

# **Undergraduate Algebra**

**MT2213**

Anupam Singh

Spring 2021

## **Contents**

<b>1</b>	<b>Pre Midsem</b>	<b>2</b>
1.1	Notes 1 . . . . .	2
1.2	Notes 2 . . . . .	2
1.3	Notes 3 . . . . .	2
1.4	Notes 4 . . . . .	2
1.5	Notes 5 . . . . .	2
1.6	Notes 6 . . . . .	2
<b>2</b>	<b>Post Midsem</b>	<b>153</b>
2.1	Notes 7 . . . . .	153
2.2	Notes 8 . . . . .	153
2.3	Notes 9 . . . . .	153
2.4	Presentation . . . . .	153

# **1 Pre Midsem**

**1.1 Notes 1**

**1.2 Notes 2**

**1.3 Notes 3**

**1.4 Notes 4**

**1.5 Notes 5**

**1.6 Notes 6**

MT 2213

08/02/2021

## Undergraduate Algebra I

We are going to cover  
group theory.

### Definition (Group)

A <sup>non-empty</sup> set  $G$  together with a binary operation  $*$  is said to be a group if it satisfies the following axioms

① the binary operation  $*$  is associative.

$$\boxed{\begin{array}{l} * : G \times G \rightarrow G \\ (a, b) \mapsto a * b := * (a, b) \end{array}}$$

Binary operation

for any  $a, b, c \in G$

$$(a * b) * c = a * (b * c)$$

(2) There exist an element  $e \in G$   
with the property

$$e * a = a = a * e$$

$$\forall a \in G$$

(3) For any element  $a \in G$  there  
exist  $\alpha \in G$  s.t.

$$a * \alpha = e = \alpha * a$$


---

\* The set  $G$  with operation  $*$ , that  
is  $(G, *)$  is called a group.

\* The element  $e \in G$  is unique and it's called the identity.

Two such elements  $e_1, e_2$

$$\rightarrow e_1 * a = a = a * e_1 \quad \forall a$$
$$e_2 * a = a = a * e_2$$

$$e_1 * e_2 = e_2 = e_1$$

\* Given  $a \in G$  there exist

$x \in G$

$$a * x = e = x * a$$

This  $x$  is unique and is called inverse of  $a$ , will be denoted as  $a^{-1}$ .

$x_1, x_2$  satisfying this equation.

Show that  $\alpha_1 = \alpha_2$ .

$$\begin{aligned}\alpha_1 &= c * \alpha_1 = (\alpha_2 * a) * \alpha_1 \\&= \alpha_2 * (a * \alpha_1) \\&= \alpha_2 * c \\&= \alpha_2\end{aligned}$$

---

When we define an object using axioms, we should have several non-trivial examples.

### Examples

① Trivial example.

$$G = \{c\}$$

$$c * c = c$$

②  $G = \mathbb{Z}$

$$*: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(a, b) \mapsto a+b$$

$(G, *) = (\mathbb{Z}, +)$  is a

group.

$$\text{identity} = 0$$

$$\text{inverse of } a = -a$$

③  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$   
groups.

④ Matrices

$$G = \left\{ A \in M_n(\mathbb{C}) \mid \det A \neq 0 \right\}$$
$$=: GL_n(\mathbb{C})$$

\* matrix multiplication.

$GL_n(\mathbb{C})$  with matrix mult.  
is a group.

Ex:  $(M_n(\mathbb{C}), +)$  is a group

Ex  $F$  is a field

$(M_n(F), +)$  is a group

$(GL_n(F), \cdot_{\text{matr}})$  is a group  
matrix mult.

Question  $M_n(F)$  with matrix  
mult. Is this a group?

/ 09/02/21

Example

$$\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$$

$(\mathbb{Q}^{\times}, \cdot)$  is a group.

$(\mathbb{Q}, \cdot)$  is not a group.

$(\mathbb{R}^{\times}, \cdot)$ ,  $(\mathbb{C}^{\times}, \cdot)$  are examples of groups.

Example

Symmetric group

$$X = \{1, 2, 3, \dots, n\}$$

$$S_n = \{f : X \rightarrow X \mid f \text{ one-one and onto}\}$$

Binary operation = composition  
of maps.

Then,  $(S_n, \circ)$  is a group.

$I : x \mapsto x \quad \forall x \in X \quad$  Identity

$n=1$   $S_1 = \{(1 \rightarrow 1)\}$  Trivial group

$n=2$   $S_2 = \left\{ \begin{array}{l} \left( \begin{smallmatrix} 1 & \rightarrow \\ 2 & \rightarrow \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & \rightarrow \\ 2 & \rightarrow \end{smallmatrix} \right) \\ \text{c''} \qquad \qquad \qquad \pi \end{array} \right\}$

$$e + e = e \quad e + \pi = \pi = \pi + e$$

$$\pi + \pi = e$$

$n=3$   $S_3 = 6$  elements

In general,  $S_n$  has  $n!$  elements.

$$\begin{array}{rcl} 1 & \rightarrow & 1 \\ 2 & \rightarrow & 2 \\ 3 & \rightarrow & 3 \end{array} \quad (1)(2)(3)$$

$$\begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 1 \\ 3 \rightarrow 3 \end{cases} \quad (1\ 2)\ (3)$$

$$\begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 3 \\ 3 \rightarrow 1 \end{cases} \quad (1\ 2\ 3)$$

New way of  
writing an element of  
the symmetric group  
"cycle" notation

$$S_3 = \left\{ (1)(2)(3), (1^x)(2^y)(3), (1^x)(3^y)(2), (1)(2^y), (1^x)(2^y), (1^x)(3^y) \right\}$$

$$\begin{aligned} \pi * \gamma &= (1^x)(2^y)(3) \circ (1^x)(3^y)(2) & f \circ g(a) \\ &= (1\ 3\ 2) & = f(g(a)) \end{aligned}$$

Definition       $x, y \in G$  we say  
 $x$  and  $y$  commute if  $x * y = y * x$ .

Def. (Abelian group)  
commutative group  
 $G$  is said to be commutative if  
any two element of  $G$  commute.  
i.e.,  $x * y = y * x \quad \forall x, y \in G$ .

Example of Abelian group:

$$(\mathbb{R}, +), (\mathbb{R}^*, \cdot)$$

Example of non-Abelian group-

$GL_n(\mathbb{C})$  is non-Abelian.  
 $n \geq 2$

Exercise find two elements in

$\text{GL}_n(\mathbb{C})$ ,  $n \geq 2$  which do not commute.

Example.  $S_1$  is commutative/Abelian  
 $S_2$  is Abelian

$S_3$  is not Abelian.

$$(13)(2) \circ \overset{\checkmark}{(11)(23)} = (132)$$

$$(11)(23) \circ (13)(2) = \overset{+}{(123)}$$

#  $S_n$  for  $n \geq 3$  is not Abelian.

#  $(13)\begin{smallmatrix} 1 \\ 2 \end{smallmatrix} \equiv \begin{smallmatrix} 1 \\ 3 \end{smallmatrix} \in S_3$

$$S_3 = \left\{ e | 1, (12), (23), (13), (123), (132) \right\}$$

Exercise Practice all of the above for  $n=4, 5$ .

Write down all possible elements in cycle notation. Practice mult. list.

---

$$S_4$$

$$(123)$$

$$(234)$$

---

Example:

$$\mathbb{Z} / n\mathbb{Z}$$

fix  $n \geq 2$

$$\mathbb{Z} = \{ 0, \pm 1, \pm 2, \dots \}$$

$$\mathbb{Z} / n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1} \}$$

$$x \in \mathbb{Z} \quad x = nq + r \quad 0 \leq r < n-1$$

Def.  $\bar{x} \equiv \overline{\underline{x}}$

$$\begin{matrix} & & n \\ & \circ & \end{matrix}$$

$$\begin{matrix} n-1 & & 1 & n+1 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ & & 2 & n+2 \end{matrix}$$

$$\mathbb{Z}/n\mathbb{Z} \ni \bar{x}, \bar{y}$$

$$\bar{x} \oplus \bar{y} := \overline{x+y}$$

check: this is well defined.

$$\bar{x} \odot \bar{y} := \overline{xy}$$

$(\mathbb{Z}/n\mathbb{Z}, \oplus)$  is a group.

