

I N D E X

NAME: AKASH MANDAL STD.: Sem 6 SEC.: _____ ROLL NO.: 16MA20³ SUB.: MODERN ALGEBRA

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

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 - Ghorion

→ Group Theory

→ Subgroups

→ Cyclic

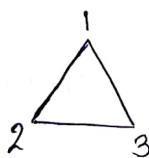
↓
→ Sylow's Theorems

→ Ring Theory.

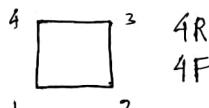
Intro

Started to study symmetry of objects. (Motivation)

Consider



Also for square



Certain operations.

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

followed by



gives

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 returns 0° or identity transformation

Symmetries \rightarrow 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.

- $|AB| = |A||B| = 1$
- $AJ = A$
- 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 ~~is orthogonal~~.

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 $f: S \times S \rightarrow S$ $f(a, b)$ often denoted by $a+b$ or ab

Examples

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

(2) $\text{GL}_n(\mathbb{R}) = A$ $f: A \times A \rightarrow A$ defined as $f(B, C) = BC$

(3) $S = \text{Set of all maps from } T \rightarrow T$, 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 $\forall a, b, c \in S$

$$(ab)c = a(bc)$$

② A law of composition is said to be commutative if $\forall a, b \in S$

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

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_1 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 $f: S \times S \rightarrow S$. $f(a, b)$ often denoted by $a+b$ or ab .

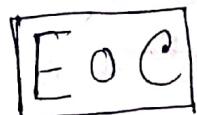
Examples

- (1) $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(a, b) = a + b$
- (2) $\text{GL}_n(\mathbb{R}) = A$ $f: A \times A \rightarrow A$ defined as $f(B, C) = BC$
- (3) $S = \text{Set of all maps from } T \rightarrow T$, T is a set
 - $f(f_1, f_2) = f_1 \circ f_2$ $f_1, f_2 \in S$
 - 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



7.1.19

Dihedral groups. Rotations Flips.

$$D_4 = \left\{ I_d, \underbrace{(1234)}_{\text{consecutive mapping}}, (13)(24), (14)(32), (24), (12)(34), (13), (14)(23) \right\}$$

Study symmetry of regular n-gon

$$D_n \rightarrow 2n \text{ elements}$$

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 i.e. $ab = ba \forall a, b \in G$ is called an abelian group. E.g. $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ abelian over + $GL_n(\mathbb{R})$ not abelian over \times .

Eg D_n : not abelian

Ex. 

Identity element is unique in a group.

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

$$\cancel{e * e' = e} \quad a * e = a \quad \forall a \in G$$

$$\therefore e' * e = e' \quad \dots \textcircled{1}$$

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

$$\therefore e' * e = e \quad \dots \textcircled{2}$$

$$\therefore \textcircled{1}, \textcircled{2} \rightarrow e' = e \Rightarrow \Leftarrow$$

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

Similar

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

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

Then the inverse of a denoted as

$$-a$$

(ii) If law of composition is written multiplicatively

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

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

Ex

Show that in a group.

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

Finite Group: A group G_1 with a finite number of elements in the associated set.

Note In a finite group $\forall a \in G_1, \exists n \in \mathbb{N}$ s.t. $a^n = \text{Id}$.

Def Let G_1 be a group and $g \in G_1$. If there exists no $n \in \mathbb{N}$ s.t. $g^n = \text{Id}$ we say g has an infinite order.

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

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

E.g. 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 ($\text{Trivial} \rightarrow G, \{e\}$)

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

$$\text{i) } a, b \in H \Rightarrow ab \in H$$

$$\text{ii) } \exists 1 \in H$$

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

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

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

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

Ex. Check $i^2 = j^2 = k^2, i^4 = Id, ji = ij$

$H \rightarrow$ Quaternionian group.

Ex

Identify the subgroups of Integers. \rightarrow Integer multiples of \mathbb{N}

★

EOC

8.1.19

Permutation Group

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

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

is a group with respect to composition operation

When we study for natural number set (not any Ω), we have $[n] = \{1, 2, 3, \dots, n\}$. 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 :

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

We can write it compactly as

$$\sigma = (1\ 5)(2\ 4\ 6) \quad \left[\begin{array}{l} \text{Can also write} \\ (1\ 5)(2\ 4\ 6)(3) \\ \text{(not used)} \end{array} \right]$$

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

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

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

$$\sigma(a_k) = a_1$$



Every permutation is a product of disjoint cycles.

Disjoint cycles commutes with each other.

The product of disjoint cycles is defined as follows:

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

done later done first

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

How to find inverse of a permutation

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

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

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

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

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. Find the number of transpositions in S_n .

- Ex** S_n can be generated by transposition of the form : <...>
- ① $S_n = \langle (1, 2), (1, 3), \dots, (1, n) \rangle$
 - 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. Definition.

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

Let $\sigma \in S_n$ we define

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

if $n=3 \quad \sigma = (1, 2, 3) \in S_3$.

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

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

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

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

Define

~~If $\sigma(P) = P$~~

if $\sigma P = P \Rightarrow$ even 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. $|S_n| = n!$ (Try to establish bijection)

Let $X = \text{set of all even permutations}$

and $Y = \text{set of all odd permutations}$.

define $f: X \rightarrow Y$ 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.

$$\therefore |X| = |Y| = \frac{n!}{2} \quad [\because |S_n| = n! \text{ and } S_n = X \cup Y]$$

Ex *

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

order

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

For each permutation in S_n , let

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

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

Prev
Ex

1. 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 $n = qb + r$ $0 \leq r < b$

$$r = n - qb \in H$$

but b is the smallest positive integer in H .

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

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

Cyclic groups

Let G_1 be a group. $x \in G_1$. Consider $H = \{ \dots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, \dots \}$

H is obviously a group. $\therefore H$ is a subgroup of G_1 .

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

Also H is the smallest subgroup of G_1 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.

$$(3) \mathbb{Z}/p\mathbb{Z} \quad \langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10} \}$$

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

Thus every number coprime to 12, generates the group.

$$\frac{6(12k+2)}{120}$$

10.1.19

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

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

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

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

Let $m \geq n$. Then

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

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

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

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

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

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

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.

$$\exists a, b \in \mathbb{Z} \text{ s.t. } x^a = x^b \\ \Rightarrow x^{a-b} = 1$$

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

Then $H = \{1, x, x^2, \dots, x^{m-1}\}$ i.e. $|H| = m$

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

$$\therefore |x| = n$$

Thm: Let H be a group generated by x

$$H = \langle x \rangle$$

(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 subgroup of H .

