = c. We, thus, speak of a closed curve C being homotopic to a constant—we sometimes say *C* is **contractible** to a point. Emotionally, the fact that two closed curves are homotopic in D means that one can be continuously deformed into the other in D. Suppose C_1 and C_2 are closed curves in a region D that are homotopic in D, and suppose f is a function analytic on D. Let H (t, s) be a homotopy between C_1 and C_2. For each s, the function γ_s (t) describes a closed curve C_s in D. Let I (s) be given by I (s) = $\int_{C_s} f(z)dz.$

6.5 KEYWORDS

Homotopy: The function H is called a homotopy between C_1 and C_2. Note that if C_1 is homotopic to C_2 in D, then C_2 is homotopic to C_1 in D. Just observe that the function K (t, s) = H (t,1 – s) is a homotopy.

Contractible: It is convenient to consider a point to be a closed curve. The point c is a described by a constant function γ (t) = c. We thus speak of a closed curve C being homotopic to a constant—we sometimes say *C* is contractible to a point.

Cauchy's Theorem: Suppose C_1 and C_2 are closed curves in a region D that are homotopic in D, and suppose f is a function analytic on D. Let H (t, s) be a homotopy between C_1 and C_2. For each s, the function γ_s (t) describes a closed curve C_s in D. Let I (s) be given by I (s) = $\int_{C_s} f(z)dz.$

6.6 QUESTIONS FOR REVIEW

1. Suppose C_1 is homotopic to C_2 in D, and C_2 is homotopic to C_3 in D. Prove that C_1 is homotopic to C_3 in D.
2. Explain how you know that any two closed curves in the plane Care homotopic in C.

3. A region D is said to be simply connected if every closed curve in D is contractible to a point in D. Prove that any two closed curves in a simply connected region are homotopic in D.

4. Prove Cauchy's Theorem.

5. Let S be the square with sides x = ± 100, and y = ± 100 with the counterclockwise orientation. Find $\int_s \frac{1}{z} dz.$

6. (a) Find $\int_C \frac{1}{z-1} dz,$ where C is any circle centered at z = 1 with the usual counterclockwise orientation: $\gamma(t) = 1 + Ae^{2\pi it}$, $0 \le t \le 1$.

   (b) Find $\int_C \frac{1}{z+1} dz,$ where C is any circle centered at z = –1 with the usual counterclockwise orientation.

   (c) Find $\int_C \frac{1}{z^2-1} dz,$ where C is the ellipse $4x^2 + y^2 = 100$ with the counterclockwise orientation. [Hint: partial fractions]

   (d) Find $\int_C \frac{1}{z^2-1} dz,$ where C is the circle $x^2 - 10x + y^2 = 0$ with the counterclockwise orientation.

7. Evaluate $\int_C \mathrm{Log}(z+3) dz,$ where C is the circle |z| = 2 oriented counterclockwise.

8. Evaluate $\int_C \frac{1}{z^n} dz$ where C is the circle described by $\gamma(t) = e^{2\pi it}$, $0 \le t \le 1$, and n is an integer ≠ 1.

9. (a) Does the function $f(z) = \frac{1}{z}$ have an antiderivative on the set of all z ≠ 0? Explain.

   (b) How about $f(z) = \frac{1}{z^n}$, n an integer ≠ 1?

10. Find as large a set D as you can so that the function have an antiderivative on D.

11. Explain how you know that every function analytic in a simply connected region D is the derivative of a function analytic in D.

6.7 SUGGESTED READINGS AND REFERENCES

21. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
22. Paul B. Garrett (2007) . *Abstract Algebra*. Chapman and Hall/CRC.
23. Vijay K Khanna (2017) .*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
24. Mitchell and Mitchell (2007) . *An Introduction to Abstract Algebra*. Wadsworth Publishing
25. John B. Fraleigh (2003) . *An Introduction to Abstract Algebra* (Relevant Portion) .Pearson Education

6.8 ANSWERS TO CHECK YOUR PROGRESS

1. curves in D (answer for Check your Progress-1 Q.1)
2. contractible (answer for Check your Progress-1 Q.2)
3. homotopic (answer for Check your Progress-2 Q.3)
4. $\int_C f(z)dz = \int_{C_1} f(z)dz + \int_{C_2} f(z)dz.$ (answer for Check your Progress-2 Q.4)

UNIT - 7: SYLOW'S THEOREMS

STRUCTURE

7.7 OBJECTIVES

After studying this unit, you should be able to:

- Discuss Sylow's Theorem
- Describe examples of Sylow's theorem

7.8 INTRODUCTION

We already know that the converse of Lagrange's Theorem is false. If G is a group of order m and n divides m, then G does not necessarily possess a subgroup of order n. For example, A4 has order 12 but does not possess a subgroup of order 6. However, the Sylow Theorems do provide a partial converse for Lagrange's Theorem: in certain cases they guarantee us subgroups of specific orders. These theorems yield a powerful set of tools for the classification of all finite non-abelian groups.

