INDEX

NAME: AKASH MANDAL STD.: Sem 6 SEC.: _____ ROLL NO.: 16MA2037 SUB.: MODERN ALGEBRA

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks
1.	3.1.19	Group, Intro. (1hr)		
2.	7.1.19	Subgroups, Dihedral Groups (1hr)		
3.	8.1.19	Permutation group, Cyclic groups (2hr)		
4.	10.1.19	Prop. of cyclic. grps. (1hr)		
5.	14.1.19	Grp. Homomorphism. (1hr)		
6.	15.1.19	Lagrange Thm (2hr)		
7.	17.1.19.	Automorphism, (1hr)		
8.	22.1.19	Isomorphism Thms (2hr)	Mondays Cancelled	
9.	12.1.19	Tutorial (1hr)		
10	24.1.19	(1hr)		
11.	29.1.19	(2hr)	5th Feb Class Test	
12.	29.1.19	Tutorial (1hr)		
13.	31.1.19	(1hr)		

3.12.18

Evaluation

Midsem 30%
End Sem 50%
Class Test 10%
Surprise Test 10%

Textbook (not just notes)

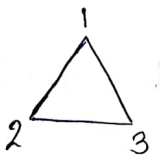
1. Algebra – Artin ✱
2. Abstract Algebra – by Dummit and Foote
3. Algebra – by Herstein
4. Abstract Algebra – Galion

→ Group Theory
  → Subgroups
  → Cyclic
  ⋮
  → Sylow's Theorems
→ Ring Theory.

Intro

Started to study symmetry of objects. (Motivation)

Consider



$\circlearrowleft 120^\circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

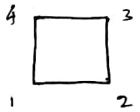
followed by

ϕ

gives

ϕ^2

Also for square



4R
4F

Certain operations.

Dihedral group

∴ Operations on elements give back same elements of the set. 3 rotations and 3 reflections.

Also for any transformation ∃ another transformation which composed with first returs 0° or identity transformation

Symmetries → Transformations to preserve invariance.

Eg

$GL_n(\mathbb{R})$ ≡ The set of all Invertible matrices.

Operation: Matrix multiplication

- Inverse exists.
- AB invertible
- $AI = A$

Eg $SL_n(\mathbb{R})$ ≡ The set of all $n \times n$ matrices such that determinant is 1.

- $|AB| = |A||B| = 1$
- $AI = A$
- A^{-1} exists. $|A| \neq 0$

Eg $O_n(\mathbb{R})$ ≡ The set of all $n \times n$ orthogonal matrices

- AB orthogonal
- I exists
- A^{-1} exists.

Eg $SO_n(\mathbb{R}) = \{ A \in O_n(\mathbb{R}) \mid \det(A) = 1 \}$

Eg $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition

Eg $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{C}^*$: non zero sets under multiplication.

Eg $S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

Definition of Group :-

A group is a set on which a law of composition is defined with certain properties. A law of composition on a set S is a map $F : S \times S \to S$

$f(a,b)$ often denoted by $a+b$ or ab

Examples:

(1) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as $f(a,b) = a + b$

(2) $GL_n(\mathbb{R}) = A$ $f : A \times A \to A$ defined as $f(B,C) = BC$

(3) S = Set of all maps from $T \to T$, T is a set

$f(f_1, f_2) = f_1 \circ f_2$ $\quad f_1, f_2 \in S$

Group if f has only bijective maps
- Identity map
- Invertible

This group : Permutation / Symmetric group

(1) A law of composition on a set S is said to be associative if

$(ab)c = a(bc)$ $\quad \forall a, b, c \in S$

(2) A law of composition is said to be commutative if

$ab = ba$ $\quad \forall a, b \in S$.

(3) An identity for a law of composition is an element $e \in S$

s.t. $ea = ae = a$ $\quad \forall a \in S$

(4) Suppose we have an identity element then an element a is said to be invertible if $\exists\, b \in S$ s.t. $ab = ba = e$

A group is a non empty set G with a law of composition that is associative, and has identity and every element has inverse. (1) (3) (4)

EOC

Definition of Group :-

A group is a set on which a law of composition is defined with certain properties. A law of composition on a set S is a map $F: S \times S \to S$

$f(a,b)$ often denoted by $a+b$ or ab

Examples:

(i) $f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as $f(a,b) = a+b$

(ii) $GL_n(\mathbb{R}) = A$ $f: A \times A \to A$ defined as $f(B,C) = BC$

(iii) S = Set of all maps from $T \to T$, T is a set

$f(f_1, f_2) = f_1 \circ f_2$ $\quad f_1, f_2 \in S$

Group if f has only bijective maps

- Identity map
- Invertible

This group : Permutation / Symmetric group

(1) A law of composition on a set S is said to be associative if

$(ab)c = a(bc)$ $\quad \forall a, b, c \in S$

(2) A law of composition is said to be commutative if

$ab = ba$ $\quad \forall a, b \in S$

(3) An identity for a law of composition is an element $e \in S$

s.t. $ea = ae = a$ $\quad \forall a \in S$

(4) Suppose we have an identity element then an element a is said to be invertible if $\exists\, b \in S$ s.t. $ab = ba = e$

A group is a non empty set G with a law of composition that is associative, and has identity and every element has inverse. (1) (3) (4)

EOC

7.1.19

Dihedral groups.

$D_4 = \{ I_d, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (2\,4), (1\,2)(3\,4), (1\,3), (1\,4)(2\,3) \}$

Rotations (1 2 3 4); Flips (2 4), (1 2)(3 4), (1 3), (1 4)(2 3)

Consecutive mapping

Study symmetry of regular n-gon

$D_{2n} \rightarrow 2n$ elements

Dihedral group: The group of symmetries of a regular polygon including both rotations and reflections.

A regular polygon with n sides has n different rotations and n different reflections with ~~total~~ $2n$ different elements and denoted as D_n (not D_{2n} as is another convention)

A group G where commutativity holds ie $ab = ba \ \forall a, b \in G$ is called an abelian group. Eg. $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ abelian over +

$GL_n(\mathbb{R})$ not abelian over x.

Eg D_n: not abelian

Ex. Identity element is unique in a group

Let e, e' be unique identity elements in $G(*)$

~~$e * e' = e$~~ $a * e = a \quad \forall a \in G$

$\therefore e' * e = e' \quad \ldots (1)$

$e' * a = a \quad \forall a \in G$

$\therefore e'' * e = e \quad \ldots (2)$

$\therefore (1), (2) \rightarrow e' = e \quad \rightarrow\leftarrow$

Ex ☆ The inverse of an element is unique in a group.

Similar

Remark (i) If the law of composition is written additively then

$$na = \underbrace{a + a + a + \cdots + a}_{n \text{ times}}$$

Then the inverse of a denoted as

$$-a$$

(ii) If law of composition is written multiplicatively

$$a^n = \underbrace{a * a * a * \cdots * a}_{n \text{ times}}$$

$a^{-1} \rightarrow$ Inverse.

Ex ☆

Show that in a group.

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

Finite Group: A group G with a finite number of elements in the associated set.

Note In a finite group $\forall a \in G$, $\exists n \in \mathbb{N}$ s.t. $a^n = e = Id$.

Def Let G be a group and $g \in G$. If there exists no $n \in \mathbb{N}$ s.t. $g^n = Id$ we say g has an infinite order.

If $\exists n$ s.t. $g^n = 1$ then

$$O(g) = \text{order of } g = \min \{i : g^i = 1\}$$

Eg. In a finite group, every element is of finite order
& Group of all roots of unity is an infinite group with elements, each having finite order.