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

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

$$\text{To show } K = \langle x^d \rangle$$

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

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

$$\text{Then, } b = qd + r, \quad 0 \leq r < d$$

$$\Rightarrow r = b - qd$$

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

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

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

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

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

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

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

Then $x^{d'm} = 1$

But $|x| = n$

$$\Rightarrow n | d'm \quad \text{or} \quad d | m$$

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

∴ $|x^{d'}| = d$

Ex

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

Ex

Let G be a group and $x \in G$

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

14.1.19.

Group homomorphism.

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

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

Example of Group homomorphism -

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

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

\det is a group homomorphism.

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

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

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

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

(4) $\phi: \mathbb{Z} \rightarrow G$, G is a group with op \circ multiplicatively
 $n \rightarrow a^n$, when a is fixed element in G .

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

This is a group homomorphism.

(5) Let H be a subgroup of G . Then
 $i: H \rightarrow G$ defined as $i(x) = x$ is a group homomorphism.

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

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

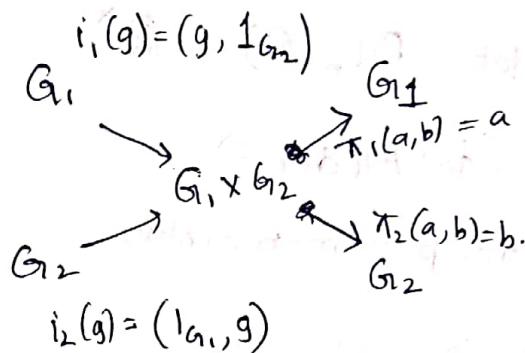
For $(a, b), (c, d) \in G_1 \times G_2$ define a law of composition on $G_1 \times G_2$ as

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

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

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

Consider



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

Properties of group homomorphisms

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

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

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

(3) Every group homo. defines two important 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 $h \in G$.

$$\begin{aligned}\phi(hgh^{-1}) &= \phi(h) \circ \phi(g) \circ \phi(h^{-1}) \\ &= \phi(h)(\phi(h))^{-1} \\ &= 1_G\end{aligned}$$

$$hgh^{-1} \in \ker \phi$$

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

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

② If $f: G_1 \rightarrow G_2$ 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 $GL_2(\mathbb{R})$. Eg. Is U a normal subgroup of $GL_2(\mathbb{R})$
[Ans: No, show Counter eg]

Center of a Group:

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

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

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

EOC

Q2

Final Exam

Not applicable for this question

Q3 The order of the center of S_3 is (A) 1 or (B) 2 or (C) 3 or (D) 4 or (E) 5

Ans: (B) 2
Sol: Center of S_3 is $\{e, (12)\}$

Q4 If G is a group of order 10, then the number of subgroups of G is (A) 1 or (B) 2 or (C) 3 or (D) 4 or (E) 5

Ans: (B) 2
Sol: If G is a group of order 10, then the number of subgroups of G is 2.

Q5 If G is a group of order 10, then the number of subgroups of G is (A) 1 or (B) 2 or (C) 3 or (D) 4 or (E) 5

Ans: (B) 2
Sol: If G is a group of order 10, then the number of subgroups of G is 2.

Q6 If G is a group of order 10, then the number of subgroups of G is (A) 1 or (B) 2 or (C) 3 or (D) 4 or (E) 5

Ans: (B) 2
Sol: If G is a group of order 10, then the number of subgroups of G is 2.

Q7 If G is a group of order 10, then the number of subgroups of G is (A) 1 or (B) 2 or (C) 3 or (D) 4 or (E) 5

15.1.19

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

Let $\phi: S \rightarrow T$ 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.

$$\phi: \mathbb{C}^* \rightarrow \mathbb{R}_{\geq 0}^* \quad (\text{modulus of complex no})$$

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

Then fibers of ϕ are concentric circles about the origin

$$\text{and } \mathbb{C}^* = \bigsqcup \phi^{-1}(r)$$

Prop: Let $\phi: G \rightarrow G'$ 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.

$$\text{Let } \phi(a) = \phi(b)$$

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

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

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

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

$$\therefore b = an$$

Conversely if $b = an$

$$\phi(b) = \phi(an)$$

$$= \phi(a) \phi(n)$$

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

$$= \phi(a)$$

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

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

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

Then

$$|G'| = |\ker \phi| \oplus |\text{Im } \phi|$$

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

ETF: The number of eq. classes given by $|G|/\ker \phi$.

* 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 $h \in H$

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

Therefore either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$ and
 G_1 is the disjoint union of distinct left cosets of H

Defn 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 all a subgroup of G .

\rightarrow It is not a subgroup of G .

for a example $\{Hx\} = \{H\}$ is not a subgroup of G .

as $Hx \cdot H = HxH \neq H$ for $x \in G$

and $Hx \cdot H = HxH = Hx \neq H$ for $x \in G$

as $Hx \cdot H = HxH = Hx \neq H$ for $x \in G$

Ex $G_1 = \mathbb{R}^2$ 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 $G_1 = \mathbb{Z}$ and $H = 5\mathbb{Z}$

$$1+H = \{-9, -4, 1, 6, 11, 16, \dots\}$$

$$2+H = \{-8, -3, 2, 7, 12, \dots\}$$

$$3+H = \{-7, -2, 3, 8, \dots\}$$

$$4+H = \{-6, -1, 4, 9, \dots\}$$

\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 $n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \dots, n-1+n\mathbb{Z}$

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

Let G_1 be a finite group and H is a subgroup of G_1 . Then $|H| = |aH|$ for some $a \in G_1$. Define a map $f: H \rightarrow aH$ 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_1 be a finite gp. and H is a subgp. of G_1 . Then $|H|$ divides $|G_1|$ and $|G_1|/|H| = \text{no. of left cosets of } H = [G_1 : H]$

Pf. Let $G = H \cup a_1H \cup a_2H \cup \dots \cup a_r H$

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

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 $H, a_1H, \dots, a_{r-1}H$, Then $\Rightarrow |H||G|$

Examples

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

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

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

Ques: Let G_1 be a group of prime order. Then G_1 is cyclic group.

Pf.: Let $1 \neq a \in G_1$. Consider the cyclic subgroup $H = \langle a \rangle$ of G_1 .
Then by Lagranges Thm. $|H| \mid |G_1|$ but $|G_1|$ is a prime no. say p . Then $|H| = p \therefore H = G_1$.

Warning Converse is not true. i.e., if $n \mid |G_1|$ for a group G_1 then G_1 need not have a subgroup of order n

Ques: Let G_1 be a finite gp. and $a \in G_1$ then $|a| \mid |G_1|$
and also $a^{|G_1|} = 1$

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

$$\begin{aligned} |H| &= |a| \\ \text{but } |a| &\nmid |G_1| \end{aligned}$$

$$\begin{aligned} \text{Let } |G_1| &= |a| r \\ \therefore a^{|G_1|} &= a^{|a|r} = 1. \end{aligned}$$

Prop

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

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

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 & no. of left cosets of $\ker \phi$.

$$\therefore [G : \ker \phi] = |\text{Im } \phi|$$

$$\frac{|G|}{|\ker \phi|} = |\text{Im } \phi|$$

$$|G| = |\ker \phi| \cdot |\text{Im } \phi|$$

e.g. sign: $S_n \xrightarrow{\sim} \{1, -1\}$

$$[S_n : A_n] = 2$$

$$[EOC]$$

17.1.19

Example (1) 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: $\phi: W \rightarrow \mathbb{R}$

$$\phi \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right) = x$$

$$\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \right) = \left(\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \right)$$

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 $G \cong \mathbb{Z}$ are

isomorphic.