$(\mathbb{Z}/n\mathbb{Z}, \circ)$  is not a grp.

$(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \circ)$  ~~may~~ not be  
a group.

When  $n$  is a prime this will  
turn out to be a grp.

---

Another way of thinking about

$\mathbb{Z}/n\mathbb{Z}$  : Given  $n$ .  
On  $\mathbb{Z}$ , we define a relation  
 $x \sim y$  if  $n|x-y$ .

Chin.  $x \sim y$  is an equivalence relation on  $\mathbb{Z}$ .

- reflexive  $x \sim x$
- symmetric  $x \sim y \Rightarrow y \sim x$
- Transitive  $x \sim y, y \sim z \Rightarrow x \sim z$

$$n|x-y, n|y-z \Rightarrow n|z-x$$

We can partition  $\mathbb{Z}$  in equivalence classes.

$$[x] = \{ y \mid y \sim x \}$$

$$[0] = \{ 0, \pm n, \pm 2n, \dots \} = \overline{0}$$

$$[1] = \{ 1, n+1, 2n+1, \dots \} = \overline{1}$$

$$\vdots$$

$$[n-1]$$

$\mathbb{Z}/n\mathbb{Z}$  := set of  $\text{tex}$  equivalence  
classes.

$$= \{ [0], [1], \dots, [n-1] \}$$

$\uparrow$              $\uparrow$              $\uparrow$   
 $\overline{0}$          $\overline{1}$          $\overline{n-1}$

---

$$[0] = [n]$$

---

11 Feb 2021

We have defined a group.

$(G, *)$      $\begin{cases} \rightarrow G \text{ a set} \\ \rightarrow \text{an operation on } G \\ \rightarrow \text{and some properties.} \end{cases}$

" $G$  is a group"     $g_1 * g_2 = g_1 g_2$

---

Def: (Group homomorphism)

$(G_1, *)$  and  $(G_2, \cdot)$

A map  $f: G_1 \rightarrow G_2$  is said to be a group homomorphism if

$$f(g * h) = f(g) \cdot f(h)$$

$\forall g, h \in G_1$ .

Def. (Isomorphism)

$(G_1, *)$ ,  $(G_2, \cdot)$

Then, we say  $G_1$  and  $G_2$  are isomorphic if  $\exists$  a group homomorphism

$\varphi: (G_1, *) \rightarrow (G_2, \cdot)$

which is also one-one and onto.

Def. an isomorphism of a group  $G$  on itself is called automorphism.

---

## Properties.

$f: G_1 \rightarrow G_2$  groups homomorphi-

then,

$$(i) \quad f(e_1) = e_2$$

$$(ii) \quad f(g^{-1}) = f(g)^{-1}.$$

## Proof:

Some practice exercises.

Use the axioms of group to prove the following.

$G$  a group, then

$$\textcircled{1} \quad a \in G \quad \text{then} \quad (a^{-1})^{-1} = a.$$

$$\textcircled{2} \quad a, b \in G \quad \text{then} \quad (ab)^{-1} = b^{-1}a^{-1}.$$

③  $x, y, a \in G$  then  
 $x a = y a \Rightarrow x = y$   
 $a x = a y \Rightarrow x = y$ .

---

(i) ↙ homom.

$$\begin{aligned} f(e_1) &= f(e_1 + e_1) = f(e_1) \cdot f(e_1) \\ &\Downarrow \\ f(e_1) \cdot e_2 &\Rightarrow f(e_1) = e_2. \end{aligned}$$

(ii)  $g \in G_1$

$$\begin{aligned} e_2 &= f(e_1) = f(g + g^{-1}) \\ &= \underline{\underline{f(g) \cdot f(g^{-1})}} \\ \Rightarrow f(g^{-1}) &\text{ is inverse of } f(g) \\ \Rightarrow f(g)^{-1} &= f(g^{-1}). \end{aligned}$$

Definition:  $G$  a group.

$|G| < \infty$  then we say  $G$  is a finite group.

Otherwise we say  $G$  is infinite.

Def:  $x \in G$

$$x * x =: x^2 \in G$$

$$(x * x) * x = x * x * x =: x^3 \in G$$

⋮

$$x^n := (x^{n-1}) * x = x * x^{n-1} \in G$$

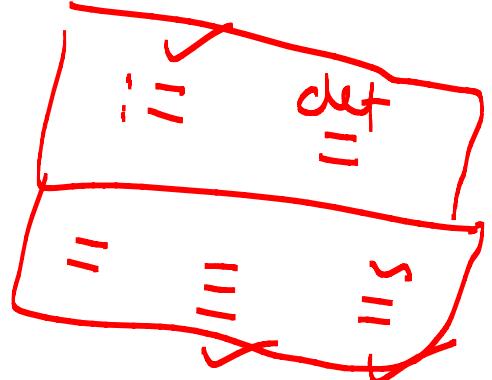
Solution  $x^r = e$

The smallest positive integer  $r$  such that  $x^r = e$  is called order of  $x$ .

Warning: such  $\alpha$  may or may not exist.

If  $\alpha$  exists then we say order of  $\alpha$  is  $n$  and  $\alpha$  has finite order.

If  $\alpha$  doesn't exist we say  $\alpha$  has infinite order.



---

Example:

$$\textcircled{1} \quad (\mathbb{Z} | n\mathbb{Z}, +) \\ = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1} \}$$

$$\text{Identity} = \bar{0}$$

What is the order of  $\bar{1}$ ?

$$\underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_n = \bar{n} = \bar{0}$$

Use Euclid's algorithm to show  $n$  is smallest.

order of  $\bar{1}$  is  $n$ .

order of  $\bar{2}$ ?

Suppose  $n = 4$ ,  $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

order  $\bar{0} = 1$

order  $\bar{1} = 4$

order  $\bar{2} = 2$

order  $\bar{3} = 4$

Example:  $(\mathbb{Z}, +)$

$$\text{order of } 1 = \infty$$

$$\text{order of } n = \infty \text{ if } n \neq 0.$$

---

Proposition:  $G$  a group. Suppose  $G$  is finite. Then, all elements of  $G$  have finite order.

Proof:  $e \neq x \in G$

Suppose  $x$  does not have finite order.

$$\{x, x^2, x^3, \dots\}$$

none of the two elements in  
this set are equal.

Suppose  $x^k = x^l$        $k \neq l$

$$x^k \cdot (x^l)^{-1} = e$$

$$x^{k-l}$$
      contradiction.

$$\{x, x^2, \dots\} \subset G$$

this contradicts that  $G$  is fin.  
=====

---

Def. (subgroup) of a group)

Let  $G$  be a group.

A subset  $H$  of  $G$  is said to  
be a subgroup of  $G$  if it  
it satisfies the following

(i)  $e \in H$

(ii) if  $x, y \in H$  then  $x+y \in H$

(iii) if  $x \in H$  then  $x^{-1} \in H$ .

Exercise  $(G, *)$  a grp.  
 $H$  a subgp

$(H, *)$  is also a grp.

Exercise.  $G$  finit  $\Rightarrow$  all elements have finite order.

Is converse true?

$$\{e^{iq\pi} \mid q \in \mathbb{Q}\}$$

16/2/21

Example  $Q_8$  quaternion group

$$Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$$

multiplication is given as follows.

$\pm 1$  commutes with all elements.

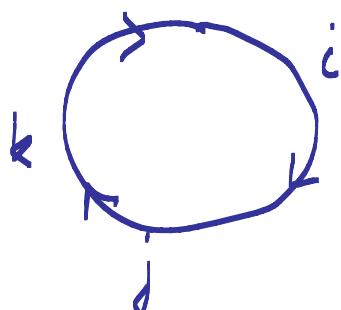
$1$  is the identity.

$$i^2 = -1 = j^2 = k^2$$

$$i j = k = -j i$$

$$j k = i = -k j$$

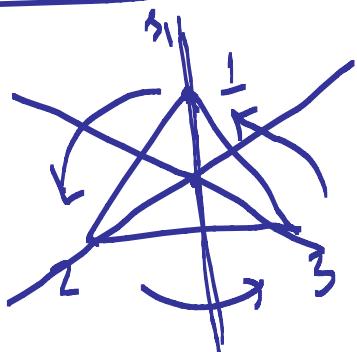
$$k i = j = -i k$$



$Q_8$  is not commutative.