Subgroup (Trivial → $G, \{e\}$)

A subset H of a group G is called a subgroup if you have the following properties:

i) $a, b \in H \Rightarrow ab \in H$

ii) $\exists\ 1 \in H$

iii) If $a \in H$ then $a^{-1} \in H$

Equivalently if $a, b \in H$ then $ab^{-1} \in H$ is satisfied. $H \neq \phi$.

Eg. ① $\mathbb{Q}^* \subseteq \mathbb{R}^* \subseteq \mathbb{C}^*$

② $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ subgroup of $\mathbb{C}^*$

③ $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$

④ $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, Id

Consider $H = \{\pm I_d, \pm i, \pm j, \pm k\} \subseteq GL_2(\mathbb{C})$

Ex. Check $i^2 = j^2 = k^2$ $\quad i^4 = I_d$ $\quad ji = i^3 j$

$H \rightarrow$ Quaternian group.

Ex Identify the subgroups of Integers. → Integer multiples of $\mathbb{N}$ /

EOC

8.1.19

Permutation Group

Let Ω be a non empty set. A permutation of Ω is simply a bijection $f: \Omega \to \Omega$. The set of all permutations on Ω forms a group and is denoted by S_Ω (aka the symmetric group of Ω)

$$S_\Omega = \{f : \Omega \to \Omega \mid f \text{ is bijective}\}$$

is a group with respect to composition operation

When we study for natural number set (not any Ω), ~~the~~ we have $[n] = \{1, 2, 3 \ldots, n\}$. The symmetric group on $[n]$ is denoted by S_n and the elements are termed permutations.

We can relate S_3 with D_3 but S_4 has $4! = 24$ elements while D_4 has 8 elements. Thus D_4 is a subgroup of S_4. This shows not every bijection corresponds to a transformation.

Notation :

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} \in S_6$

We can write it compactly as

$\sigma = (1\ 5)(2\ 4\ 6)$ [Can also write (15)(246)(3) (not used)]

Known as cycle decomposition of permutation

The permutation $(a_1\ a_2\ a_3 \dots a_k)$ where $a_i \in [n]$ are distinct is called a k cycle.

A two cycle is called a transposition. The k cycle $\sigma = (a_1 a_2 \dots a_k)$ is a permutation described as

$\sigma(i) = i$ if $i \notin \{a_1, \dots, a_k\}$

$\sigma(a_i) = a_{i+1}$ for $i = 1, 2, \dots, k-1$

$\sigma(a_k) = a_1$

Ex Every permutation is a product of disjoint cycles. Disjoint cycles commutes with each other.

The product of disjoint cycles is defined as follows :-

$(1\ 2\ 3)(1\ 2)(3\ 4)$

done later — done first

$(1\ 2\ 3) \cdot (1\ 2)(3\ 4) = (1\ 3\ 4)$

How to find inverse of a permutation

Let $\sigma = (1\ 5)(2\ 4\ 6)$ then

$\sigma^{-1} = (5\ 1)(6\ 4\ 2)$

Check: $\sigma \cdot \sigma^{-1}$

$(1\ 5)(2\ 4\ 6) \cdot (5\ 1)(6\ 4\ 2) = Id$

For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by the numbers of each cycle of the cycle decompositions of σ in reverse order.

To write every permutation as product of transposition :-

$$(a_1 a_2 a_3 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2)$$

Ex ☆

① $S_n = \langle (1,2), (1,3), \dots, (1\ n) \rangle$ [S_n can be generated by transposition of the form : $\langle \dots \rangle$]

② $S_n = \langle (1,2), (2,3), (3\ 4), \dots, (n-1\ n) \rangle$

Even and odd permutation

If permutation can be written as product of even k cycles

$\Rightarrow$ even permutation

else $\Rightarrow$ odd permutation.

Thus definition is not well defined since many transposition decomposition are possible.

Alt. Definitions.

Consider polynomial: $P(x_1, x_2, \dots, x_n) = \prod (x_i - x_j) \quad 1 \le j < i \le n$

Let $\sigma \in S_n$ we define

$$\sigma P(x_1, x_2, \dots, x_n) = \prod_{1 \le j < i \le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Eg $n = 3 \quad \sigma = (1\ 2\ 3) \in S_n.$

$$P(x_1, x_2, x_3) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1)$$

$$\sigma P(x_1, x_2, x_3) = (x_{\sigma(3)} - x_{\sigma(2)})(x_{\sigma(3)} - x_{\sigma(1)})(x_{\sigma(2)} - x_{\sigma(1)})$$

$= (x_1 - x_3)(x_1 - x_2)(x_3 - x_2)$

Obviously $\sigma P = P$ or $-P$

Define

~~if $\sigma(P) = +$~~

if $\sigma P = P \Rightarrow$ even permutation ~~transposition~~

if $\sigma P = -P \Rightarrow$ odd permutation

$\therefore$ transposition is always an odd permutation *

This definition being well defined and together with (*) makes the original ~~permutation~~ definition well defined

Therefore, formalising

If σ is a transposition $\sigma P = -P$

If σ is a product of an even number of transposition then $\sigma P = P$

Definition σ is said to be an even permutation if $\sigma P = P$

and σ is said to be an odd permutation if $\sigma P = -P$

Let σ be a k cycle. If k is even then σ is odd permutation and if k is odd then σ is even permutation.

Thm: The set of all even permutations forms a subgroup of the set of permutations.

Proof. $|S_n|$ (order of) $= n!$ (Try to establish bijection)

Let X = set of all even permutations
and Y = set of all odd permutations.
define $f: X \to Y$ as $f(\sigma) = (1\ 2)\sigma$

Injective: $(1\ 2)\sigma_1 = (1\ 2)\sigma_2$

$\Rightarrow (1\ 2)(1\ 2)\sigma_1 = (1\ 2)(1\ 2)\sigma_2$

$\Rightarrow \sigma_1 = \sigma_2$

Surjective:

If τ is an odd permutation,

then $(1\ 2)\tau$ is an even permutation

and $f((1\ 2)\tau) = \tau$

$\therefore f$ is a surjective map.

$\therefore |X| = |Y| = \frac{n!}{2}$ $\left[\because |S_n| = n! \text{ and } S_n = X \sqcup Y\right]$

Ex If σ is a k cycle then $\text{ord}(\sigma) = k$

Let Π be a permutation which is a product of disjoint cycles $k_1, k_2, \ldots, k_r$ then $\text{ord}(\Pi) = \text{L.C.M.}(k_1, k_2, \ldots, k_r)$

For each permutation in S_n, let

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma P = P \\ -1 & \text{if } \sigma P = -P \end{cases}$$

$\varepsilon(\sigma)$ is called the sign of σ

X ——— X

Prev Ex

4. Identify all subgroups of $\mathbb{Z}$

Let H be a subgroup of $\mathbb{Z}$, Let b be the smallest positive integer $\in H$. ~~(H is defined as smallest subgroup containing b)~~

Want to show (WTS) $H = b\mathbb{Z}$

Obviously $b\mathbb{Z} \subseteq H$

WTS $H \subseteq b\mathbb{Z}$,

Let $n \in H$ be any (+) integer

Then by division algorithm $n = qb + r \quad 0 \leq r < b$

$\therefore r = \underset{\in H}{n} - q\underset{\in H}{b} \in H$

but b is the smallest positive integer in H.