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

$$n \mapsto a^n$$

Check: ϕ is an isomorphism.

Ex (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.

$\text{Aut}(G) = \left\{ \phi: G \rightarrow G \mid \phi \text{ is an automorphism} \right\}$
isomorphism from $G \rightarrow G$

$\text{Aut}(G)$ is a group w.r.t. fn. composition operation

Eg: Let $G_1 = (\mathbb{Z}/3\mathbb{Z}, +)$. Then find $\text{Aut}(G_1)$

Eg. Inner automorphism.

Let G_1 be a group. Fix $g \in G_1$

Define $i_g: G_1 \rightarrow G_1$

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

$$i_g(xy) = g x y g^{-1}$$

$$= g x g^{-1} y g^{-1}$$

$$= g x g^{-1} \cdot y g^{-1}$$

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

\therefore Homomorphism.

$$\text{let } i_g(x) = i_g(y)$$

$$\Rightarrow g x g^{-1} = g y g^{-1}$$

$$\Rightarrow x = y$$

i_g is 1-1.

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

$\therefore i_g$ is an automorphism.

The elts $g x g^{-1}$ 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:

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

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

[Ans]

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.

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

Similarly starting with Ha 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

$$\text{Let } aH = Hb$$

$$\text{Then } a \in Ha \quad \left. \begin{array}{l} a \in aH = Hb \\ \text{identity in } H \end{array} \right\} \Rightarrow a \in Ha \cap Hb$$

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 $H \trianglelefteq G$

$$\begin{aligned} \text{Let } a \notin H \quad \text{Then } G &= H \cup aH \\ &= H \cup Ha \end{aligned}$$

$$\Rightarrow aH = Ha \Rightarrow H \trianglelefteq G$$

$\forall a \in G$,

$$aH = bH \stackrel{?}{=} abH$$

[EOC]

2) G is a group of order n . If H is a subgroup of G and $|H| = \frac{n}{2}$, then H is normal in G .

$\forall a \in H$ we have to show $aH = Ha$

$$aH = Ha \Leftrightarrow aH \cap Ha \neq \emptyset$$

The elements of aH are $aH_1, aH_2, \dots, aH_{\frac{n}{2}}$ and the elements of Ha are $H_1a, H_2a, \dots, H_{\frac{n}{2}}a$

$$H_i \neq H_j$$

$$H_i \neq H_j$$

Since $aH \cap Ha \neq \emptyset$ there exists H_i such that $aH_i = H_i a$

$$aH_i = H_i a$$

iff $aH_i = H_i a$

long as $aH_i = H_i a$ then $aH = Ha$

$H = aH \Leftrightarrow aH = Ha \Leftrightarrow aH = H$

$\therefore H$ is normal in G

22.1.19. Product of Groups

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

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

$$(h_1, k_1)(h_2, k_2) \in HK ?$$

Let H be a normal subgroup.

$$h_1 k_1 h_2 k_2 = h_1 h^* k_1 k_2 \in HK$$

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

Ihm Let H, K are subgroups of G .

① If $H \cap K = \{1\}$ then $p: H \times K \rightarrow G$
 defined by $p(h, k) = hk$ is bijective
 and its image is $HK = \{hk \mid h \in H, k \in K\}$

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

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

$$\Rightarrow h_1 k_1 = h_2 k_2$$

$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K = \{1\}$$

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

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

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

$H \times K$

$$p((h', k') \cdot (h, k)) = p(h', k') \cdot p(h, k) = 1.$$

$$p(h'h, k'k) = h'hk'k = h'k' \in H \cap K = \{1\}$$

$$h'hk'k$$

$$\text{ETS } hk' = k'h$$

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

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

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

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

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

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

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

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

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

= set of all left cosets of H .

Lemma:

The product of two left cosets aH and bH is the

left coset abH . i.e. $(aH \cdot bH) = abH$

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

$$ah_1 b h_2 = abh_1' h_2 \in abH$$

Note that this is well defined.

$$\text{Let } aH = a'H \text{ and } bH = b'H$$

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

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

i.e. $b'^{-1}a'^{-1}ab \in H$

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

Propn 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 $\phi: G \rightarrow G'$ be a surjective gp. homo. Then

$$G/\ker(\phi) \cong G'.$$

Pf

Let $N = \ker \phi$

Define a map $\bar{\phi}: G/N \rightarrow G'$

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

E²: 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

$$(1) \det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$$

This is a subjective gp. homo. with

Ker as $SL_n(\mathbb{R})$. Therefore by 1st isomorphism

$$\text{thm } GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$$

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

Thus is a surjective gp. homo

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

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

This is a surj. gp. homo.

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

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

$$z \mapsto |z|.$$

ϕ is a surj. gp. homo.

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

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

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

$$AB \quad \text{Use } gB^{-1}g = B \\ a_1 b_1 a_2 b_2 \quad \forall g \in A$$

Ex. Show AB is a subgroup of G

WTS: $A \cap B \trianglelefteq A$
Let $x \in A \cap B$. Then $g^{-1}xg \in A \Leftrightarrow \forall g \in A \exists a \in A \text{ s.t. } g^{-1}xg = a \in A$
 $\therefore A \subseteq N_G(B)$

$\therefore A \cap B \trianglelefteq A$

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

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

swap as A in $N_G(B)$

$$\phi(ab \cdot a_1 b_1) = \phi(ab a_1 b_1) = \phi(a_1 a_2 b_1 b_2) = a_1(A \cap B)$$

$$\begin{aligned}\phi(ab) \phi(a_1 b_1) &= a(A \cap B) a_1(A \cap B) \\ &= a a_1(A \cap B)\end{aligned}$$

ϕ is surjective as well

$$\begin{aligned}\ker \phi &= \{ab \mid \phi(ab) = A \cap B\} \\ &= \{ab \mid a(A \cap B) = A \cap B\} \\ &= \{ab \mid a \in A \cap B\}\end{aligned}$$

check $\ker \phi = B$.

Then by 1st isomorphism thm:

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

$$B \trianglelefteq AB$$

$$BA$$

$\Rightarrow B$ is normal in AB and $AB/B \cong A/A \cap B$

Third isomorphism theorem.