Example

(Dihedral groups)



$r :=$  rotation by  $\frac{2\pi}{3}$   
 $s_1, s_2, s_3$

$$D_6 = \{1, r, r^2, r^3 = 1, s_1, s_2, s_3\}$$

$$r^3 = 1, \quad s_1^2 = s_2^2 = s_3^2$$

$$s := s_1$$

$$rs = s_3$$

$$\begin{matrix} 1 & \rightarrow & 2 \\ 2 & \rightarrow & 1 \\ 3 & \rightarrow & 3 \end{matrix}$$

$$sr = s_2$$

$$\begin{matrix} 1 & \rightarrow & 3 \\ 2 & \rightarrow & 2 \\ 3 & \rightarrow & 1 \end{matrix}$$

$$rs \neq sr$$

$$r^2 s = s_2$$

$$sr^2 = s_3$$

$$D_6 = \{ 1, r, r^2, s, rs, r^2s \}$$

$$r^3 = 1, \quad rs = sr^{-1}$$

$$s^2 = 1$$

$$D_{2n} = \{ 1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s \}$$

$$r^n = 1, \quad s^2 = 1, \quad sr = rs^{-1}$$

Intuition for this group comes  
for geometry and this group is  
important to be isometry of n-gon.

---

Theorem: (Lagrange's Theorem)

Let G be a finite group and

$H$  a subgroup of  $G$ . Then,

$$(H) \quad | \quad (G).$$

---

Question Is correct true?

No. Find a counterexample.

---

$G$  a finite group } Given  
 $H$  a subgroup of  $G$  } to us.

Recall the definition of subgroup.

- ①  $c \in H$  //
- ②  $x, y \in H \Rightarrow xy \in H$  //
- ③  $x \in H \Rightarrow x^{-1} \in H$  //

Steps

(i) Relation , equivalence relation.

(ii) Size of equivalence classes.

$$x, y \in G$$

Define the following relation

$$x \sim y \text{ if } x^{-1}y \in H$$

Claim: This relation is an equivalence relation.

(i) Reflexive :  $x \sim x$

$$x^{-1}x = e \in H$$

(ii) Symmetry  $x \sim y \Rightarrow y \sim x$

$$\begin{aligned}
 x \sim y &\Rightarrow x^{-1}y \in H \\
 &\Rightarrow (x^{-1}y)^{-1} \in H \\
 &\Rightarrow y^{-1}x \in H \\
 &\Rightarrow y \sim x
 \end{aligned}$$

(iii)

Transitive

$$x \sim y, y \sim z \Rightarrow x \sim z$$

$$\begin{aligned}
 x^{-1}y \in H, y^{-1}z \in H \\
 &\Rightarrow x^{-1}y, y^{-1}z \in H \\
 &\Rightarrow x^{-1}z \in H \\
 &\Rightarrow x \sim z
 \end{aligned}$$

We know that the relation  $x \sim y$  defined on  $G$  is an equivalence relation.

This means  $G$  is a disjoint union of equivalence classes.

$$e \in G$$

$$\begin{aligned}[e] &= \{y \in G \mid y \sim e\} \\ &= \{y \in G \mid y^{-1} \in H\} \\ &= H\end{aligned}$$

$$e \neq x \in G$$

$$\begin{aligned}[x] &= \{y \in G \mid x \sim y\} \\ &= \{y \in G \mid x^{-1}y \in H\} \\ &= \{y \in G \mid \underbrace{x^{-1}y = h}_{y = xh} \in H\} \\ &= \{xh \mid h \in H\} \subset G \\ &\equiv xH\end{aligned}$$

Equivalence classes are subsets  
of form  $\underline{xH}$ .

"left cosets of  $G$  by  $H$ "

$$G = \bigcup [x] = \bigcup xH$$

Several properties follow

①  $x_1H, x_2H$  then either

$$x_1H = x_2H \text{ or}$$

$$x_1H \cap x_2H = \emptyset$$

②  $H = \{h\}$

③  $G$  is a disjoint union of  
the left cosets.

Exhibit:  $S_3 = \{ 1, (12), (13), (23), (123), (132) \}$

$$H = \{ 1, (12) \}$$

①  $H$  is a subgroup

② Write down all left cosets.

---

We can also define right cosets  
which are of the form  $Hx$

③ Compute the right cosets also.

---

1	8	2	2
---	---	---	---

Recall left cosets.

---

$G$  a group }  
 $H$  a subgroup }

Use this to define an equivalence relation on  $G$ , for  $x, y \in G$   
 $x \sim y$  if  $x^{-1}y \in H$ .

This is an equivalence relation.

We get equivalence classes.

These classes are called left cosets.

$$[x] = xH = \{xh \mid h \in H\}$$

For example for  $h' \in H$

$$[h'] = h'H = H$$

(check equality here).

$$G/H := \{ [x] = xH \mid x \in G \}$$

↑ set of all left cosets of  $G$  w.r.t  $H$

---

right cosets

$$x \sim y \text{ if } xy^{-1} \in H$$

This is also an equivalence relation  
and we get right cosets as  
equivalence classes.

$$[x] = Hx = \{ hx \mid h \in H \}$$

$$H \setminus G := \{ Hx \mid x \in G \}.$$

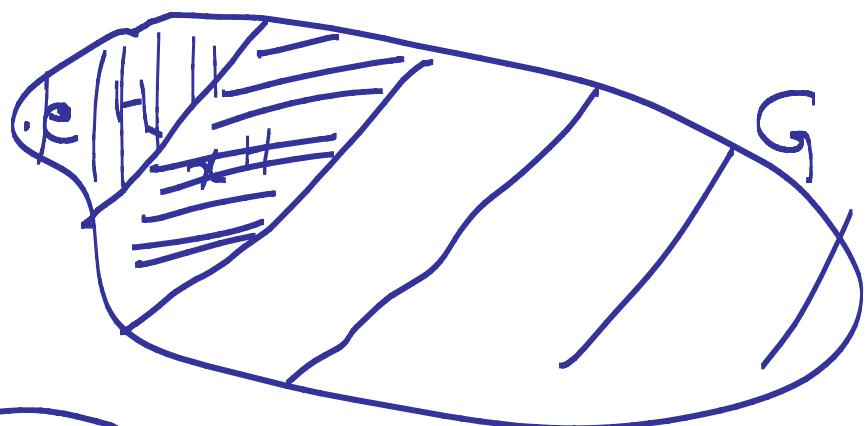
Classification

$$G \setminus H := \left\{ \underbrace{xH}_{\text{a subnt of } G} \mid x \in G \right\}$$

$(x), \bar{x}$

a subnt of  $G$

$$a \setminus G$$



$$G/H$$

$$H/G$$

Example

$$S_3 = \{ \text{id}, (12), (13), (23), (123), (132) \}$$

$$H = \{ \text{id}, (12) \}$$

$$\begin{aligned} S_3 | H &= \left\{ \begin{array}{l} H = \{ \text{id}, (12) \}, (13)H \\ = \{ (13), (123) \} \\ (23)H = \{ (23), (132) \} \end{array} \right\} \end{aligned}$$

$$S_3 / H = \{ H, (13)H, (23)H \}$$

$$H \setminus S_3 = \left\{ \begin{array}{l} H, H(13), H(23) \\ \{ (131), (132) \} \quad \{ (23), (123) \} \end{array} \right\}$$

Example  $G = (\mathbb{Z}, +)$

$$H = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$$

$$\begin{aligned} G/H &= \left\{ \begin{matrix} [0] \\ 3\mathbb{Z} \end{matrix}, \quad \begin{matrix} [1] \\ 1+3\mathbb{Z} \end{matrix}, \quad \begin{matrix} [2] \\ 2+3\mathbb{Z} \end{matrix} \right\} \\ &\quad \left\{ \begin{matrix} 1+3n \\ \{1+3n\} \end{matrix} \quad \begin{matrix} 2+3n \\ \{2+3n\} \end{matrix} \right. \\ &= \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

Warning  $\mathbb{Z}_n$  what we call  $\mathbb{Z}/n\mathbb{Z}$ .

$$H = n\mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} = \left\{ \begin{matrix} n\mathbb{Z} \\ 0 \end{matrix}, \quad \begin{matrix} 1+n\mathbb{Z} \\ 1 \end{matrix}, \quad \dots, \quad \begin{matrix} (n-1)+n\mathbb{Z} \\ n-1 \end{matrix} \end{right\}}$$

The  $+$  operation of  $\mathbb{Z}$  gives

rise to the group operation  $\oplus$   
on  $\mathbb{Z}/n\mathbb{Z}$  which we defined  
earlier.