Hence $r = 0 \quad \therefore H = b\mathbb{Z}$

$\therefore$ Every subgroup of $\mathbb{Z}$ is of the form $b\mathbb{Z}$ for some integer b. (under addition)

Cyclic groups

Let G be a group. $x \in G$. Consider $H = \{\ldots x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$

H is obviously a group $\therefore$ H is a subgroup of G.

Also H is a cyclic group, since H generated by single element x.

Also H is the smallest subgroup of G containing x.

Ex ☆ How many subgroups are there in S_3?

(1) Consider the cyclic group generated by the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$$

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \forall n$$

$\langle A \rangle$: This group is an infinite cyclic group of $GL_2(\mathbb{R})$

(2) $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$

generates a cyclic group of order 6.

$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

(3) $\mathbb{Z}/p\mathbb{Z}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$

$\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \overline{10}, \bar{3}, \bar{8}, \bar{1}, \bar{6}, \overline{11}, \bar{4}, \bar{9}, \bar{2}, \bar{7}\} = \langle T \rangle$

$= \langle \bar{7} \rangle = \langle \overline{11} \rangle$

Thus every number coprime to 12 generates the group.

$\bar{2} = 12k+2$

$x, y \in \bar{2}$

$\Rightarrow x \equiv 2 \bmod n$

$y \equiv 2 \bmod 12$

$6(12k+12)$

$12\mathbb{Q}$.

10.1.19

Proposition. Let $H = \langle x \rangle$. Then

(i) If $|H| = \infty$, then $x^n \neq 1$ for any $n = 0$

(ii) If $|H| = n$ then $x^n = 1$ and $H = \{1, x, x^2, \ldots, x^{n-1}\}$

Pf (i) Suppose $x^n = 1$ for some $n \neq 0$ and assume $n > 0$.

Let $m \geq n$. Then

$$m = qn + r \quad , \quad 0 \leq r < n$$

$$\therefore x^m = x^{qn+r} = x^{qn} \cdot x^r = 1 \cdot x^r = x^r$$

Choose smallest n s.t. $x^n = 1$, $n > 0$ Then

$$x^n = 1 \Rightarrow x^{-1} = x^{n-1}$$

Then $H = \{1, x, x^2, \ldots, x^{n-1}\}$

But order of H is infinite, ie $|H| = \infty$.

Thus $x^n \neq 1$ for any $n \neq 0$

(ii) Enough to prove, order of $x = n$

Since $H = \langle x \rangle$ and H is of finite order.

$\exists a, b \in \mathbb{Z}$ s.t. $x^a = x^b$

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

Pick smallest int $m > 0$ s.t $x^m = 1$ $\quad |x| = m$

Then $H = \{1, x, x^2, \ldots, x^{m-1}\}$ ie $|H| = m$

But given $|H| = n \Rightarrow m = n$

$\therefore |x| = n$

Thm: Let H be a cyclic group generated by x

~~$H = \langle x \rangle$~~ b

(i) Every subgroup K of H is either $\{1\}$ or $\langle x^d \rangle$ where d is the smallest power of x in K

(ii) If $|H| = n$ then for every divisor d of n $\exists$ a subgroup K of order d. This subgroup is cyclic and $\langle x^{n/d} \rangle$

Proof (i) $K \neq \{1\}$ K is a subroup of H.

Consider $P = \{ n \geq 1 \mid x^n \in K \}$

By well ordering principle, P has a smallest positive integer, say d.

To show $K = \langle x^d \rangle$

It is obvious $\langle x^d \rangle \subseteq K$

Choose any element $b \in P$ s.t $x^b \in K$ & $b > d$

Then, $b = qd + r$, $0 \leq r < d$

$\Rightarrow r = b - qd$

$\therefore x^r = x^{b-qd} \in K$ but $r < d$ $\therefore r = 0$

$x^b \in \langle x^d \rangle$

$\therefore K \subseteq \langle x^d \rangle$

$\Rightarrow K = \langle x^d \rangle$

(ii) $\therefore |H| = n \Rightarrow |x| = n$. Let $n = dd'$. Now consider $\langle x^{d'} \rangle$

To show $|x^{d'}| = d$

Assum $|x^{d'}| = m$

$\Rightarrow x^{d'm} = 1$

But $|x| = n$

$\Rightarrow n \mid d'm$ or $d \mid m$

Also $(x^{d'})^d = 1$

$\therefore |x^{d'}| = d$

Ex ★ Try to prove there exists unique subgroup of order d for every divisor of n

Ex ★ Let G be a group and $x \in G$

If $|x| = n$ the $|x^a| = \frac{n}{\gcd(n,a)}$

14.1.19

Group homomorphism.

Let G and G' be groups. Then a map $f: G \to G'$ is called a group homomorphism if.

$$f(gh) = f(g)\, f(h) \qquad \forall\ g, h \in G$$

Example of Group homomorphism.

(1) Consider map det : $GL_n(\mathbb{R}) \to \mathbb{R}^\times$

$$\det(AB) = (\det A)(\det B).$$

det is a group homomorphism.

(2) $f: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$

$f(a) = e^a$ is a group homomorphism.

(3) $f: S_n \to \{\pm 1\}$

$f(\sigma) = \text{sign}(\sigma)$ is a group homomorphism.

(4) $\phi: \mathbb{Z} \to G$, G is a group with op^n multiplicatively

$n \longrightarrow a^n$ when a is fixed element in G.

$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\,\phi(n)$

$\therefore$ This is a group homomorphism.

(5) Let H be a subgroup of G. Then

$i: H \to G$ defined as $i(x) = x$ is a group hmo—

(6) Let G_1, G_2 be 2 groups. Define their product

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

For $(a,b), (c,d) \in G_1 \times G_2$ define a law of composition on $G_1 \times G_2$ as

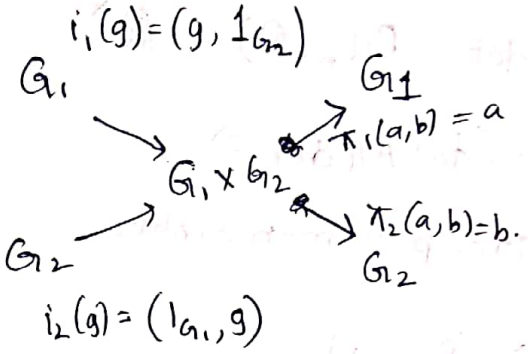
$$(a,b)\cdot(c,d) = (ac, bd)$$

Identity : $(1_{G_1}, 1_{G_2})$

Inverse of (a,b) is (a^{-1}, b^{-1})

1_{g_1}
$i(g_1, g_2)$
$= i(g_1)\ i(g_2)$
$= i($

Consider



i_1, i_2, π_1, π_2 are gp. homomorphism.

Properties of group homomorphisms.

(1) If $f: G \to G'$ be a gp homomorphism then

$f(1_G) = 1_{G'}$ and $f(a^{-1}) = (f(a))^{-1}$

(2) Let $G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3$ where $f * g$ are group homo. Then $gof : G_1 \to G_3$ is also a gp. homo.

(3) Every group homo. defines two impodant ~~sug~~ subgroups its image and kernel.

The image of a gp. homo is defined as

$$\text{im}\,\phi = \{ x \in G' \mid x \in \phi(a) \text{ for some } a \in G \}$$

Check : $\text{im}\,\phi$ is a subgrp.

The kernel of a gp. homo is defined as

$$\ker \phi = \{ x \in G \mid \phi(x) = 1_{G'} \}$$

Note that $1 \in \ker \phi$

$\ker \phi$ is a subgroup of G.