Let G_1 be a gp and H and K are normal subgroups of G_1 with H is a subgroup of K .

Then $K/H \trianglelefteq G/H$

$$\text{and } G/H /_{K/H} \cong G/K$$

$$\text{Pf: } \phi: G/H \rightarrow G/K.$$

$$\phi(gH) = gK$$

Show gp homo; find $K \cdot H = H$

22.1.19

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

$$Z(SL_n(\mathbb{C})) = \{cI_n \mid c \in \mathbb{C}^\times \text{ and } c^n = 1\}$$

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

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

Ch. 2

TM. 6? Pf 10

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

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

$$x: [0, 1] \rightarrow \mathbb{R}^n$$

$$t \mapsto x(t) = (x_1(t), \dots, x_n(t))$$

~~24.1.19~~

24.1.19

Let G be a gp. and H, K are normal subgroups of G

with $H/K \trianglelefteq$, Then $K/H \trianglelefteq G/H$. { \trianglelefteq is subgroup & \trianglelefteq is normal}

$$\text{and } G/H /_{K/H} \cong G/K$$

Pf

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

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

K/H is a normal subgroup of G/H .

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

$$\varphi(gH) = gK$$

check φ is well defined when $gH = H$ and $gK = K$

φ is a gp. homomorphism.

φ is surjective. $H \in \{H\}$

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

By first isomorphism theorem

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

$$I = (g, gK)$$

$$I = (g)$$

$H \oplus I \neq I$ unless $gH = g$

$$H \oplus I$$

$$H \oplus (gK) \neq I$$

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

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

$$\begin{array}{ccc} \{ \text{subgroups of } G \} & \xleftarrow{\quad \text{containing } K \quad} & \{ \text{subgroups of } \tilde{G} \} \\ H & \xleftrightarrow{f} & f(H) \end{array}$$

Verify it is a sgp of \tilde{G}

$$f^{-1}(f(H)) \xrightarrow{\quad \text{Verify } f \text{ is surj} \quad} f(H)$$

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

And the bijection restricts to

$$\begin{array}{ccc} \{ \text{normal subgrps} \} & \xleftarrow{\quad \text{of } G \text{ cont. } K \quad} & \{ \text{normal subgrps} \} \\ \{ \text{normal subgrps} \} & \xleftarrow{\quad \text{of } \tilde{G} \quad} & \{ \text{normal subgrps} \} \end{array}$$

Pf let H be a subgroup of G containing K .

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

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

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

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

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

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

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

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

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

$$\Rightarrow g \in H$$

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

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

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

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

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

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

Using surjectivity, prove the other containment [Ex]

Containment

[Ex]

The bijection restricts to normal subgroups [Ex].

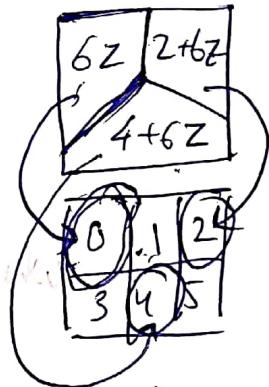
The bijection restricts to normal subgroups [Ex].

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

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

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

$$= \{6\mathbb{Z}, 0\}$$



$$\frac{G/H}{K/H} \cong \frac{G/K}{H} = \mathbb{Z}_2$$

(Ex: $\mathbb{Z}/6\mathbb{Z}$)

(Ex: $\mathbb{Z}/3\mathbb{Z}$)

$$\begin{aligned} & \{[0][2][4]\}, \\ & \{[3][5]\} \end{aligned}$$

test (and) tel zotu

dot wtf do we do?

Converse of Lagrange Thm is not true.

~~Ex~~ $|S_4| = 24 \quad G = A_4 \quad |A_4| = 12$

W.T.S There doesn't exist any subgroup of order 6 in A_4 .

Let H be a subgroup of G of order 6.

$[G:H] = \frac{|G|}{|H|} = 2$. Since index is 2, so H is a normal subgroup of G .

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

Klein 4-grp $\subseteq A_4$

$$|H \cap V_4| \geq 2$$

$$(123)(12)(34)(123)^{-1} \in H$$

$$[(123)(12)(34)(123)^{-1}]^2 = (14)(23) \in H$$

$$= (14)(23)$$

which implies $V_4 \subseteq H$ (contradiction)

$$|H \cap V_4| = 1$$

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

Note: 1st Class Test

5th Feb

29.1.19

Group Action.

29.1.19

A gp action of a gp. G_1 on a set A is a map

from $G_1 \times A \rightarrow A$

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

satisfying the following properties.

$$(1) g_1(g_2s) = g_1g_2s \quad \forall g_1, g_2 \in G_1 \text{ & } s \in A$$

$$(2) 1.s = s \quad \forall s \in A \text{ and } 1 \in G_1$$

Example (1) $G_1 = \{1, \tau\}$, where τ is reflection w.r.t x-axis.

$$G_1 \times \mathbb{C} \rightarrow \mathbb{C}$$

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

$$\begin{cases} z \mapsto \bar{z} & \text{if } g = 1 \\ z \mapsto -\bar{z} & \text{if } g = \tau \end{cases}$$

is a gp. action

(2) $G_1 \times G_1 \rightarrow G_1$,
 $(g, x) \mapsto gxg^{-1}$ is a gp. action

(3) G_1 is a gp. and H a subgroup of G_1 .

$$G_1 \times G_1/H \rightarrow G_1/H$$

$(g, aH) \mapsto gah^{-1}$ is a gp. action

(4) $G \times G \rightarrow G$

$$(g, x) \mapsto gx$$

Another representation of group action :-

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

$$\sigma_g : A \rightarrow A$$

$$\sigma_g(a) = ga$$

W.T.S

σ_g is an inj. map.

$a_1, a_2 \in A$ s.t.

$$\sigma_g(a_1) = \sigma_g(a_2)$$

$$\Rightarrow ga_1 = ga_2$$

$$\Rightarrow g^{-1}(ga_1) = g^{-1}(ga_2)$$

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

$$\Rightarrow 1.a_1 = 1.a_2$$

$$\Rightarrow a_1 = a_2 \quad (\text{Prop 2})$$

Surjective.

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

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

$$g \mapsto \underline{\sigma_g}$$

$$\underline{\phi(g)}$$

$$[\phi(g_1) \phi(g_2)](a)$$

$$= \sigma_{g_1}(\sigma_{g_2}(a)) = \sigma_{g_1}(g_2 a) = g_1 g_2 a$$

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

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

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:

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

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

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

Is $stab(s)$ is a subgroup?

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

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

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

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

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

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

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

$stab(s)$ is a subgp.