---

Theorem (Lagrange's theorem)

Let  $G$  be a finite group. Let  
 $H$  be a subgroup of  $G$ . Then,

$$|H| \mid |G|.$$

Proof.

$$G/H = \{ xH \mid x \in G \}$$

set of all left cosets of  $G$   
wrt  $H$ .

Claim:  $|H| = |\pi H|$

$$\varphi: H \longrightarrow xH$$

$$h \mapsto xh$$

$\varphi$  is a set bijection

(i)  $\varphi$  is a well-defined map.

(ii)  $\varphi$  is one-one

$$xh_1 = xh_2 \Rightarrow h_1 = h_2$$

(iii)  $\varphi$  is onto

$$\Rightarrow |H| = |\varphi(H)| \quad \text{for any } x.$$

$$G = \bigcup_{x \in G} xH$$

$$|G| = \sum_{xH \in G/H} |xH|$$

$$= \sum |H|$$

$$zH \in G/H$$

$$= |G/H| \cdot |H|$$

$$|G| = |G/H| \cdot |H|$$

$$\Rightarrow |H| \sqrt{|G|} \cdot =$$

---

$$|G| = |G/H| \cdot |H|$$

Some applications of Lagrange's Th.

Corollary 1:

Let  $G$  be a group with  $p$  elements where  $p$  is a prime. Then, only subgroups of  $G$  are  $\{e\}$ ,  $G$  itself.

Proof. Let  $H$  be a subgroup of  $G$ .  
Lagrange's theorem  $\Rightarrow |H| \mid |G| = p$   
 $\Rightarrow |H| = 1$  or  $p$   
 $\Rightarrow H = \{e\}, H = G.$

In fact we will prove that  
if  $|G| = p$ , then  $G \cong \mathbb{Z}/p\mathbb{Z}$ .

Corollary 2 Let  $G$  be a group.

Let  $x \in G$ . Then, order of  $x$  divides  $|G|$ .

Pruf:  $H = \{1, x, x^2, \dots, x^{r-1}, \dots\}$

If order of  $x$  is  $r$  then

$$|H| = r$$

Check  $H$  is a subgp

$$\begin{aligned} \text{Lagrange's Th.} \Rightarrow |H| &\mid |G| \\ &\Rightarrow r \mid |G|. \end{aligned}$$

Corollary 3 (Fermat's Little Thm)

a positive integer,  $p$  is a prime  
Then,  $a^p \equiv a \pmod{p}$ .

$$\mathbb{P}_{\mathbb{Z}/p\mathbb{Z}} \cdot \mathbb{Z}/p\mathbb{Z} - \{0\} =: \mathbb{Z}/p\mathbb{Z}^*$$

is a group with multiplikat.

$$(x + p\mathbb{Z}) \cdot (y + p\mathbb{Z}) := xy + p\mathbb{Z}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \underline{\underline{a^p \equiv a \pmod{p}}}$$

23 | 02 | 21

## Generators

Recall from linear algebra.

$V$  a vector space,  $S \subset V$

Defined Span of  $S$

Definition:  $G$  a group

$S \subset G$

$\langle S \rangle$  is the smallest subgroup of  $G$  containing  $S$ , called the subgroup generated by  $S$ .

Def:  $S \subset G$  if  $\langle S \rangle = G$

then we say  $S$  generates

$G \ni s$  is a generator of  $G$ .

---

Example :

$$\textcircled{1} \quad \mathbb{Z}_{|n\mathbb{Z}} = \{0, 1, 2, \dots, n-1\}$$

$$S = \{0\}, \langle S \rangle = \{0\}$$

$$S = \{1\}, \langle S \rangle = \mathbb{Z}_{|n\mathbb{Z}}$$

$$S = \{2\} \quad \langle S \rangle = ?$$

$$\mathbb{Z}_{|4\mathbb{Z}}, S = \{2\} \Rightarrow \langle S \rangle = \{0, 2\}$$

Example -

$$S = \{1\} \quad \langle S \rangle = ?$$

$$S = \{1, -1\} \quad \langle S \rangle = \mathbb{Z}$$

$$S = \{2, 4\} \quad \langle S \rangle = 2\mathbb{Z}$$

$$S = \{2, 3\} \quad \langle S \rangle = \mathbb{Z}$$

Example  $Q_8$

$$S = \{i, j\} \quad \langle S \rangle = Q_8$$

---

Practical way of thinking about  
 $\langle S \rangle$ .

Given

$G$  a group

$$S \subset G$$

$$\langle S \rangle = ?$$

$s \in S$

$\langle s \rangle$  is mapped  
to be a subg)

$\Rightarrow s^2 \in \langle s \rangle$

$s^i \in \langle s \rangle, i \in \mathbb{Z}$

$s_1^{i_1} s_2^{i_2} \dots s_k^{i_k} \in \langle s \rangle$

where  $s_1, s_2, \dots \in S$

$i_1, i_2, \dots \in \mathbb{Z}$

$H(S) = \left\{ \underbrace{s_1^{i_1} s_2^{i_2} \dots s_k^{i_k}}_{s_1, \dots \in S, i_1, \dots \in \mathbb{Z}} \mid \right.$

Claim:

$$H(S) = \langle S \rangle$$

Pwf:

$$\langle S \rangle \supset H(S) \rightarrow \text{①} \checkmark$$

- $\mathcal{H}(S)$  is a subgp
- $\mathcal{H}(S) \supset S$  ✓

To prove  $\mathcal{H}(S)$  is a subgp

$$(i) c \in \mathcal{H}(S)$$

$$(ii) x, y \in \mathcal{H}(S) \Rightarrow xy \in \mathcal{H}(S)$$

$$x = s_1^{i_1} \dots s_k^{i_k} \quad y = t_1^{j_1} \dots t_n^{j_n}$$

$$s_1, \dots, t_1, \dots \in S$$

$$\Rightarrow xy = s_1^{i_1} \dots s_k^{i_k} t_1^{j_1} \dots t_n^{j_n} \in \mathcal{H}(S)$$

$$(iii) x \in \mathcal{H}(S) \Rightarrow x^{-1} \in \mathcal{H}(S)$$

$$x = s_1^{i_1} \dots s_k^{i_k}$$

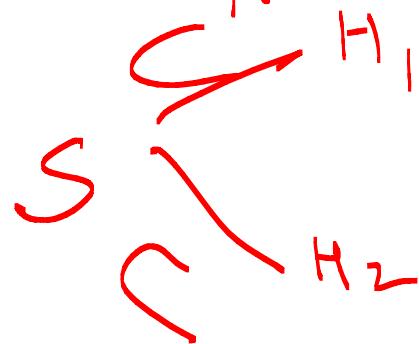
$$x^{-1} = s_k^{-i_k} \dots s_1^{-i_1} \in \mathcal{H}(S)$$

We have  $\mathcal{H}(S)$  is a subgp containing  $S$ .

$$\Rightarrow \langle S \rangle \subset \mathcal{H}(S)$$

→ ②

Ques. Why  $\langle S \rangle$  is a unique subsp.



$$S \subset H_1 \cap H_2$$

Examp.