Let $g \in \ker \phi$ and $h \in G$.

$$\phi(hgh^{-1}) = \phi(h)\, g\, \phi(g)\, \phi(h^{-1})$$
$$= \phi(h)(\phi(h))^{-1}$$
$$= 1_{G'}$$
$$hgh^{-1} \in \ker \phi$$

Defⁿ A subgroup N of G is called a normal subgp. of G $(N \triangle G)$ if $ghg^{-1} \in N$ for all $h \in N$ and $g \in G$.

Ex

① $SL_n(\mathbb{R}) \triangle GL_n(\mathbb{R})$ since $\ker(\det) = SL_n(\mathbb{R})$ so it is a normal subgroup of $GL_n(\mathbb{R})$

② If $f : G_1 \longrightarrow G_2$ is a gp. homo. then

$$\ker f \triangleleft G_1$$

③ A_n is a normal subgroup of S_n.

↳ Set of all even permutation of S_n since

$$\ker(\text{sign}) = A_n .$$

(4) Every subgroup of an abelian group is a normal subgroup.

(5) Consider sub.grp. U of invertible Upper triangular matrices of $GL_2(\mathbb{R})$. Ex. Is U a normal subgroup of $GL_2(\mathbb{R})$ [Ans: No, show counter eg]

Center of a Group:

Def: Let G be any group. Then its ~~Center~~ centre $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$

Ex Is $Z(G)$ is a subgp. of G?

Ex. Let $G = S_n$ then $Z_G = \begin{cases} S_n & \text{if } n = 1, 2 \\ 1 & \text{if } n \geq 3 \end{cases}$

Show that $Z(GL_n(\mathbb{R})) = \{c I_n \mid c \in \mathbb{R}^\times\}$

EoC

15.1.19

Q. Let $f: G \to G'$ be a group homomorphism. When is it injective?

Let $\phi: S \to T$ be a mapping of sets. This map defines an equivalence relation on the domain S by the rule $a \sim b$ if $\phi(a) = \phi(b)$. For every element $t \in T$ the inverse image of t is defined as $\phi^{-1}(t) = \{s \in S \mid \phi(s) = t\}$

The inverse images are called the fibers of ϕ

Consider the group homomorphism.

$\phi : \mathbb{C}^* \longrightarrow \mathbb{R}^*_{>0}$ (modulus of complex no)

defined by $\phi(z) = |z|$

Then fibers of ϕ are concentric circles about the origin and $\mathbb{C}^* = \bigcup \phi^{-1}(r)$

Prop^{n} Let $\phi: G \to G'$ be a group homomorphism with $\ker(\phi) = N$

Let $a, b \in G$ then $\phi(a) = \phi(b)$ iff $b = an$ for some $n \in N$ or equivalently, if $a^{-1}b \in N$

Proof. Let $\phi(a) = \phi(b)$

$\phi(a)^{-1}\phi(b) = 1_{G'}$

$\phi(a^{-1}b) = 1_{G'}$

$a^{-1}b \in N$

$a^{-1}b = n$ for some $n \in N$

$\therefore \quad b = an$

Conversely if $b = an$

$$\begin{aligned}\phi(b) &= \phi(an) \\ &= \phi(a)\,\phi(n) \\ &= \phi(a)\,1_{G'} \\ &= \phi(a)\end{aligned}$$

Corollary: A grp. homo $\phi: G \to G'$ is injective if $\ker\phi = \{1_G\}$

Defn: A gp homomorphism $\phi: G \to G'$ is called an isomorphism if ϕ is 1-1 and onto. If $G' = G$ then an isomorphism is called an automorphism.

Propn: Let $\phi: G \to G'$ be a gp. homo. of finite groups.

Then

$$|G| = |\ker\phi| \cdot |\mathrm{Im}\,\phi|$$

There is a bijective map b/w elements of the image and the equivalence classes.

E.T.F the number of eqv. classes given $|G|$ on $|\ker\phi|$

* Let G be a grp and H be a subgroup of G.

A Left coset of H is defined as the subset

$$aH = \{ ah \mid h \in H \}$$

Let us define an equivalence relation on G &

Let $a, b \in G$ then $a \sim b$ if $a = bh$ for some $h \in H$

ies $b^{-1}a \in H$. This is an equiv. relation & eq. classes are of the form gH.

Therefore either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$ and G is the disjoint union of distinct left cosets of H

Def^n Number of left cosets of a subgroup H in a group G is known as the index of H in G $= [G:H]$

Is a left coset aH a subgrp of G.

→ It is not a subgroup of G.

Eg $G = \mathbb{R}^2$ and $H = \langle (1,0) \rangle$.

Then the left coset are of the form

$$v + H = \{ v + \alpha(1,0) \mid \alpha \in \mathbb{R} \}$$

This is the line parallel to x-axis that passes through pt v.

Two left cosets are either parallel or ~~disjoint~~ same.

Ex $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$

$$\left.\begin{aligned} 1+H &= \{\ldots -9, -4, 1, 6, 11, 16, \ldots\} \\ 2+H &= \{\ldots -8, -3, 2, 7, 12, \ldots\} \\ 3+H &= \{\ldots -7, -2, 3, 8, \ldots\} \\ 4+H &= \{\ldots -6, -1, 4, 9, \ldots\} \end{aligned}\right\} \text{Covers } \mathbb{Z}$$

$\mathbb{Z}$ is disjoint union of these left cosets

Let $H = n\mathbb{Z}$. Then G & H are of infinite order but there are only finitely many cosets of H namely $n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots n-1+n\mathbb{Z}$

$\therefore [\mathbb{Z} : n\mathbb{Z}] = n$.

Let G be a finite group and H is a subgroup of G. Then $|H| = |aH|$ for some $a \in G$

Define a map $f : H \to aH$ by $f(h) = ah$.

Let $f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$

$\therefore f$ is 1-1 map

f is clearly a surjective map.

$\therefore f$ is a bijection. Then $|H| = |aH|$

Lagranges Thm:

Let G be a finite gp. and H is a subgp. of G. Then $|H|$ divides $|G|$ and $|G|/|H|$ = no. of left cosets of H $= [G : H]$

Pf Let $G = H \cup a_1H \cup a_2H \cup \ldots \cup a_{r-1}H$

$$|G| = |H| r \quad \ldots (*)$$

Note that. Left cosets are equivalence classes and G can be written as disjoint union of these left cosets. Let there be r distinct left cosets say $H, a_1H, \ldots a_{r-1}H$. Then $* \Rightarrow |H|/|G|$

Examples

Let $O_n(\mathbb{R})$ be the group of all $n \times n$ orthogonal matrices. $\det : O_n(\mathbb{R}) \to \{1, -1\}$. $\ker(\det) = SO_n(\mathbb{R})$

$A \in O_n(\mathbb{R})$ now consider the left coset $A SO_n(\mathbb{R})$

$$[O_n(\mathbb{R}) : SO_n(\mathbb{R})] = 2$$

Cor Let G be a group of prime order. Then G is cyclic group.

Pf: Let $1 \neq a \in G$. Consider the cyclic subgroup $H = \langle a \rangle$ of G Then by Lagranges thm. $|H| \mid |G|$ but $|G|$ is a prime no. say p. Then $|H| = p$. $\therefore H = G$.

Warning Converse is not true. ie, if $n \mid |G|$ for a group G then G need not have a subgroup of order n

Cor: Let G be a finite gp. and $a \in G$ then $|a| \mid |G|$ and also $a^{|G|} = 1$

Proof Let $H = \langle a \rangle$ generated by a.