Defn

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

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

\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 $stab(s)$

$$set \quad O(s) = \{gs | g \in G\}$$

$$G_s = stab(s) = \{g \in G | gs = s\}$$

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

$$gG_s \mapsto gs$$

Check: ϕ is well defined

M.T.S ϕ is injective.

$$\text{Let } \phi(g_1 G_s) = \phi(g_2 G_s)$$

$$\Rightarrow g_1 s = g_2 s$$

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

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

$\therefore \phi$ is injective.

$$|O(s)| = [G : G_{s_s}]$$

Prop^n Let G_1 be a gp. acting on A .

For each $s \in A$ $|O(s)| = [G_1 : G_{s_s}]$

Second hour

Def^n A gp. action of G_1 on a set A is called

transitive if there is only one orbit.

i.e given any two elements ~~in~~ $x, y \in A$

$$\exists x, y \in A \quad \exists g \in G \text{ st. } x = gy$$

Ex Find example of transitive group action

$$\phi: G \rightarrow S_A$$

Cayley'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: $G \times G \rightarrow G$

$$(g, x) \mapsto gx$$

$$\phi: G \rightarrow S_n$$

$$\phi(g) = \sigma_g \text{ where } \sigma_g(x) = gx$$

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

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

$\therefore G$ is isomorphic to sgr 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 order p .

Pf Consider the set

$$S = \{(x_1, \dots, x_p) \mid (x_1, \dots, x_p) \in G \times \dots \times G \text{ and } x_1 \cdot x_2 \cdot \dots \cdot x_p = 1\}$$

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

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

Define a grp. action.

$$H \times S \longrightarrow S$$

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

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

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

Suppose that $|\mathcal{O}(s)| = 1$.

$$\mathcal{O}((x_1, \dots, x_p)) = (x_1, \dots, x_p)$$

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

⇒ But $O(s)$ has 1 elt.

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

Observe $O(1, 1, 1, \dots, 1) = (1, 1, \dots, 1)$

Note that $S = O(s_1) \cup \dots \cup O(s_k)$
 $|O(s)| = 1$.

$$|S| = n^p; |G| = n.$$

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

If rest of orbits have cardinality p .

$$\text{then } 1 + (k-1)p = |S|.$$

$$\text{But } p \mid |S|$$

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

In fact $p-1$ elts. exist with $x^p = 1$.

Group action by Conjugation

$$G \times G \rightarrow G$$

$$(g, x) \xrightarrow{\text{def}} gxg^{-1}$$

$$\text{stab}(x) = \{g \in G \mid g^{-1}xg = x\}$$

$=: G(x)$ known as centraliser

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

Conjugacy class of $x := Gx$

$$|O(x)| = 1$$

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

$$\rightarrow x \in Z(G)$$

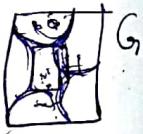
$x \in Z(G)$ iff $|OG(x)| = 1$

$$|G| = \sum_{i=1}^n (1 + \sum_{j=1}^n |G_{g_i}|)$$

This is dan eqn:

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

5th Feb. Class Test



alt

G/H [0]



[z]

alt

bH

abH

1 - 1000

29.1.19

Tutorial.

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

Type 1: $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$ and transpose of a col swap.

Type 2: $\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{bmatrix}$ and row swap.

Type 3: $\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{bmatrix}$ and col swap.

Example: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

Row 1 and 2 swap: $\begin{pmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \\ 7 & 8 & 9 \end{pmatrix}$

Row 1 and 3 swap: $\begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$

(Col 1, 2, 3)

Col 1 and 2 swap: $\begin{pmatrix} 5 & 4 & 6 \\ 2 & 1 & 3 \\ 8 & 7 & 9 \end{pmatrix}$

(Col 1, 2)

Col 1 and 3 swap: $\begin{pmatrix} 5 & 6 & 4 \\ 2 & 3 & 1 \\ 8 & 9 & 7 \end{pmatrix}$

(Col 1, 3)

Col 2 and 3 swap: $\begin{pmatrix} 5 & 4 & 6 \\ 2 & 3 & 1 \\ 8 & 7 & 9 \end{pmatrix}$

(Col 2, 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_1 be a p -group. Then $|Z(G_1)| \geq p$.

Let $|Z(G_1)| = 1$

$$\text{Then } |G_1| = 1 + \sum_{i=1}^n |G_{g_i}|$$

Now $p \mid |G_{g_i}| \forall i$ & $p \mid |G_1|$

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

$$|Z(G_1)| \geq p$$

Corr

An group of order p^2 is abelian.

By prev. prop.ⁿ we have $|Z(G_1)| \geq p$

WTS $|Z(G_1)| = p^2$

Let $|Z(G_1)| = p$ & $x \in G_1 \setminus Z(G_1)$

$$Z(G_1) \subsetneq C(x)$$

$$|C(x)| = p^2$$

$$\text{as } x \in G_1 \setminus Z(G_1)$$

$$\therefore C(x) = G_1$$

which is a contradiction

~~$\therefore |C(x)| = p^2$~~

$$\therefore Z(G_1) = G_1$$

$\therefore G_1$ is abelian gp.

Corr Any group of order p^2 is isomorphic to

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

↳ check if G has ~~an~~ elt. of order p^2 if not then we are done
else go for 2nd case value of $\phi(x)$ is below

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

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

C/w Assume that \nexists any elt. of order p^2 in G .

\therefore All elts. of order p ~~and hence~~ remaining \Rightarrow $x \in H$

Consider $H = \langle x \rangle$

Let $1 \neq y \in G \setminus H$

Let $K = \langle y \rangle$

Then $|y| = p$ [As its order divides p^2]

$H \cap K = \{1\}$ [But cannot be $p > 1$]

Consider HK [normal subgrps H, K as G abelian]

HK is a subgroup.

$$|HK| = p^2$$

$\therefore G = HK$ ~~but~~ \therefore no relation b/w H, K

Consider $\phi: H \times K \rightarrow HK \cong G$

$$(h, k) \mapsto hk$$

ϕ is a homomorphism

ϕ is an isomorphism ~~as~~ ϕ is bijective

$$\therefore G \cong H \times K$$

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

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

Sylows

Defn Let G_1 be a group of order $p^\alpha m$ where $p \nmid m$, then the subgroup of order p^α is called a Sylow p -subgroup of G_1 . n_p denotes no. of Sylow p -subgroups of G_1 .

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. i.e. 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. $Q \subseteq gPg^{-1}$

if 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

$$15 = 3 \cdot 5$$

$$n_3 \equiv 1 \pmod{3} \quad n_3 | 5 \Rightarrow n_3 = 1$$

$$n_5 \equiv 1 \pmod{5} \quad n_5 | 3 \Rightarrow n_5 = 1$$

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.

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

$$\begin{aligned} G &\cong H \times K \\ &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z} \end{aligned}$$

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

* Characterize the group of order 21

5.2.15

If there is only one sylow p subgroup

of G then $gPg^{-1} = P$, $\forall g \in G$.

Thus P is a normal sgp. of G .