$\mathbb{Z}$

$$S = \{1\}$$

$$n \in \mathbb{Z} \quad 1 + \underbrace{\dots + \frac{1}{n}}_{n} = n$$

$$S = \{ \text{primes} \} =$$

$$\langle S \rangle = \mathbb{Z}$$

$$\langle \{2, 3\} \rangle$$

$$(2, 3) = 1$$

$$n = r_1 2 + r_2 3$$

Example Gauss elimination:

$$E_{ij}(t) = \begin{cases} 1 & i=j \\ -t & i \neq j \end{cases} \quad i \neq j$$

$$\langle E_{ij}(t) | 1 \leq i \neq j \leq n, t \in \mathbb{R} \rangle$$

$$= \text{SL}_n(\mathbb{R})$$

No concept of lin. indep.?

bin. index is generating in grp  
then to say there are no  
relation.

$$\left. \begin{array}{l} x \in G \quad x^n = 1 \\ x_1^{i_1} x_2^{i_2} \dots x_k^{i_k} = 1 \end{array} \right\}$$

---

---

Def. If a grp is generated  
by 1 elent then it is -  
called a cyclic grp.

Examl  $\mathbb{Z}/n\mathbb{Z}$ ,  $\mathbb{Z}$

Quesn Are these more cyclic  
grps?

## Graph

Cayley graph.

$G$  a grp,  $S \subset G$

$\Gamma(G, S)$  : ① Vertices are elements of  $G$

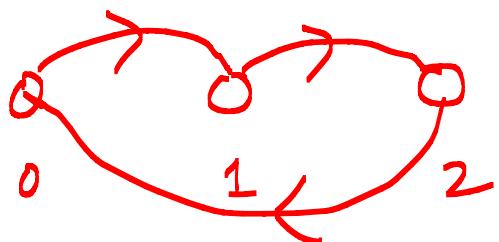
② We make

an edge (directed) between  $x_1$  &  $x_2$  if  $x_1 = x_2 s$  for some  $s \in S$ .

---

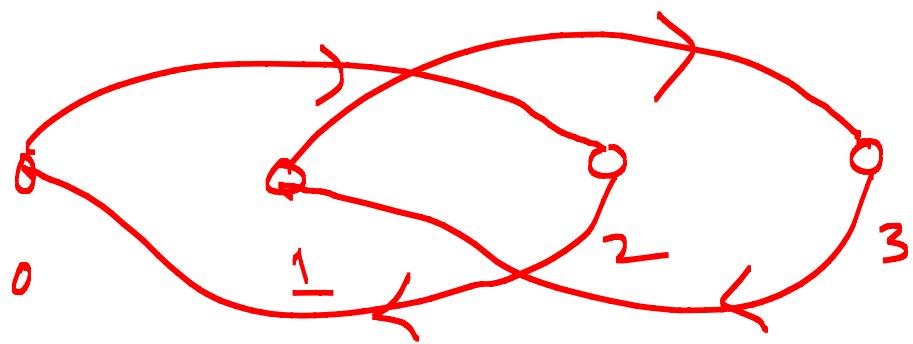
Ex:

$$\mathbb{Z}/3\mathbb{Z} \quad S = \{1\}$$



$24 \mid 4z$ 

$$S = \{2\}$$



Example

$$PSL_2(\mathbb{Z})$$

$$SL_2(\mathbb{Z})$$

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{array}{l} a, b, c, d \in \mathbb{Z} \\ ad - bc = 1 \end{array} \right\}$$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$\mathbb{Z}(SL_2(\mathbb{Z})) = \pm I$$

$$PSL_2(\mathbb{Z}) = \frac{SL_2(\mathbb{Z})}{\mathbb{Z}(SL_2(\mathbb{Z}))}$$

$$\left\langle z_1, z_2 \mid z_1^2 = 1, z_2^3 = 1 \right\rangle$$

$$SL_2(\mathbb{Z}) = \langle \gamma, \delta \rangle$$

$\gamma^4 = 1, \delta^6 = 1$

$$\left\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \right\rangle$$

25 Feb 21

## Normal subgroups

$G$  a group.  $H$  a subgp of  $G$ .  
Then,  $H$  is said to be a normal subgroup of  $G$  if

$$g H g^{-1} \subset H \quad \forall g \in G.$$

---

$$g H g^{-1} = \{ g h g^{-1} \mid h \in H \}$$

In fact,  $g H g^{-1}$  is a subgroup in general.

$$gh_1g^{-1} \cdot gh_2g^{-1} = g \underline{h_1h_2} g^{-1}$$

$$(gh_1g^{-1})^{-1} = (g^{-1})^{-1} h_1^{-1} g^{-1} = g h_1^{-1} g^{-1}$$

Example  $G$  an Abelian group

$H$  a subgroup of  $G$

Then,  $H$  is also normal.

$$gHg^{-1} = \{ ghg^{-1} = hgh^{-1} = h \mid h \in H \} \\ = H$$

Example  $S_3 = \{ 1, (12), (23), (13) \}$

$$(123), (132) \}$$

$$H = \{ 1, (12) \}$$

Is this a normal subgroup?

$$\forall g \in S_3 \quad gHg^{-1} \subseteq H$$

$$g = (23)$$

$$gHg^{-1} = \{ (23)1(23)^{-1}, (23)(12)(23)^{-1} \}$$

$$= \{ 1, (13) \} \not\subset H$$

$H$  is not a normal subgp.

Proposition

$G$  a group

$H$  a subgp of  $G$

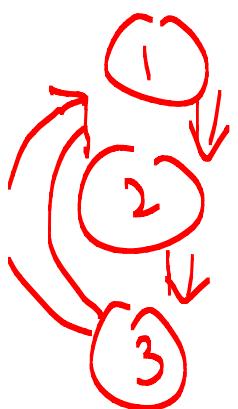
Then, the following are equivalent.

$H$  is a normal subgp  $\Leftrightarrow gHg^{-1} \subset H \forall g \in G$ .

$gH = Hg \quad \forall g \in G$

$gHg^{-1} = H \quad \forall g \in G$ .

Proof: (1)  $\Rightarrow$  (2)      (2)  $\Rightarrow$  (3)      (3)  $\Rightarrow$  (1)



$\textcircled{1} \Rightarrow \textcircled{2}$  Given  $H$  is normal  
i.e.  $gHg^{-1} \subset H \quad \forall g \in G.$

To show :  $\underline{\underline{g \in G}}, \quad gH = Hg ?$

$$\begin{aligned} gH &= gH \cdot e = \underline{\underline{gHg^{-1}}}g \subset Hg, \\ Hg &= \underline{\underline{gg^{-1}}}Hg \subset g \cdot H \\ &\Rightarrow gH = Hg. \end{aligned}$$

$\textcircled{2} \Rightarrow \textcircled{3}$

Given :  $gH = Hg \quad \forall g \in G.$

To show  $xHx^{-1} = H \quad \forall x \in G.$

$$x\underline{\underline{Hx^{-1}}} = x \cdot x^{-1}H = H$$

③  $\Rightarrow$  ①

Given  $gHg^{-1} = H \forall g \in G$

To prove

$$gHg^{-1} \subset H \forall g \in G.$$



---

$$\begin{array}{ccc} A = B & & \\ a \in A \Rightarrow a \in B & & A \subset B \\ G \subset B \Rightarrow G \subset A & & B \subset A \end{array}$$

---

Why normal subgroups  
are important?

$G$  a group  
 $H$  a subgroup of  $G$

$$G/H = \{ xH \mid x \in G \}$$

if  $G$  is finite,  $H$  finite  
 $\Rightarrow |G/H| = \frac{|G|}{|H|}$ .

This is also called index  
of  $H$  in  $G$ ,  $[G : H] := \frac{|G|}{|H|}$

$$\begin{matrix} G \\ \downarrow \\ H \end{matrix}$$

---

$$G/H = \{ xH \mid x \in G \}$$

Can we make this into a group?

$$x_1 H \cdot x_2 H = x_1 x_2 H$$

Suppose we take this as  
a definite of multiplication, does  
this make  $S_3/H$  a group.