7.9 THE SYLOW THEOREMS

We will use the idea of group actions to prove the Sylow Theorems. Recall for a moment what it means for G to act on itself by conjugation

and how conjugacy classes are distributed in the group according to the class equation. A group G acts on itself by conjugation via the map $(g, x) \rightarrow gxg^{-1}$. Let $x_1,...,x_k$ be representatives from each of the distinct conjugacy classes of G that consist of more than one element. Then the class equation can be written as

$$|G| = |Z (G)| + [G : C (x_1)] + ... + [G : C (x_k)],$$

where $Z (G) = \{ g \in G : gx = xg \text{ for all } x \in G \}$ is the center of G and $C (x_i) = \{ g \in G : gx_i = x_i g \}$ is the centralizer subgroup of x_i.

We now begin our investigation of the Sylow Theorems by examining subgroups of order p, where p is prime. A group G is a p-group if every element in G has as its order a power of p, where p is a prime number. A subgroup of a group G is a p-subgroup if it is a p-group.

7.2.1 A Proof of Sylow's Theorems

In this handout, we give proofs of the three Sylow theorems which are slightly different from the ones in the book. Recall the following lemma:

Lemma: Let p be a prime number, and let G be a p-group (a finite group of order p^k for some $k \geq 1$) acting on a finite set S. Then the number of fixed points of the action is congruent to |S| modulo p.

We make the following definition: if G has order $p^k m$ with $p \nmid m$, a Sylow p-subgroup of G is a subgroup of order p^k.

Theorem (Sylow's First Theorem) : If G is a finite group of order $n = p^k m$ with p prime and $p \nmid m$, then G has a subgroup of order p^k. In other words, if $Syl_p (G)$ denotes the set of Sylow p-subgroups of G, then $Syl_p (G) \neq \emptyset$.

Proof. The proof is by induction on |G|, the base case |G| = 1 being trivial. If there exists a proper subgroup H of G such that $p \nmid [G : H]$, then a Sylow p-subgroup of H is also a a Sylow p-subgroup of G and we're finished by induction. So without loss of generality, we may assume that $p \mid [G : H]$ whenever $H < G$. From the class equation, it follows that $p \mid |Z_G|$. By Cauchy's theorem, there exists a subgroup $N \leq$

Z_G of order p, which is necessarily normal in G. Let $\bar{G}$ = G/N, so $|\bar{G}| = p^{k-1}m$. By induction, $\bar{G}$ has a subgroup of order p^{k-1}. Let P be the subgroup of G containing N which corresponds to $\bar{P}$ by the first isomorphism theorem. Then

$|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k$,

so that P is a Sylow p-subgroup of Gas desired.

Theorem (Sylow's Second Theorem) : If G is a finite group and p is a prime number, then all Sylow p-subgroups of G are conjugate to one another.

Proof: We show more precisely that if H is any subgroup of G of p-power order and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H \leq xPx^{-1}$. (This implies the theorem, since if $H \in Syl_p(G)$ then $|H| = |P| = |xPx^{-1}|$, which implies that $H = xPx^{-1}$, so that H is conjugate to P.) Note that H acts on G/P (the set of left cosets of P in G) by left multiplication. Let Fix denote the elements of G/P fixed by this action. Then $|Fix| \equiv |G/P| \pmod p$ by the Lemma. Since $p \nmid m = |G/P|$, $|Fix| \neq 0$, and thus $Fix \neq \emptyset$;. Let xP be a left coset fixed by the action. Then $hxP = xP \; \forall \; h \in H \Rightarrow x^{-1}Hx \leq P$,

so that $H \leq xPx^{-1}$ as desired.

Theorem (Sylow's Third Theorem) : If G is a finite group and p is a prime number, let
$n_p = |Syl_p(G)|$. Then $n_p \mid |G|$ and $n_p \equiv 1 \pmod p$.

Proof: We consider the action of G on Sylp (G) by conjugation. By the second Sylow theorem, this action is transitive, so there is just one orbit. Hence n_p, which is the size of this orbit, divides |G|.

To prove the congruence $n_p \equiv 1 \pmod p$, we fix a Sylow p-subgroup $P \in Syl_p(G)$ and consider the action of P on $Syl_p(G)$ by conjugation. Let Fix denote the set of fixed points of this action. Note that $Q \in Fix \Leftrightarrow P \leq N_G(Q)$, and in particular $P \in Fix$. If $Q \in Fix$, then $P, Q \leq N_G(Q)$ are both Sylow p-subgroups of $N_G(Q)$, so they are conjugate in N_G (

Q) (again by the second Sylow theorem) . But Q is a normal subgroup of N_G (Q) , so P = Q. Thus Fix = { P } , and in particular |Fix| = 1. By the Lemma, np ≡ 1 (mod p) as desired.