Prop" Let p and q be two distinct primes and $q < p$ and G be a group of order pq . Then

$$\textcircled{1} \quad G \cong \mathbb{Z}/pq\mathbb{Z} \quad \text{if } q \nmid p-1$$

$$\textcircled{2} \quad G \cong \langle x, y \mid |x|=p, |y|=q, yxy^{-1} = x^s \rangle$$

where $s^q \equiv 1 \pmod{p}$, if $q \nmid p-1$

Pf $n_p \equiv 1 \pmod{p}$ and $n_p \mid q \Rightarrow n_p = 1$

$n_q \equiv 1 \pmod{q}$ and $n_q \mid p$

$$\therefore n_{pq} = 1 \cdot p$$

Case 1 $n_p = 1$ $n_q = 1$, $q \nmid p-1$

let P be a sylow-p subgp and Q be

a sylow-q subgroup of G .

$$P = \langle x \rangle \text{ s.t. } |x| = p$$

$$Q = \langle y \rangle \text{ s.t. } |y| = q$$

$P \cap Q = \{1\}$ P & Q both are normal sgps of G

$$|PQ| = pq \rightarrow PQ = G$$

$$P \cong P \times Q = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$$

Case 2 $m_p=1$, $n_q=p$ $q \mid p-1$

Let $P = \langle x \rangle$ st. $|x|=p$.

Let $y \in G$ st. $|y|=q$.

$$yPy^{-1} = P \rightarrow yxy^{-1} \in P.$$

$$yxy^{-1} = x^r \text{ for some } r, 1 \leq r \leq p-1$$

Check if $r=1$, then $yx = xy$

$$\text{In this case } G \cong \mathbb{Z}/pq\mathbb{Z}$$

Let $r \neq 1$.

$$yxy^{-1} = x^r$$

$$y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^ry^{-1} \quad \cancel{\text{---}}$$

$$= yxy^{-1}yxy^{-1}yxy^{-1} \dots \text{r times.}$$

$$= x^{r^2}$$

Similarly we get,

$$y^qxy^{-q} = x^{rq}$$

$$\Rightarrow x = x^{rq}$$

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

$$p \nmid qr+1 \Rightarrow qr \equiv 1 \pmod{p}$$

Ex

Classify group of order 21

$$21 = 3 \cdot 7$$

$$n_3 \equiv 1 \pmod{3} \quad n_3 \mid 7 \Rightarrow n_3 = 7$$

$$n_7 \equiv 1 \pmod{7} \quad n_7 \mid 3 \Rightarrow n_7 = 1$$



Case 2 $n_3 = 7$ $n_7 = 1$

There are 7, 3 sylow sgp of G

There is only 1 sylow 7 sbgp

Let $H = \langle x \rangle$ st $|x| = 7$

Let $y \in G$ st. $|y| = 3$

$$yxy^{-1} \in H$$

$$yxy^{-1} = x^r$$

$$r^3 \equiv 1 \pmod{7}$$

$$\Rightarrow r = 1, 2, 4.$$

$$\text{If } r=2 \quad yxy^{-1} = x^2$$

$$G \cong \langle x, y \mid |x|=7, |y|=3, yxy^{-1} = x^2 \rangle$$

$$\text{If } r=4 \quad yxy^{-1} = x^4$$

$$yxy^{-1} = x^2$$

$$y^2xy^{-2} = x^4$$

Since y and y^2 have the same order which is 3 so we are back to prev case

Ex. Let p be an odd prime and G be a group of order $2p$. Then either $G \cong \mathbb{Z}/2p\mathbb{Z}$ or $G \cong D_p$.

[EoC]

7.2.19 (Absent: Notes from Himanshu)

Groups of order 12.

There are 5 classes of group of order 12.

$$\textcircled{1} \quad \mathbb{Z}/12\mathbb{Z}$$

$$\textcircled{2} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

$$\textcircled{3} \quad A_4$$

$$\textcircled{4} \quad D_6 = \langle x, y \mid x^6 = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

$$\textcircled{5} \quad G_1 = \langle xy \mid x^4 = 1, y^3 = 1, xy = y^2x \rangle$$

$$\text{Pf} \quad 12 = 2^2 \cdot 3$$

$$n_3 \equiv 1 \pmod{3} \times n_3 \mid 4 \Rightarrow n_3 = 1, 4$$

$$n_2 \equiv 1 \pmod{2} \times n_2 \mid 3 \Rightarrow n_2 = 1, 3$$

Let H is a Sylow 2-subgp $\mathbb{Z}/4\mathbb{Z}$ cyclic.

$$\therefore |H| = 4 \text{. Then } H$$

$$\begin{aligned} & \nearrow \mathbb{Z}/4\mathbb{Z} \\ & \nearrow V_4 \\ & \langle x, y \mid x^2 = 1, y^2 = 1, xy = yx \rangle \\ & \hookrightarrow \text{ klein group} \end{aligned}$$

Let K be a Sylow 3 subgp.

$\Rightarrow K$ is a cyclic gp of order 3.

$$H \cap K = \{1\} \text{ and } |HK| = 12 \Rightarrow G = HK.$$

Lemma. Either H or K is a normal subgp of G .

Pf. Let K be a Sylow 3 subgp which is not normal.

$$\Rightarrow n_3 = 4$$

Any 2 sylow 3 subgp. intersect only at identity.

Therefore # of non identity elts in all sylow 3 subgps is 8

Hence there is only 1 Sylow 2 subgp

\therefore That sylow 2 subgp. will be a normal subgp. i.e. $H \triangleleft G$

Case 1. H, K both are normal in G

$$G \cong H \times K / \frac{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}{\mathbb{Z}/12\mathbb{Z}}$$

$$\downarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

(2' of P 5 done)

Case 2. $H \triangleleft G$ and $K \not\triangleleft G$

$\therefore \exists$ 4 Sylow 3 subgps of G say k_1, k_2, k_3, k_4

$$S = \{k_1, k_2, k_3, k_4\}$$

$$G \times S \rightarrow S$$

$$(g, k_i) \mapsto gk_ig^{-1}$$

This gp. action has only 1 orbit.

$$\phi : G \rightarrow S_4$$

$$g \rightarrow \sigma_g, \sigma_g(k_i) = gk_ig^{-1}$$

$$\ker \phi = \{g \in G \mid gk_ig^{-1} = k_i \ \forall i\}$$

$$|O(k_i)| = [G : \text{stb}(k_i)] = \frac{|G|}{|\text{stb}(k_i)|}$$

$$|\text{stb}(k_i)| = 3$$

$$\text{Then } k_i \subseteq \text{stb}(k_i)$$

$$k_i = \text{stb}(k_i)$$

$$\text{Note } \ker \phi = \bigcap_{i=1}^4 \text{stb}(k_i) = \{1\}$$

$$G \cong \phi(G) < S_4$$

$$\therefore |\phi(G) \cap A_4| \geq 8$$

Order of intersection should divide 12 so 2, 3, 4, 6.