$|H| = |a|$.

but $|a| \mid |G|$

Let $|G| = |a| r$

$\therefore a^{|G|} = a^{|a| r} = 1$.

Prop^n Let $\phi : G \to G'$ be a gp. homo. of finite groups. Then $|G| = |\ker \phi| \cdot |\mathrm{Im}\, \phi|$

We have seen that the left cosets of $\ker \phi$ are the fibers of the map ϕ. There is a bijection b/w the elements of image set and no. of left cosets of $\ker \phi$.

$$\therefore [G : \ker \phi] = [\mathrm{Im}\, \phi]$$

$$\frac{|G|}{|\ker \phi|} = |\mathrm{Im}\, \phi|$$

$$|G| = |\ker \phi| \, |\mathrm{Im}\, \phi|$$

Eg. $\mathrm{sign} : S_n \longrightarrow \{1, -1\}$

$$[S_n : A_n] = 2$$

[EOC]

17.1.19

Example (1)

Q $K \subset H \subset G$ Let $K \triangleleft H$ and $H \triangleleft G$. Is $K \triangleleft G$?

A: Not always

Consider $W = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\} \triangleleft SL_2(\mathbb{R})$

and $SL_2(\mathbb{R}) \triangleleft GL_2(\mathbb{R})$

Ex: Show that W is not a normal subgroup of $GL_2(\mathbb{R})$

But isomorphic to $\mathbb{R}$

Define: $\phi : W \to \mathbb{R}$

$$\phi \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = x$$

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

We have $\phi(AB) = \phi(A)\,\phi(B)$

$\therefore \phi$ is a group homomorphism.

ϕ is obviously 1-1 and onto. $\Rightarrow \phi$ is an isomorphism.

Example (2) Let G be an infinite cyclic group. Show that G & $\mathbb{Z}$ are isomorphic.

Define: $\phi : \mathbb{Z} \to G = \langle a \rangle$

$n \longmapsto a^n$

Check: ϕ is an isomorphism.

Exer (3) Any finite cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$

Hint: ϕ is same as in (2)

Rem: Let G be a group.

$$Aut(G) = \{ \phi : G \to G \mid \phi \text{ is an automorphism} \}$$

automorphism: isomorphism from $G \to G$

$Aut(G)$ is a group w.r.t. fn. composition operation

Ex: Let $G = (\mathbb{Z}/3\mathbb{Z}, +)$. Then find $Aut(G)$

Eg. Inner automorphism.

Let G be a group. Fix $g \in G$

Define $i_g : G \to G$

$i_g(x) = gxg^{-1}$

$i_g(xy) = gxyg^{-1}$

$= gxIyg^{-1}$

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

$= i_g(x)\, i_g(y)$

$\therefore$ Homomorphism.

Let $i_g(x) = i_g(y)$

$\Rightarrow gxg^{-1} = gyg^{-1}$

$\Rightarrow x = y$

i_g is 1-1.

Note, $i_g(g^{-1}xg) = x$ i_g is onto.

$\therefore i_g$ is an automorphism.

The elts gxg^{-1} are called conjugates of x $\forall g \in G$

You can talk about the right coset of a subgroup H in a gp. G as well, which is denoted by

$$Hg = \{hg \mid h \in H\}$$

In general left and right cosets need not be equal.

Ex Let $H = \langle (1,2) \rangle$ be the subgroup of S_3
Find all left and right cosets of H.

Left Cosets:

$$gH = \{gh \mid h \in H\}$$

Proposition

A subgroup H of G is normal iff every left coset is also a right coset

Pf Let H be a normal subgroup of G.

Let aH be a left coset.

$$\underbrace{ah}_{\in aH} = \underbrace{aha^{-1}}_{\in H}a = \underbrace{h'a}_{\in Ha} \Rightarrow aH \subseteq Ha$$

Silly starting with elt in Ha, we can reach element aH

$$\Rightarrow Ha \subseteq aH$$

$$\Rightarrow aH = Ha.$$

Conversely, let every left coset of H be a right coset

Let $aH = Hb$

Then $a \in Ha$ (identity in H)

$a \in aH = Hb$ $\Rightarrow a \in Ha \cap Hb$

Since two left cosets are either disjoint or equal

$\Rightarrow Ha = Hb \Rightarrow aH = Ha \Rightarrow aHa^{-1} = H$

$\therefore H$ is normal sgp.

Cor If $[G:H] = 2$ Then $H \triangle G$ $a \in Ha$

Let $a \notin H$ Then $G = H \cup aH$ (aH)
$= H \cup Ha$

$\Rightarrow aH = Ha \Rightarrow H \triangleleft G.$
$\forall a \in G.$

$aH = bH \overset{?}{\Longrightarrow} abH.$

[EOC]

22.1.19

Product of Groups

Eg Let G be a group and H, K are subgroups of G.

$H \times K$. $HK = \{hk \mid h \in H, k \in K\}$

$(h_1k)(h_2k_2) \in HK$?

Let H be a normal subgroup.

$h_1k_1h_2k_2 = h_1h^*k_1k_2 \in HK$.

Ex If H or K is a normal subgroup of G then $HK = KH$ and HK is a subgroup of G.

$k^{-1}h^{-1}$

h^*k^{-1}

Thm Let H, K are subgroups of G.

① if $H \cap K = \{1\}$. then $p: H \times K \to G$ defined by $p(h,k) = hk$ is injective and its image is HK.

Pf Let (h_1, k_1) and (h_2, k_2)

$p(h_1, k_1) = p(h_2, k_2)$

$\Rightarrow h_1k_1 = h_2k_2$

$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$

$h_2^{-1}h_1 = 1 \Rightarrow h_1 = h_2$

$k_2k_1^{-1} = 1 \Rightarrow k_1 = k_2$

② If either H or K is normal. Then $HK = KH$ and HK is a sgp. of G

Pf : Ex -

(3) If both H and K are normal, and $H \cap K = \{1\}$ identity and $G_1 = HK$. Then G_1 is isomorphic to $H \times K$

$$p((h',k')\cdot(h,k)) = p(h',k')\,p(h,k)$$

$$p(h'h, k'k) = \quad = h'k'hk$$

$$\| \\ h'hk'k$$

ETS $hk' = k'h$

$\Leftrightarrow k'^{-1} h k' = h$

$\Rightarrow h^{-1}k'^{-1}hk' = 1$

$h^{-1}k'^{-1}hk' \in H$ as $k'^{-1}hk^{-1} \in H$

$h^{-1}k'^{-1}hk' \in K$ as $h^{-1}k'^{-1}h \in K$

$h^{-1}k'^{-1}hk' \in H \cap K = \{1\}$

Ex Show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$

Ex $\mathbb{Z}_r \times \mathbb{Z}_s \simeq \mathbb{Z}_{rs}$ if $\gcd(r,s) = 1$

Quotient Group : Let G be a group and H is a s'gp of G.

$G/H = \{aH \mid a \in G \text{ where } H \triangle G\}$

$=$ set of all left cosets of H.

Lemma:

The product of two left cosets, aH and bH is the left coset abH. ie $aH \cdot bH = abH$

Pf $aH \cdot bH = \{ah_1 bh_2 : h_1, h_2 \in H\}$

$ah_1 bh_2 = abh'h_2 \in abH$

Note that this is well defined.