The more precise fact established in our proof of Sylow's Second Theorem yields the following useful result:

Corollary: If G is a finite group and p is a prime number, then any subgroup of G of p-power order is contained in some Sylow p-subgroup.

Since G acts transitively by conjugation on Syl_p (G) , and the stabilizer of P ∈ Syl_p (G) is N_G (P) , we deduce that np = [G : N_G (P)] for any P ∈ Syl_p (G) .

Therefore:

Corollary: If G is a finite group and p is a prime number, let n_p be the number of Sylow p-subgroups of G. Then the following are equivalent:

1. np = 1.
2. Every Sylow p-subgroup of G is normal.
3. Some Sylow p-subgroup of G is normal.

Example*:* By direct computation, find the number of Sylow 3-subgroups and the number of Sylow 5-subgroups of the symmetric group S_5. Check that your calculations are consistent with the Sylow theorems.

Solution: In S_5 there are (5 · 4 · 3) / 3 = 20 three cycles. These will split up into 10 subgroups of order 3. This number is congruent to 1 mod 3, and is a divisor of 5 · 4 · 2.

There are (5!) / 5 = 24 five cycles. These will split up into 6 subgroups of order 5. This number is congruent to 1 mod 5, and is a divisor of 4 · 3 · 2.

Example*:* How many elements of order 7 are there in a simple group of order 168?

Solution: First, 168 = 2^3 **.** 3 **.** 7. The number of Sylow 7-subgroups must be congruent to 1 mod 7 and must be a divisor of 24. The only possibilities are 1 and 8. If there is no proper normal subgroup, then the

number must be 8. The subgroups all have the identity in common, leaving $8 \cdot 6 = 48$ elements of order 7.

Example: Prove that a group of order 48 must have a normal subgroup of order 8 or 16.

Solution: The number of Sylow 2-subgroups is 1 or 3. In the first case there is a normal subgroup of order 16. In the second case, let G act by conjugation on the Sylow 2-subgroups. This produces a homomorphism from G into S_3. Because of the action, the image cannot consist of just 2 elements. On the other hand, since no Sylow 2-subgroup is normal, the kernel cannot have 16 elements. The only possibility is that the homomorphism maps G onto S_3, and so the kernel is a normal subgroup of order 48 / 6 = 8.

Example: Let G be a group of order 340. Prove that G has a normal cyclic subgroup of order 85 and an abelian subgroup of order 4.

Solution: First, $340 = 2^2 \cdot 5 \cdot 17$. There exists a Sylow 2-subgroup of order 4, and it must be abelian. No divisor of $68 = 2^2 \cdot 17$ is congruent to 1 mod 5, so the Sylow 5-subgroup is normal. Similarly, then Sylow 17-subgroup is normal. These subgroups have trivial intersection, so their product is a direct product, and hence must be cyclic of order $85 = 5 \cdot 17$. The product of two normal subgroups is again normal, so this produces the required normal subgroup of order 85.

Example: Show that there is no simple group of order 200.

Solution: Since $200 = 2^3 \cdot 5^2$, the number of Sylow 5-subgroups is congruent to 1 mod 5 and a divisor of 8. Thus there is only one Sylow 5-subgroup, and it is a proper nontrivial normal subgroup.

Example: Show that a group of order 108 has a normal subgroup of order 9 or 27.

Solution: Let S be a Sylow 3-subgroup of G. Then [G:S] = 4, since $|G| = 2^2 3^3$, so we can let G act by multiplication on the cosets of S. This defines a homomorphism $\mu : G \to S_4$, so it follows that $| \mu (G) |$ is a divisor of 12, since it must be a common divisor of 108 and 24. Thus |

ker (μ) | ≥ 9, and it follows that ker (μ) ⊆ S, so | ker (μ) | must be a divisor of 27. It follows that | ker (μ) | = 9 or | ker (μ) | = 27.

Example: If p is a prime number, find all Sylow p-subgroups of the symmetric group S_p.

Solution: Since $|S_p| = p!$, and p is a prime number, the highest power of p that divides $|S_p|$ is p. Therefore, the Sylow p-subgroups are precisely the cyclic subgroups of order p, each generated by a p-cycle. There are (p-1) ! = p! / p ways to construct a p-cycle $(a_1, \ldots, a_p)$. The subgroup generated by a given p-cycle will contain the identity and the p-1 powers of the cycle. Two different such subgroups intersect in the identity, since they are of prime order, so the total number of subgroups of order p in S_p is (p-2) ! = (p-1) ! / (p-1) .