Case 3: $K \trianglelefteq G$ and $H \trianglelefteq G$

$$K = \langle x \rangle \text{ st. } |x| = 3$$

$$\text{either } H = \langle y \rangle \text{ st. } |y| = 4$$

$$\text{or } H = V_4 \rightarrow \text{Klein gp.}$$

Consider $H = \langle y \rangle$

$$\text{if } yxy^{-1} = x \text{ then } G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z} \times 4\mathbb{Z}$$

$$\text{let } yxy^{-1} = x^2 \Rightarrow yx = x^2 y$$

$$G \cong \langle xy \mid |x|=3, |y|=4, yx=x^2y \rangle$$

$$\text{let } K \trianglelefteq G \text{ and } H = V_4 \quad -\{1, v, v, uv \mid v^2=1, u^2=1 \\ uv=vu\}$$

$$uxu^{-1} = x^a \quad vxv^{-1} = x^b$$

where a, b are either 1 or -1

$$uvx(vv)^{-1} = uvxv^{-1}v^{-1} = x^{ab} \text{ (check)}$$

$$ux^b v^{-1}$$

$$ux \cdot x \cdot x \cdots x v^{-1}$$

$$= uxu^{-1} x v^{-1} v \cdots uxu^{-1} \cancel{v^{-1}}$$

If $a = b = 1 \Rightarrow G$ abelian which is a contradiction.

Assume $a=1$ $b=-1$

$$vxv^{-1} = z$$

$$vzv^{-1} = zx^{-1}$$

Let $z = xv$ then $|z|=6$

$$v \notin \langle z \rangle \Rightarrow \cancel{v^i z^j}$$

$$v = z^i - xv^i$$

$$v^2 = x^{2i} v^{2i}$$

$$\begin{cases} = x^{2i} = 1 \\ \text{order 2 elt} \end{cases}$$

$$G \cong \langle v, z \mid z^6 = 1, v^2 = 1, vzv^{-1} = z^{-1} \rangle$$

$$vzv^{-1} = vxv^{-1} = vxv^{-1}$$

$$= vx^{-1} = v^{-1}x^{-1}$$

$$\begin{cases} \text{order 2} \\ v^{-1}x^{-1} = (xv)^{-1} \\ = z^{-1} \end{cases}$$

[EoC]

It is clear that $v^2 = 1$ since $v^{-1} = v$

Now we have $vzv^{-1} = z^{-1}$ and $v^2 = 1$.
We can multiply both sides by v to get $zv^{-1} = z^{-1}$.

Since $v^{-1} = v$, we have $zv = z^{-1}$.
Multiplying both sides by v again, we get $z = z^{-1}$.

Thus $z^2 = 1$, which contradicts the fact that $|z| = 6$.

11.2.19.

Fundamental theorem of f.g. abelian group.

Def" for each $r \in \mathbb{N}$, $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ be the direct product of r copies of the group \mathbb{Z} , where $\mathbb{Z}^0 = 1$. The group \mathbb{Z}^r is called the free abelian group of rank r .

Thm: Let G be a finitely generated abelian group. Then

Let G be a finitely generated abelian group. Then

$$(1) G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_s}.$$

For some integers r, n_1, n_2, \dots, n_s .

satisfying the following conditions

(a) $r \geq 0$ and $n_j \geq 2 \quad \forall j$ and

(b) $n_{i+1} \mid n_i \quad \forall i \leq s-1$

(2) The expression in (1) unique ie

$$\text{if } G \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$$

where t, m_1, \dots, m_k satisfies the

conditions (a) and (b) then $t=r, u=s$

and $m_i = n_i$ for all i

The int r is called the free rank of G and

the int n_1, n_2, \dots, n_k are called the invariant factor of G and this expression is

called the invariant factor decomposition of G .

If $r=0$ then G is a finite abelian group

Ex

$$n = 180$$

Let p be prime no. which divides n , and any $p \mid n_i$ for some i . Then $p \mid n_j$ for all $j \leq i$. It follows that every prime divisor of n must divide the first invariant factor n_1 .

$$180 = 2^2 3^2 5$$

By the above observation.

$$2 \cdot 3 \cdot 5 \mid n_1$$

So the possible values of n_1 are

$$n_1 = 2^2 3^2 5, \quad 2^2 3 5, \quad 2^3 5, \quad 2 3 5$$

Now if $n_1 = 2^2 3^2 5$

$$n_1 = 2^2 3 5$$

$$n_2 = 3$$

$$n_1 = 2^3 5$$

$$n_2 = 2$$

$$n_1 = 2 3 5$$

$$n_2 = 6$$

$$[n_2 \neq 2 \text{ or } 3]$$

Invariant factor groups

$$2^2 3^2 5$$

$$\mathbb{Z}_{180}$$

$$2^2 3 5, 3$$

$$\mathbb{Z}_{60} \times \mathbb{Z}_3$$

$$2^3 5, 2$$

$$\mathbb{Z}_{90} \times \mathbb{Z}_2$$

$$2 3 5, 1, 6$$

$$\mathbb{Z}_{30} \times \mathbb{Z}_6$$

Cor. If n is the product of distinct primes
then upto isomorphism only one abelian gp
of order n is there, ie cyclic gp of order n .

\mathbb{Z}_n

Thm

Let G_1 be an abelian group of order $n > 1$

and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ then

$$(1) G_1 \cong A_1 \times \dots \times A_k$$

$$\text{where } (A_i) = p_i^{\alpha_i}$$

$$(2) \text{For each } A = \{A_1, \dots, A_k\}$$

$$|A| = p^\alpha$$

$$A \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

$$p_1 \geq p_2 \geq p_3 \dots \geq p_k$$

$$p_1 + p_2 + \dots + p_k = \alpha.$$

(3) The decomposition in (1) and (2) is unique

If $G_1 \cong B_1 \times B_2 \times \dots \times B_m$
with $|B_i| = p_i^{\alpha_i}$ Then $B_i \cong A_i$

and B_i and A_i have same invariant factors.

Definition

The integers p^{β_i} are called elementary divisors of G . This is called elementary divisor decomposition of G .

Remark:

The subgroups A_i are actually the Sylow p_i subgroups of G . Since G is abelian, so every Sylow p_i subgroup is normal. Thus 3 unique Sylow p_i subgroup of G .

Example $n = 1800 = 2^3 3^2 5^2$

Order of p^β

$$2^3$$

$$3^2$$

$$5^2$$

partition of β

$$3 - 2+1 \quad 1+1+1 \quad \mathbb{Z}_8 \quad \mathbb{Z}_4 \times \mathbb{Z}_1$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$2 \quad 1+1 \quad \mathbb{Z}_2 \quad \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$2 \quad 1+1$$

$$\mathbb{Z}_{25} \quad \mathbb{Z}_5 \times \mathbb{Z}_5$$

Total 12 non isomorphic abelian gp of

order 1800, $\mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

Obtaining elementary divisors from invariant factor decomposition.