Let $aH = a'H$ and $bH = b'H$

$a'^{-1}a \in H$ $\quad b'^{-1}b \in H$

W.T.S. $abH = a'b'H$

ie $b'^{-1}a'^{-1}ab \in H$

$b'^{-1}a'^{-1}ab = b'^{-1}hb \in H$

Prop^n G/H is a group w.r.t the operation defined as $aH \cdot bH = abH$, and identity is H, and inverse of $(gH)^{-1} = g^{-1}H$. Therefore G/H is a group.

First isomorphism Thm:

Let $\phi : G \to G'$ be a surjective gp homo. Then $G/\ker(\phi) \cong G'$

Pf Let $N = \ker \phi$

Define a map $\bar{\Phi} : G/N \to G'$

$$\bar{\Phi}(gN) = \phi(g)$$

E: Check $\bar{\phi}$ is well defined, $\bar{\phi}$ is a gp homo

Since ϕ is surjective so is $\bar{\phi}$.

$$\bar{\Phi}(g_1N) = \bar{\Phi}(g_2N)$$

$$\Rightarrow \phi(g_1) = \phi(g_2)$$

$$\Rightarrow [\phi(g_2)]^{-1}\phi(g_1) = 1.$$

$$\Rightarrow \phi(g_2^{-1}g_1) = 1$$

$$\Rightarrow g_2N = g_1N$$

$\bar{\phi}$ is injective. $\therefore \bar{\phi}$ is an isomorphism.

Examples

(1) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$

This is a subjective gp homo with ker as $SL_n(\mathbb{R})$. Therefore by 1st isomorphism thm $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$

(2) $\det : O_n(\mathbb{R}) \longrightarrow \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$

This is a surjective gp. homo

$\therefore O_n(\mathbb{R})/SO_n(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$

(3) $\text{sign} : S_n \longrightarrow \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$

This is a surj. gp. homo.

$\therefore S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$

(4) $\phi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times_{>0}$

$z \longmapsto |z|$

u is
You are

ϕ is a surj. gp homo.

$\mathbb{C}^\times/U \cong \mathbb{R}^\times_{>0}$

where $U = \ker \phi = \{ z \in \mathbb{C}^\times \mid |z| = 1 \}$

2nd Isomorphism Thm

For a non empty subset A of G define the normaliser as $N_G(A) = \{ g \in G \mid gAg^{-1} = A \}$

Thm Let G be a gp. Let A, B be subgroups of G and assume that $A \subseteq N_G(B)$ Then $A \cap B$ is a normal subgroup of A and $AB/B \cong A/A \cap B$

AB
$a_1b_1 a_2b_2$

Use $gB^{-1}g = B$
$\forall g \in A$

Ex. Show AB is a subgroup of G

WTS: $A \cap B \trianglelefteq A$

Let $x \in A \cap B$. Then $gxg^{-1} \in A$ $\forall g \in A$ i.e. $gxg^{-1} \in B$

$[\because A \subseteq N_G(B)]$

$\therefore A \cap B \trianglelefteq A$.

Now define $\phi : AB \longrightarrow A/A \cap B$.

$$\psi(ab) = a(A \cap B)$$

Swap as A in $N_G(B)$

$$\psi(ab \cdot a_1 b_1) = \psi(ab\, a_1 b_1) = \phi(a\, a_1 a_1 b_2 b_1) = aa_1(A \cap B)$$

$$\psi(ab)\psi(a_1 b_1) = a(A \cap B)\, a_1(A \cap B)$$

$$= aa_1(A \cap B)$$

ϕ is surjective as well

$$\ker \phi = \{ab \mid \phi(ab) = A \cap B\}$$

$$= \{ab \mid a(A \cap B) = A \cap B\}$$

$$= \{ab \mid a \in A \cap B\}$$

check $\ker \phi = B$.

Then by 1st isomorphism thm.

$$AB/B \cong A/A \cap B.$$

Third isomorphism theorem.

Let G be a gp and H and K are normal subgroups of G with H is a subgroup of K

Then $K/H \triangle G/H$

and $\dfrac{G/H}{K/H} \cong G/K$

Pf: $\phi : G/H \to G/K$.

$\phi(gH) = gK$

Show gp homo; find K.

—

22.1.19

$Z(GL_n(\mathbb{R})) = \{cI_n \mid c \in \mathbb{R}^*\}$ also holds for $\mathbb{C}$

$Z(SL_n(\mathbb{C})) = \{cI_n \mid c \in \mathbb{C}^*, c^n = 1\}$

$GL_n(\mathbb{C}_n) / Z(GL_n(\mathbb{C})) = PGL_n(\mathbb{C})$

$SL_n(\mathbb{C}) / Z(SL_n(\mathbb{C}))$

Ch. 2

M. 67 Pg 10

$a = (a_1 \dots a_k) \in \mathbb{R}^*$

$b = (b_1 \dots b_k) \in \mathbb{R}$

$X : [0,1] \longrightarrow \mathbb{R}^n$

$t \longrightarrow X(t) = (x_1(t) \dots x_t(t))$

~~24.1.19~~

24.1.19

Let G be a gp. and H, K are normal subgroups of G with H/K, Then $K/H \trianglelefteq G/H$.

and $\dfrac{G/H}{K/H} \cong G/K$

Pf $K/H = \{kH \mid k \in K\}$ is a subgroup of G/H.

$gH\ kH\ g^{-1}H = (gkg^{-1})H \in K/H$

$\therefore$ K/H is a normal subgroup of G/H

maybe not needed since $\ker(\phi)$ is always normal ??

Let $\varphi : G/H \to G/K$

$\varphi(gH) = gK$

Check φ is well defined

φ is a gp homomorphism.

φ is surjective.

$\ker \varphi = \{gH \mid gK = K\} = \{gH \mid g \in K\} = K/H$

$\therefore$ By first isomorphism thm

$\dfrac{G/H}{K/H} \cong G/K$

Prop Let $f: G \to \tilde{G}$ be a surj gp. homa and $K = \ker(f)$. Then $\exists$ bijection:

$$\{\text{subgroups of } G \text{ containing } K\} \longleftrightarrow \{\text{Subgroups of } \tilde{G}\}$$

$$H \longmapsto f(H)$$

verify it is a sgp of $\tilde{G}$

$$f^{-1}(\tilde{H}) \longmapsto \tilde{H}$$

And the bijection restricts to

$$\{\text{normal subgroups of } G \text{ cont. } K\} \longleftrightarrow \{\text{normal subgrps of } \tilde{G}\}$$

Pf Let H be a subgroup of G containing K.

① Then $f(H)$ is a subgroup of $\tilde{G}$ (Ex)

$f^{-1}(f(H)) \supseteq H$ is trivial.

To show $f^{-1}(f(H)) \subseteq H$

Choose $g \in f^{-1}(f(H))$

$f(g) \in f(H)$

$f(g) = f(h)$ for some $h \in H$

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

$h^{-1}g \in K$

$g = hk$ for some $k \in K \subset H$

$\in H$

$\therefore f^{-1}(f(H)) \subseteq H$

$\therefore H = f^{-1}(f(H))$

~~To show~~ ~~$f(f^{-1}(\tilde{H}) =$~~

Let $\tilde{H}$ be a subgroup of $\tilde{G}$. Consider ~~$f^{-1}(\tilde{G})$~~

$f^{-1}(\tilde{H})$ is a subgroup of G (Ex) containing K.

To show $f(f^{-1}(\tilde{H})) \subseteq \tilde{H}$ is clear.

Using surjectivity Prove the other containment [Ex]

The bijection restricts to normal subgroups [Ex].