Example.  $S_3$ ,  $H = \{1, (12)\}$

$$(13)H = \{(13), (13)(12) = (123)\}$$

$$(23)H = \{(23), (23)(12) = (132)\}$$

$$S_3/H = \{H, (13)H, (23)H\}$$

$$(13)H \cdot (23)H = ?$$

$$\{(13), (123)\} \cdot \{(23), (132)\}$$

$$= \{ (13)(25), (13)(152), (123)(23), \\ (123)(152) \}$$

$$= \{ (132), (1)(23), (12), 1 \}$$

$\notin$  any of the 3 cont.

Proposition

$G$  a group  
 $H$  a subgroup

Then,

$G/H$  is a group with multiplication defined using that of  $G$

$\Leftrightarrow H$  is a normal subgroup.

Proof:

( $\Rightarrow$ ) Given  $G/H$  is a group  
with  $g_1H \cdot g_2H = g_1g_2H \forall g_1, g_2 \in G$

To show :  $gHg^{-1} = H \quad \forall g \in G$

$$\underbrace{g_1H \cdot g_2H}_{\text{L}} = g_1g_2H \in \underbrace{g_1g_2H}_{\text{R}}$$

Take  $g_1 = h, g_2 = h^{-1}$

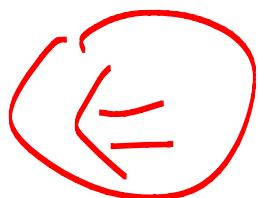
$$\Rightarrow hHh^{-1} = H \rightarrow \begin{cases} g_1 = h \\ g_2 = h^{-1} \end{cases}$$

Taken  $xHx^{-1} = H \quad \forall x \in G$

$$\Rightarrow xHx^{-1} = x \cdot x^{-1}H = H$$

$$\underbrace{g_1h \cdot g_2h^{-1}}_{\text{L}} = \underbrace{g_1g_2h}_{\text{R}}$$

$$\Rightarrow \underbrace{g_1 \underline{h} g_2}_{} = \underbrace{g_1 g_2 h h_2^{-1}}_{=} = \underline{g_1 g_2 h_3}$$



Given  $H$  is norm.

To show  $G/H$  is a grp

$$\underline{x_1 H} \cdot \underline{x_2 H} = \underline{\underline{x_1 x_2 H}}$$

$$\begin{aligned} \underline{x_1 h_1} \cdot \underline{x_2 h_2} &= \underline{\underline{x_1 x_2 x_2^{-1}}} \cdot \underline{h_1 x_2 h_2} \\ &= \underline{x_1 x_2} \cdot \underline{\underline{(x_2^{-1} h_1' x_2) h_2}} \end{aligned}$$

But we complete the proof.

$$g_1 H \cdot g_2 H = g_1 g_2 H$$

$$\text{Identity? } H = eH$$

$$\cdot (gH)^{-1} = g^{-1}H$$

---

---

Quotient group

$G$  a grp  
 $N$  a normal subgrp

$$G/N = \{gN \mid g \in G\}$$

$$g_1N \cdot g_2N := g_1g_2N$$

Then,  $G/N$  is a grp.

This is called quotient group  
quotient of  $G$  by  $N$ .

---

---

Example:

$$\mathbb{Z} / H = \mathbb{Z} / n\mathbb{Z}$$

$\mathbb{Z} / H = \left( \mathbb{Z} / n\mathbb{Z} \right) \text{ def}$

↑  
construction by quot'it.

---

$$G/H = \overbrace{\{ xH \mid x \in G \}}$$

↙  
H

$$\underline{\underline{xH}} \cdot \underline{\underline{xH}} = \underline{\underline{x}} H = xH$$

---

$$\underline{\underline{gH}} = H \underline{\underline{g}}_x = \underline{\underline{gh}} H = gH$$

02 March 2021

## Groups, examples

Can we produce more examples  
knowing the examples we have?

- ① Subgroups
  - ② Normal subgroups, quotients  
 $N$        $G/N$
  - ③  $\phi : G_1 \rightarrow G_2$  group homomorphism

Then, define

$$\ker \varphi := \{ x \in G_1 \mid \varphi(x) = e \}$$

$\text{Im } \varphi := \text{Image of } \varphi$ .

#  $\ker \varphi$  is a normal subgroup of  $G_1$ .

②  $\text{Im } \varphi$  is a subgroup of  $G_2$ .

Verify ①  $\ker \varphi \subset G_1$

•  $c \in \ker \varphi$

•  $x, y \in \ker \varphi \Rightarrow xy \in \ker \varphi$

$$\varphi(xy) = \varphi(x)\varphi(y) = e \cdot e = e$$

•  $x \in \ker \varphi \Rightarrow x^{-1} \in \ker \varphi$

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

•  $g \in G \quad g \cdot \ker \varphi \cdot g^{-1} \subset \ker \varphi ? \quad \varphi(gng^{-1})$

# Given a group  $G$ ,  $\text{Aut}(G) = \{ \varphi: G \rightarrow G \mid \varphi \text{ isom} \}$   
is a group under composition.

Exercise: Compute  $\text{Aut}(G)$  for  
the examples of  $G$  you know?

#  $\text{Im } \phi$  is a subgp of  $G_2$ .

.  $c \in \text{Im } \phi$   
 $\stackrel{\text{"def."}}{=}$

.  $x, y \in \text{Im } \phi \Rightarrow xy \in \text{Im } \phi$

$x = \phi(g_1) \quad y = \phi(g_2)$

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

$\Rightarrow xy \in \text{Im } \phi$

.  $x \in \text{Im } \phi \Rightarrow x^{-1} \in \text{Im } \phi$

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

---

#  $G$  a group.  $H$  a subgp of  $G$ .

Defintion Normaliser of  $H$  in  $G$

$$N_G(H) := \{x \in G \mid xHx^{-1} \subset H\}$$

Remarks:

①  $H \subset N_G(H) \subset G$

②  $N_G(H)$  is a subgroup

•  $e \in N_G(H)$

•  $x, y \in N_G(H) \Rightarrow xy \in N_G(H)$

$xHx^{-1} \subset H, yHy^{-1} \subset H \checkmark$

$xyH(xy)^{-1} = \underbrace{xyH}_{\in N_G(H)} \underbrace{y^{-1}x^{-1}}$

•  $x \in N_G(H) \subset H \Rightarrow x^{-1} \in N_G(H).$

③ If  $H$  is normal then

$$N_G(H) = G.$$

---

Def: Centraliser of  $H$  in  $G$ .

$$C_G(H) := \{x \in G \mid xhx^{-1} = h \forall h \in H\}$$

$\Downarrow$   
 $xh = hx$

Properties

①  $C_G(H) \subset N_G(H)$

Question: Is it true  $H \subset C_G(H)$ ?

Example  $S_3 = \{1, (12), (13), (23), (123), (132)\}$

$$H = \{1, (123), (132)\}$$
$$N_{S_3}(H) = S_3$$

$(12)H(12)^{-1} = (12)(123)(12)$   
 $= (12)(13) = (12)$   
 $= (132)$

$$C_{S_3}(H) = H.$$

---

$$\therefore H = S_3$$

$$C_{S_3}(H) = 1$$

Def. Center of a group.

$$\begin{aligned} Z(G) &:= \{x \in G \mid xg = gx \forall g \in G\} \\ &= C_G(G). \end{aligned}$$


---

Example:

$$S_4 \quad H = \{1, (12)\}$$

$(12)$

$$C_{S_4}(H) = ?$$

$$(34) \in C_{S_4}(H)$$

$$(12)(34) = (34)(12)$$


---

Def:  $x \in G$

$$Z_G(x) := C_G(\langle x \rangle)$$

$$= \{ g \in G \mid g x = x g \}$$

$$x \in Z_G(x) \rightarrow \text{Subgroup of } G.$$

## # Direct Product

$G_1$  and  $G_2$  are groups.

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

$$(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$$

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 h_1, g_2 h_2)$$

Then,  $G_1 \times G_2$  is a group.

Example:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \neq \mathbb{Z}/4\mathbb{Z}$$

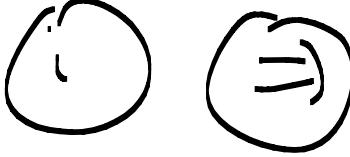
all elements have  
order 2

has an  
element of  
order 4.