Propⁿ $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $(m, n) = 1$.

If $n = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

Let G_1 be an abelian group of type (m_1, \dots, m_s) .

(m_1, \dots, m_s) i.e. $G_1 \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s}$.

For each $m_i = p_1^{\beta_{i1}} \times \dots \times p_k^{\beta_{ik}}$ where $\beta_{ij} \geq 0$

Then by above propⁿ

$$\mathbb{Z}_{m_i} \cong \mathbb{Z}_{p_1^{\beta_{i1}}} \times \dots \times \mathbb{Z}_{p_k^{\beta_{ik}}}$$

Ex Let G_1 be a gp of type $(30, 30, 2)$.
Write down elementary factor decomposition of G_1 .

12.2.19

Ex G_1 is an abelian group of type $(30, 30, 2)$.

Then write down the elementary divisor decomposition of G_1 .

Obtain invariant factors from elementary divisors:

Suppose elementary divisors of G_1 given as

$$2, 3, 2, 25, 3, 2.$$

~~$G_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots \times \mathbb{Z}_7$~~

$$G_1 \cong 0\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_2$$

$p=2$	$p=3$	$p=5$
2	3	
2	3	1
2	1	1

$$n_1 = 2 \times 3 \times 25$$

$$n_2 = 2 \times 3$$

$$n_3 = 2$$

$$G_1 \cong \mathbb{Z}_{150} \times \mathbb{Z}_6 \times \mathbb{Z}_2$$

$$\text{Ex } \mathbb{Z}_6 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{10} \times \mathbb{Z}_9 ?$$

$\mathbb{Z}_6 \times \mathbb{Z}_{15}$ elementary divisors are 2, 3, 3, 5

ans: Isomorphic b.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_{10} \times \mathbb{Z}_9 \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \underline{\mathbb{Z}_9}$$

The two groups are not isomorphic.



Thm [Fixed pt congruence]

Let G be a finite p-group acting on a finite set

$$X. \text{ Then } |X| \equiv |\text{fixed pt}| \pmod{p}$$

Fixed pts: $x \in X$ is a fixed pt if
 $gx = x \quad \forall g \in G$ $\begin{bmatrix} G \times X \rightarrow X \\ (g, x) \mapsto gx \end{bmatrix}$

Pf: Let x_1, x_2, \dots, x_t be different orbits.

$$|X| = |O(x_1)| + |O(x_2)| + \dots + |O(x_t)|$$

~~= no. of orbits~~

Order of orbit is either 1 or p^α

Ex.

let G be a finite p gp. Any subgroup of G with index p is a normal subgroup.

Pf: Let H be a subgroup of G with index p .

Consider the gp. action

$$G \times G/H \rightarrow G/H$$

$$(g, hH) \mapsto ghH$$

The permutation representation

$$\phi: G \rightarrow S_p$$

$$\phi(g) = \sigma_g$$

$$\sigma_g (hH) \mapsto ghH$$

Claim $\ker \phi = H$

let $g \in K$ then σ_g is identity map.

$$\text{ie } \sigma_g(H) = H$$

$$gH = H$$

$$\Rightarrow g \in H$$

$$K \subseteq H$$

W.T.S : $[G : K] \neq p$

$G/K \cong$ subgp of S_p

$$\Rightarrow [G : K] \mid p!$$

$\therefore [G : K] = 1$ or p [$\because [G : K]$ is a power of p]

Since $[G : H] \neq p$

$$\Rightarrow [G : K] \neq 1$$

$$\Rightarrow [G : K] = p \Rightarrow [H : K] = 1 \quad H = K \quad \square$$

Ex Let G be finite gp with $|G| > 1$. p be the smallest prime factor of $|G|$ any subgp. of G with index p is a normal subgp.

Tutorial

Prop Let $H \triangleleft G$ and $\sigma_g : H \rightarrow H$
 $g, h \in G \quad \sigma_g(h) = ghg^{-1}$

$G/\langle \sigma_g(H) \rangle \cong$ subgp of $\text{Aut}(H)$
↳ centraliser

Pf: Let $\phi : G \rightarrow S_{|H|}$

$$\phi(g) = \sigma_g \quad \sigma_g : H \rightarrow H \quad \sigma_g(h) = ghg^{-1}$$

Note: $\text{Im}(\phi) \subseteq \text{Aut}(H)$

$\ker \phi = \{g \in G \mid \sigma_g = \text{Id}\} = G_G(H)$, follows.

Q8

$$|Sp| = p! = p(p-1)!$$

$n_p = \# \text{ of Sylow } p \text{ subgp.}$

$$n_p \mid (p-1)! \quad \text{and} \quad n_p \equiv 1 \pmod{p}$$

A Sylow p subgp will have order p .

An elt. of order p in Sp is a p -cycle.

The no. of p -cycles in $Sp = (p-1)!$

Each p Sylow p subgp. contains $p-1$ ~~elts~~ of order p and any 2 Sylow p subgps intersect at identity.

The total no. of Sylow p -subgroups.

$$n_p = \frac{(p-1)!}{p-1} = (p-2)!$$

$$(p-2)! \equiv 1 \pmod{p}$$

$$(p-1)! \equiv p-1 \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p}$$

Q4 Let G_1 be a gp with 3 conjugacy classes.

$$\cdot |G| = 1+x+y$$

$x \mid |G|$ and $y \nmid |G|$

$$[G] \vdash x = 1+y$$

~~Since~~ Since $x \mid |G| \Rightarrow x \mid 1+y$

$$y \mid 1+x$$

$$x \leq 1+y \leq 2+x$$

$$y = 1+x$$

$$\Rightarrow y \leq x+1$$

$$x, y = p_m^2 - 1$$

$$y = x, x-1, x+1$$

Def A gp. G_1 is called a simple group if the only normal subgroups of G are either the identity or the whole group.

Q11 Show group of order 30 is not simple.

$$30 = 5 \cdot 3 \cdot 2$$

$$\text{By } n_5 \equiv 1 \pmod{5} \Rightarrow n_5 \mid 6 \Rightarrow n_5 = 1, 6$$

$$n_3 \equiv 1 \pmod{3} \Rightarrow n_3 \mid 10 \Rightarrow n_3 = 1, 10$$

$$n_2 \equiv 1 \pmod{2} \Rightarrow n_2 \mid 15 \Rightarrow n_2 = 1, 3, 5, 15$$

$$\text{Let } n_5 = 6, n_3 = 10$$

There will be total $4 \times 6 = 24$ elts of order 5

There will be total $2 \times 10 = 20$ elts of order 3.