Ex $G = \mathbb{Z}$ $K = 2\mathbb{Z}$ $H = 6\mathbb{Z}$

$G/H = \{\mathbb{Z}/6\mathbb{Z}$

$K/H = \{m + 6\mathbb{Z} \mid m$ is a multiple of $2\}$

~~$= \{6\mathbb{Z}, 6$~~

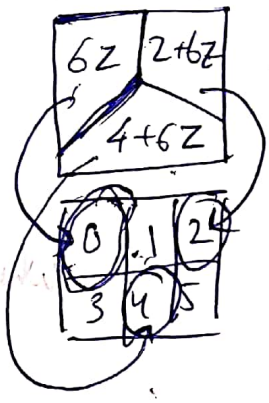
$\frac{G/H}{K/H} \cong G/K$

(2)

$6\mathbb{Z}$

$2+6\mathbb{Z}$

$4+6\mathbb{Z}$



$\{[0][2][4]\}$,

$\{[1],[3][5]$

Converse of Lagranga Thm is not true!

Eg $|S_4| = 24$ $G = A_4$ $|A_4| = 12$

W.T.S There doesnt exist any subgroup of order G in A_4.

Let H be a subgroup of G of order 6.

$[G:H] = |G|/|H| = 2$. Since index is 2, so H is a normal subgroup of G.

$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$

Klien 4-grp $\subseteq A_4$

$|H \cap V_4| \geq 2$

$(1\,2\,3)(12)(34)(1\,2\,3)^{-1} \in H$

$[\because H \trianglelefteq A_4]$

$= (14)(23)$

which implies $V_4 \subseteq H$ (contradiction)

$|H \cap V_4) = 1$

$H = \{Id, 5\ 3\text{-cycles}\}$

Note: 1st Class Test

5th Feb

29.1.19

Group Action.

29.1.19

A gp action of a gp. G on a set A is a map

from $G \times A \to A$

$$(g, s) \longmapsto gs$$

satisfying the following properties.

(1) $g_1(g_2 s) = (g_1 g_2)s \quad \forall g_1, g_2 \in G$ & $s \in A$

(2) $1 \cdot s = s \quad \forall s \in A$ and $1 \in G$

Example (1) $G = \{1, \tau\}$. where τ is reflection w.r.t x axis.

$$G \times \mathbb{C} \longrightarrow \mathbb{C}$$

$$(g, z) \longmapsto gz$$

$$gz = \begin{cases} z & , g = 1 \\ \bar{z} & , g = \tau \end{cases}$$ is a gp. action

(2) $G \times G \longrightarrow G$

$(g, x) \longmapsto gxg^{-1}$ is a gp. action

(3) G is a gp. and H a subgroup of G.

$$G \times G/H \longrightarrow G/H$$

$(g, aH) \longmapsto gaH$ is a gp. action

(4) $G \times G \longrightarrow G$

$(g, x) \longmapsto gx$.

Another representation of group action :-

Let G be a gp, A be a set. Let $g \in G$, be a fixed elt, we get a map.

$$\sigma_g : A \longrightarrow A$$
$$\sigma_g(a) = ga$$

W.T.S

σ_g is an inj. map.

$a_1, a_2 \in A$ s.t

$$\sigma_g(a_1) = \sigma_g(a_2)$$
$$\Rightarrow g a_1 = g a_2$$
$$\Rightarrow g^{-1}(g a_1) = g^{-1}(g a_2)$$
$$\Rightarrow (g^{-1}g) a_1 = (g^{-1}g) a_2 \quad \text{(Prop 1)}$$
$$\Rightarrow 1.a_1 = 1.a_2$$
$$\Rightarrow a_1 = a_2 \quad \text{(Prop 2)}$$

Surjective.

Since $\sigma_g(g^{-1}a) = a$. $\therefore$ Thus σ_g is a bijective map.

Define $\phi : G \longrightarrow S_A$ (permutation)

$$g \longrightarrow \sigma_g$$

$$[\phi(g_1)\,\phi(g_2)](a)$$
$$= \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1}(g_2 a) = g_1 g_2 a$$
$$= \sigma_{g_1 g_2}(a) = \phi(g_1 g_2)(a)$$

$\Rightarrow \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$

ϕ is a gp. homomorphism.

The above homomorphism ϕ is called the permutation representation of a given group action.

Defn The kernel of a group action is defined as

$$\{g \in G \mid gs = s \quad \forall\, s \in A\}$$

Defn For each $s \in A$, the stabilizer of s is denoted by

$$stb(s) = \{g \in S \mid gs = s\}$$

$\therefore$ Is $stb(s)$ is a subgroup?

(i) $g_1, g_2 \in stb(s)$

$\Rightarrow g_1 s = s \quad g_2 s = s.$

$g_1 g_2 s = g_1 s = s \quad \Rightarrow g_1 g_2 \in S.$

(ii) $g_1 \in stb(s)$

$g_1 s = s.$

$g_1^{-1} g_1 s = g_1^{-1} s.$

$g_1^{-1} s = s. \quad \Rightarrow g_1^{-1} \in S.$

$\therefore$ $stb(s)$ is a subgp.

Def^n

The orbit of an elt $s \in S$ denoted by $O(s) = \{gs \mid g \in G\}$

[$s \sim t$ if $\exists\, g \in G$ st. $t = gs$. $s, t \in A$]

$\sim$ is an equiv. relation on A

The orbits, therefore are equivalence classes and hence, $O(s)$ partition A

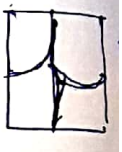
* Relation b/w $O(s)$ and $Stb(s)$

Set $O(s) = \{gs \mid g \in G\}$

$G_s = Stb(s) = \{g \in G \mid gs = s\}$

$G/G_s \xrightarrow{\phi} O(s)$

$gG_s \longmapsto gs$



Check: ϕ is well defined

W.T.S ϕ is injective.

Let $\phi(g_1 G_s) = \phi(g_2 G_s)$

$\Rightarrow g_1 s = g_2 s$

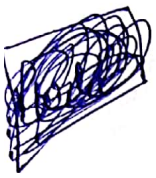
$\Rightarrow g_2^{-1} g_1 s = s$.

$g_2^{-1} g_1 \in G_s \Rightarrow g_1 G_s = g_2 G_s$

$\therefore \phi$ is injective.

$|O(s)| = [G : G_s]$

Prop^n Let G be a gp. acting on A.
For each $s \in A$ $|O(s)| = [G : G_s]$



Second hour

Def^n A gp. action of G on a set A is called transitive if there is only one orbit.
i'e given any two elements ~~from~~ $x, y \in A$

$\exists\, g \in G$ st. $x = gy$

Ex Find example of transitive group action

$\phi : G \longrightarrow S_A$

Calay's Thm

Every finite gp. G is isomorphic to a subgroup of a permutation gp. If $|G| = n$ then G is isomorphic to a subgroup of S_n.

Pf: $G \times G \longrightarrow G$

$(g, x) \longmapsto gx$

$\phi : G \longrightarrow S_n$

$\phi(g) = \sigma_g$ where $\sigma_g(x) = gx$

$\ker \phi = \{g \in G \mid \sigma_g = 1_G\} = \{g \in G \mid gx = x \ \forall x \in G\}$

$= \{1_G\}$

$\therefore$ Injective gp. homo. from $G \to S_n$.

$\therefore$ G is isomorphic to sgp of S_n.

~~Thm (Gau~~

Thm (Cauchy):

Let G be a finite group and p be a prime number s.t. $p \mid |G|$. Then G has a subgroup of ord p.