What is the rule of  $\ker \phi$  &  $\text{Im } \phi$ ?

i)  $\ker \phi = e \Leftrightarrow \phi$  is injective.

ii)  $\text{Im } \phi = G_2 \Leftrightarrow \phi$  is surjective.

Pruf:  Given  $\ker \varphi = e$

To show  $\varphi(x_1) = \varphi(x_2) \Rightarrow x_1 = x_2$   
 $\forall x_1, x_2 \in G_L$

$$\varphi(x_1) = \varphi(x_2)$$

$$\Rightarrow \varphi(x_1) \varphi(x_2)^{-1} = e$$

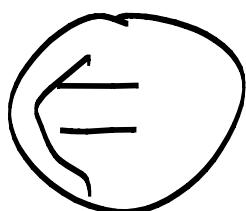
$$\Rightarrow \varphi(x_1) \varphi(x_2^{-1}) = e$$

$$\Rightarrow \varphi(x_1 x_2^{-1}) = e$$

$$\Rightarrow x_1 x_2^{-1} \in \ker \varphi = \{e\}$$

$$\Rightarrow x_1 x_2^{-1} = e$$

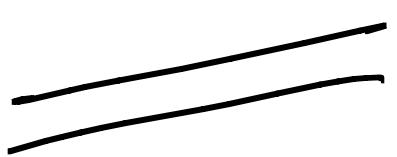
$$\Rightarrow x_1 = x_2.$$

  $\varphi$  inj  $\Rightarrow \ker \varphi = \{e\}$

$x \in \ker \varphi$  and  $x \neq e$

$$\varrho(x) = e \Rightarrow x = e \Rightarrow \infty$$

is



Examples:

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

$$\varrho(A) = \det A$$

$\varrho$  is a group homomorphism.

$$\ker \varrho = SL_n(\mathbb{R})$$

$$\text{Im } \varrho = \mathbb{R}^* \quad \varrho \text{ is surjective}$$

$$x \in \mathbb{R}^*$$

$$\begin{pmatrix} x & \\ & \ddots \\ & & 1 \end{pmatrix}$$

$$\textcircled{2} \quad \varphi: (\mathbb{R}, +) \rightarrow \mathbb{C}^*$$

$$t \mapsto e^{2\pi i t}$$

group homomorph.

$$\ker \varphi = \mathbb{Z}$$

$$\operatorname{Im} \varphi = \text{circle } S^1$$

$$\textcircled{3} \quad \varphi_m: \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{where } m \text{ is an int.}$$

$$x \mapsto mx \quad m \neq 0$$

group.

$$\ker \varphi_m = 0 \text{ if } m \neq 0$$

$$\operatorname{Im} \varphi_m = m\mathbb{Z}$$

$$N_G(H) = \left\{ g \in G \mid \underbrace{g H g^{-1}}_{\{ghg^{-1} \mid h \in H\}} \subset H \right\}$$

$$S_3 \quad H = \{1, (12)\}$$

$$(23)H(23) = \{1, (23)(12)(23)\} \\ = \{1, (13)\}$$

$$g H g^{-1} \subset H$$

$$h \mapsto ghg^{-1}$$

#  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z}$

$\varphi : G_1 \rightarrow G$  isomorphism  
 $\text{order } n \xrightarrow{\varphi} \text{order } (\varphi(n))$

#  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

#  $\mathbb{Z}/m\mathbb{Z}$  not a subgroup of  $\mathbb{Z}$ .

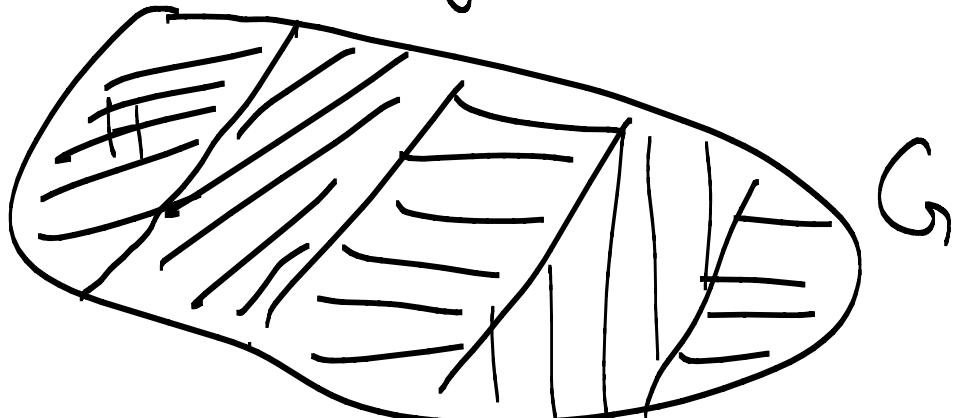
#  $G/N \xrightarrow{\sim} K$

If we know  $G$  what  
 are all  $G/N$ ?

04 | 03 | 21

Recall: quotient

$G$  a group // Given  
 $H$  a subgroup



left cosets  $G/H = \{aH \mid a \in G\}$

$$aH \cdot bH = abH$$

This multiplication makes  
sense on  $G/H$  only when  
 $H$  is a normal subgroup.

When we have  $N$  a normal subgroup of  $G$ , the set of left cosets

$$G/N = \{gN \mid g \in G\}$$

is a group with mult. given by  $g_1 N \cdot g_2 N := g_1 g_2 N$ .

---

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ g & \mapsto & gN \end{array}$$

(1)  $\pi$  is well-defined

②  $\pi$  is a group homomor.

$$\pi(g_1 g_2) = \pi(g_1) \cdot \pi(g_2)$$

$$\pi(g_1 g_2) = g_1 g_2 N$$

$$= g_1 N \cdot g_2 N$$

$$= \pi(g_1) \pi(g_2)$$

③  $\ker \pi = N$

④ Is it surjective?

Yes.

---

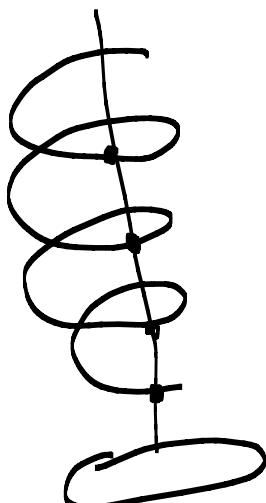
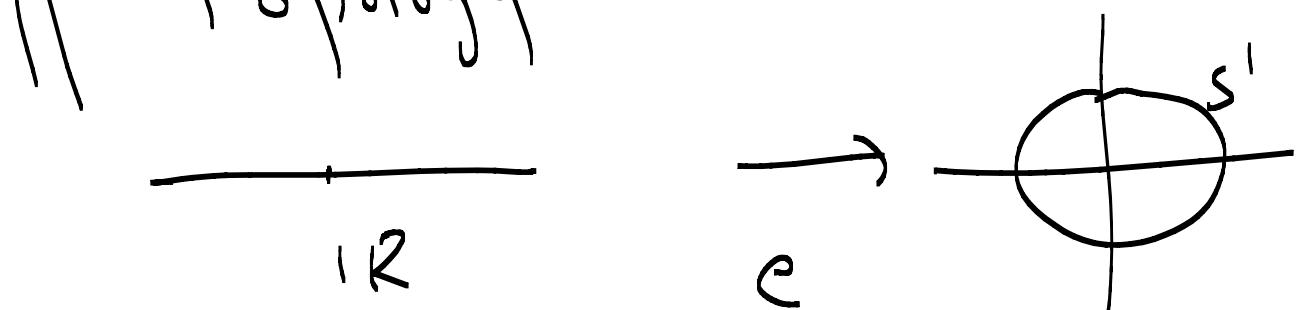
$\pi$  is a surjective group homomor. (projection)

This construction is quite common.