Example: Prove that if G is a group of order 56, then G has a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.

Solution: The number of Sylow 7-subgroups is either 1 or 8. Eight Sylow 7-subgroups would yield 48 elements of order 7, and so the remaining 8 elements would constitute the (unique) Sylow 2-subgroup.

Example: Prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G.

Solution: Suppose that N contains the Sylow p-subgroup P. Then since N is normal it also contains all of the conjugates of P. But this means that N contains all of the Sylow p-subgroups of G, since they are all conjugate. We conclude that N and G have the same number of Sylow p-subgroups.

Example*:* Prove that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Solution: The notation $n_p (G)$ will be used for the number of Sylow p-subgroups of G. Since $105 = 3 \cdot 5 \cdot 7$, we have $n_3 (G) = 1$ or 7, $n_5 (G) = 1$ or 21, and $n_7 (G) = 1$ or 15 for the numbers of Sylow subgroups. Let P be a Sylow 5-subgroup and let Q be a Sylow 7-subgroup. At least

one of these subgroups must be normal, since otherwise we would have 21 · 4 elements of order 5 and 15 · 6 elements of order 7. Therefore, PQ is a subgroup, and it must be normal since its index is the smallest prime divisor of |G|, so we can apply the result in the previous problem. Since PQ is normal and contains a Sylow 5-subgroup, we can reduce to the number 35 when considering the number of Sylow 5-subgroups, and thus n_5 (G) = n_5 (PQ) = 1. Similarly, since PQ is normal and contains a Sylow 7-subgroup, we have n_7 (G) = n_7 (PQ) = 1.

Check Your progress-1

1. A group G is a p-group of every element in G has its order a power of .....

   (a) g (b) p

   (c) g-1 (d) p-1

2. If G is a finite group. Then G is p-group of and only if |G| = ...

   (a) p^{-p} (b) p^p

   (c) p^n (d) p^n

3. Let P be a Sylow p-subgroups of a ..... G and let x have as its order a power of p. If

   $x^{-1}p$ (x) = p. Then x ∈ p.

   (a) indirect (b) infinite

   (c) finite (d) direct

4. A subgroup of a group G is a p- ..... if it is a p-group.

   (a) subgroup (b) normal group

   (c) infinite group (d) cyclic group

5. How many elements of order 7 are there is a simple group of order 168.

   (a) 7 (b) 8

   (c) 9 (d) 48

7.10 LET US SUM UP

Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p. **(First Sylow Theorem)** Let G be a finite group and p a prime such that p^r divides |G|.

Then G contains a subgroup of order p^r.Let P be a Sylow p-subgroup of a finite group G and let x have as its order a power of p.

If $x^{-1}Px = P$. Then $x \in P$.

Let H and K be subgroups of G. The number of distinct H-conjugates of K is

[H : N (K) I H]. **(Second Sylow Theorem)** Let G be a finite group and p a prime dividing |G|. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.

7.11 KEYWORDS

Cauchy*:* Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.

First Sylow Theorem: Let G be a finite group and p a prime such that p^r divides |G|. Then G contains a subgroup of order p^r.

7.12 QUESTIONS FOR REVIEW

1. What are the order of all Sylow p-subgroups where G has order 18, 24, 54 and 80?
2. Find all the Sylow 3-subgroups of S_4 and show that they are all conjugate.
3. Show that every group of order 45 has a normal subgroup of order 9.

4. Let H be a Sylow p-subgroup of G. Prove that H ps the only Sylow p-subgroup of G contained in N (H) .
5. Prove that no group of order 96 is simple.
6. If H is normal subgroup of a finite group G and $|H| = p^k$ for some prime p, show that H is a contained in every Sylow p-subgroup of G.

7.13 SUGGESTED READINGS AND REFERENCES

26. Thomas W Judson (2013) . *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
27. Paul B. Garrett (2007) . *Abstract Algebra*. Chapman and Hall/CRC.
28. Vijay K Khanna (2017) . *A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
29. Dan Saracino (2008) .*Abstract Algebra; A First Course*. Waveland Press, Inc.; 2 edition
30. Mitchell and Mitchell (2007) . *An Introduction to Abstract Algebra*. Wadsworth Publishing

7.14 ANSWERS TO CHECK YOUR PROGRESS

15. (b) (answer for Check your Progress-1 Q.1)
16. (c) (answer for Check your Progress-1 Q.2)
17. (c) (answer for Check your Progress-1 Q.3)
18. (a) (answer for Check your Progress-1 Q.4)
19. (d) (answer for Check your Progress-1 Q.5)