Pf Consider the set.

$$S = \{(x_1, \ldots, x_p) \mid (x_1, \ldots, x_p) \in G \times \cdots \times G \text{ and } x_1 \circ x_2 \circ \cdots x_p = 1\}$$

Let $\sigma = (1, 2, \ldots, p) \in S_p$.

$H = \langle \sigma \rangle$ & $|H| = p$

Define a gp. action.

$$H \times S \longrightarrow S$$

$$(\sigma^i, (x_1, \ldots, x_p)) \mapsto (x_{\sigma^i(1)}, x_{\sigma^i(2)}, \ldots x_{\sigma^i(p)})$$

$$|O(s)| = [H : Hs] = \frac{|H|}{|Hs|}.$$

$\therefore |O(s)|$ is either 1 or p

Suppose that $|O(s)| = 1$.

$$O((x_1, \ldots x_p)) = (x_1, \ldots, x_p)$$

$(\sigma, (x_1, \ldots, x_p)) = (x_2, x_3, \ldots, x_1)$

$\Rightarrow$ But $O(s)$ has 1 elt.

$\therefore x_1 = x_2 = \ldots = x_p$.

Observe $\sigma((1,1,1,\ldots,1)) = (1,1,\ldots,1)$

Note that $S = O(s_1) \cup \ldots \cup O(s_k)$

$|O(s)| = 1$.

$|S| = np^{-1}$; if $|G| = n$.

Since $p \mid n$ $\quad p \mid |S|$

If rest of Orbits have cardinality p.

then $1 + (k-1)p = |S|$.

But $p \mid |S|$

$\therefore \exists$ element with cardinality 1 other than identity

Infact $p-1$ elts. exist with $x^p = 1$.

Group action by Conjugation

$G \times G \longrightarrow G$

$(g, x) \longrightarrow gxg^{-1}$

$\text{Stb}(x) = \{g \in G \mid gx = xg\}$

$=: G(x)$ known as centraliser

$O(x) = \{gxg^{-1} \mid g \in G\}$

↳ Conjugacy class of $x := Gx$

$|O(x)| = 1$

$\Rightarrow gxg^{-1} = x \quad \forall g \in G$

$\Rightarrow x \in Z(G)$

$x \in Z(G)$ iff $|O(x)| = 1$

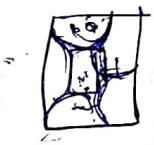
$$|G| = \sum_{i=1}^{n} 1 + \sum_{i=1}^{n} |G_i|$$

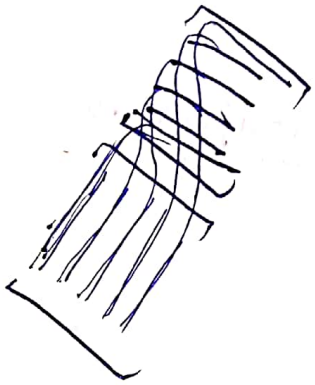
This is class eqn:

$$|G| = |Z(G)| + \sum_{i=1}^{m} |G_i|$$

5th Feb. Class Test

$aH = \{ah \mid h \in H\}$





aH

G/H

ab

9

[7]

aH

bH

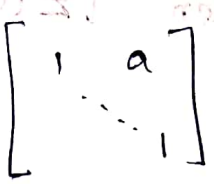
abH

29.1.19

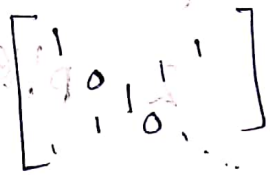
Tutorial.

Elementary matrices generate $GL_n(\mathbb{R})$.

Type 1



Type 2



Type 3

31.1.19

Defⁿ A gp. of order p^n, p is a prime number and $n \in \mathbb{N}$ is called a p group.

Propⁿ Let G be a p-group. Then $|Z(G)| \geq p$.

Let $|Z(G)| = 1$

Then $|G| = 1 + \sum_{i=1}^{n} |G_{g_i}|$

Now $p \mid |C_{g_i}| \ \forall i$ & $p \mid |G|$

$\Rightarrow p \mid 1$ which is a contradiction

$|Z(G)| \geq p$.

Corr

An group of order p^2 is abelian.

By prev. propⁿ. we have $|Z(G)| \geq p$

WTS $|Z(G)| = p^2$

Let $|Z(G)| = p$ & $x \in G \setminus Z(G)$

& $Z(G) \subsetneq C(x)$ as $x \in C(x) \setminus Z(G)$

$|C(x)| = p^2$ i.e $C(x) = G$

which is a contradiction

~~$\therefore |C(x)| =$~~

$\therefore Z(G) = G$.

$\therefore G$ is abelian gp.

Corr Any group of order p^2 is ismorphic to

$\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

↳ check if G has ~~order~~ elt. of order p^2
if yes we are done
else go for 2nd case.

Pf Let $1 \neq x \in G$. Then $|x| = p$ or $|x| = p^2$.

If $|x| = p^2$ then $G \cong \mathbb{Z}/p^2\mathbb{Z}$

O/w Assume that $\nexists$ any elt. of order p^2 in G.
∴ All elts. of order p.
Consider $H = \langle x \rangle$
Let $1 \neq y \in G \setminus H$
Then $|y| = p$. Let $K = \langle y \rangle$
$H \cap K = \{1\}$. [As its order divides p. But cannot be p.]

Consider HK [normal subgrps H, K as G abelian]
↳ is a subgroup.

$|HK| = p^2$
∴ $G = HK$

Consider $\phi : H \times K \longrightarrow HK \equiv G$
$(h, k) \longrightarrow hk$

is an isomorphism.
∴ $G \cong H \times K$, where $H \cong \mathbb{Z}/p\mathbb{Z}$ and $K \cong \mathbb{Z}/p\mathbb{Z}$

∴ $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Sylow's Th...

Defn Let G be a group of order $p^\alpha m$ where $p \mid m$ then the subgroup of order p^α is called a Sylow p subgroup of G.

n_p denotes no. of Sylow p subgroup of ~~order~~ G.

Thm Let G be a gp. of order $p^\alpha m$ where $p \nmid m$ and p is a prime number. Then

1. Sylow p subgroup exist. ie a sbgp of order p^α in G
2. If P is a Sylow p-subgp of G and Q is any p-subgroup of G then $\exists\ g \in G$ s.t. $Q \subseteq gPg^{-1}$ ie Q is contained in some conjugate of P

In particular any two Sylow p subgroups are conjugate in G.

Remark If there is only 1 Sylow p-subgp of G then it will be a normal subgroup of G

3. $n_p \equiv 1 \pmod p$ and $n_p \mid m$

Group of order 15

$15 = 3 \cdot 5$

$n_3 \equiv 1 \pmod 3 \qquad n_3 \mid 5 \Rightarrow n_3 = 1$

$n_5 \equiv 1 \pmod 5 \qquad n_5 \mid 3 \Rightarrow n_5 = 1$

Let H and K be subgroups of G of order 3 and 5 respectively

Let $H = \langle x \rangle$ and $K = \langle y \rangle$

$|x| = 3$ and $|y| = 5$

$H \cap K = \{1\}$

H, K are normal subgroups.

$|HK| = 15 \Rightarrow HK = G$

$G \cong H \times K$

$\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$

$\therefore \exists$ only one gp. of ord. 15 which is $\mathbb{Z}/15\mathbb{Z}$ upto isomorphism.

Ex Characterize the group of order 21