// linear algebra.       $V$  v.s.  
 $W$  subspn of  $V$

$$\dim(V/W) = \dim V - \dim W$$

// Topology



$$G / H$$
$$|G/H| = \frac{|G|}{|H|}$$

\* Theorem: (First Isomorphism theorem)

Let  $\phi : G_1 \rightarrow G_2$  be group homomorphism. Then,

- ① We have  $\bar{\phi} : G_1 / \ker \phi \rightarrow G_2$  a group homomorphism.
- ②  $\bar{\phi}$  is injective.
- ③ If  $\phi$  is surjective then  $\bar{\phi}$  is also surjective.

---

$$\begin{array}{ccc} G_1 & \xrightarrow{\phi} & G_2 \\ \pi \downarrow & & \searrow \bar{\phi} \\ G_1 / \ker \phi & & \end{array}$$

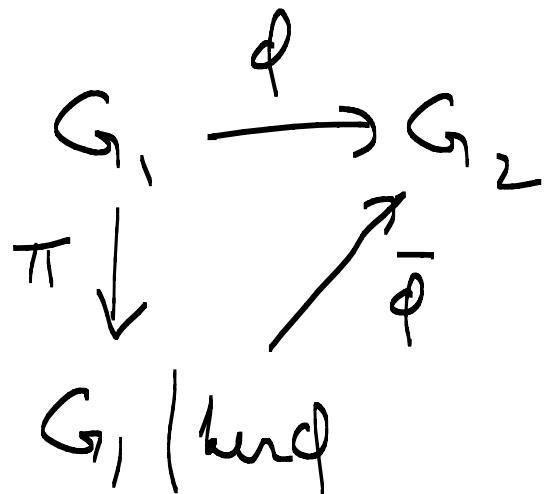
#  $\phi: G_1 \rightarrow G_2$  group homomorphism.  
 Then,  $\phi$  is injective  $\Leftrightarrow \ker \phi = \{e\}$ .

---

Proof of Thm.

(1)

Given  $\phi$   
 how to define  $\bar{\phi}$



define:  $\boxed{\bar{\phi}(g \cdot \ker \phi) := \phi(g)}$

Why it should work see -  
 $n \in \ker \phi$   $\phi(g_n) = \phi(g)\phi(n) = \phi(g)$

•  $\bar{\varphi}$  is a group homomorphism.

$$\bar{\varphi}((g \cdot \ker \varphi) \cdot (h \cdot \ker \varphi))$$

$$= \bar{\varphi}(g \cdot \ker \varphi) \bar{\varphi}(h \cdot \ker \varphi)$$

$$\bar{\varphi}((g \cdot \ker \varphi)(h \cdot \ker \varphi)) \quad (\text{def. of quotient})$$

$$= \bar{\varphi}(gh \cdot \ker \varphi) \leftarrow \text{def } \bar{\varphi}$$

$$= \varphi(gh) \quad \leftarrow \varphi \text{ is a group homom.}$$

$$= \varphi(g)\varphi(h)$$

$$= \bar{\varphi}(g \cdot \ker \varphi) \bar{\varphi}(h \cdot \ker \varphi)$$

② To show  $\bar{\varphi}$  is injective.

i.e.,  $\ker(\bar{\varphi})$  is trivial.

$$\ker \bar{\varphi} = \left\{ g \cdot \ker \varphi \mid \underbrace{\bar{\varphi}(g \cdot \ker \varphi)}_{\in G_1 / \ker \varphi} = e \right\}$$

$$\begin{aligned} \bar{\varphi}(g \cdot \ker \varphi) &= e \\ \varphi(g) &\Rightarrow g \in \ker \varphi \end{aligned}$$

$$\Rightarrow \ker \bar{\varphi} = \left\{ \ker \varphi \right\} \subset G_1 / \ker \varphi$$

↑ identity of this group.

③  $\varphi$  is surj ( $\Rightarrow \bar{\varphi}$  is surj)

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \downarrow \ker \varphi & \nearrow \bar{\varphi} & \end{array}$$

We have defined group?

Question Can we classify

all groups?

finite

vs

infinite

?

Theorem 1: Let  $G$  be a finite

group of prime order. Then,

$G$  is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$  for some prime  $p$ .

Theorem 2: Any cyclic group  
is either isomorphic to  $\mathbb{Z}$   
or  $\mathbb{Z}/n\mathbb{Z}$  for some  $n$  positive.

Lemma: If  $G$  cyclic, then any  
subgroup of  $G$  is also cyclic.

Part of Theorem 1.

Let  $|G| = p$ ,  $p$  a prime.

Take  $x \neq e \in G$

$$H = \langle x \rangle \quad |H| \geq 2$$

Lagrange's Theorem implies

$$|H| \mid |G| = p \Rightarrow |H| = \cancel{p} \text{ or } p.$$

$$\Rightarrow |H| = p$$

$$\Rightarrow H = G = \langle \alpha \rangle.$$

Now we have  $G$  is cyclic  
of finite order  $p$ . Now

---


$$\text{using Thm 2} \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$$


---

Proof of Thm 2.

Given  $G$  is a cyclic grp.

$$G = \langle \alpha \rangle = \left\{ \alpha^0, \alpha^1, \alpha^{-1}, \alpha^2, \alpha^{-2}, \dots \right\}$$

Define a map

$$\varphi : (\mathbb{Z}, +) \longrightarrow G$$
$$n \mapsto x^n$$

check ①  $\varphi$  is a group homomph.  
②  $\varphi$  is surjective.

$$\begin{aligned} \checkmark \varphi(n+m) &= x^{n+m} = x^n x^m \\ &= \varphi(n) \varphi(m) \end{aligned}$$

$\checkmark$   $\varphi$  is surj because  $G$  is cyclic.

Now, what is  $\ker \varphi$ ?

triv  $\leftarrow$   $\rightarrow$  non-triv.

Case 1 :  $\ker \phi = \{0\}$

$\Rightarrow \phi$  is inj

$\Rightarrow \mathbb{Z} \cong G$ .

Case 2  $\ker \phi$  non-triv.

$\ker \phi = n\mathbb{Z} \quad n \geq 1$

Apply first isomorphism th.

$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong G$ .

---

9 March 2021

## Group Action.

Let  $G$  be a group.

Let  $A$  be a set.

A map  $G \times A \rightarrow A$  is said to be a group action if it satisfies the following properties.

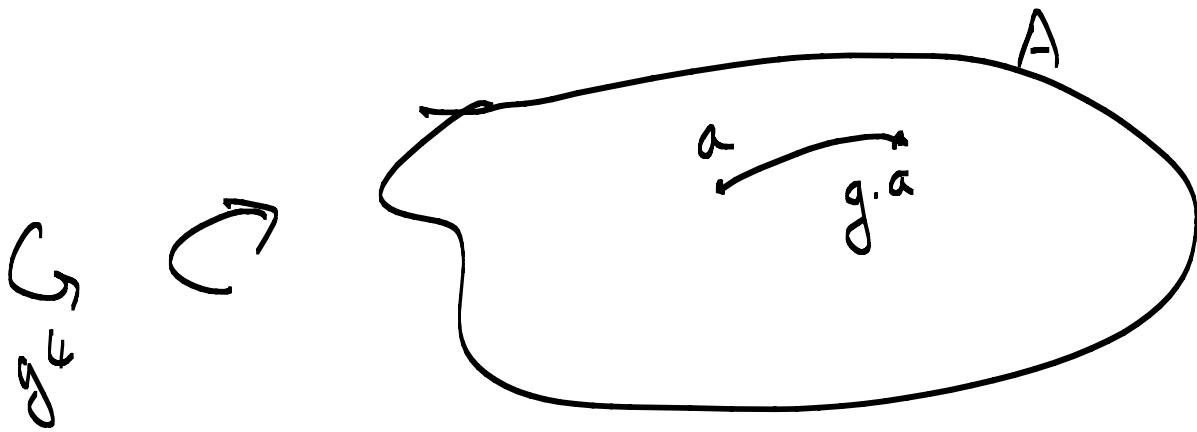
(i)  $e \cdot a = a \quad \forall a \in A.$

(ii)  $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$

$\forall g_1, g_2 \in G$   
and  $\forall a \in A.$

---

Given a grp  $G$



Example

①  $G$  any group  
 $A$  a set

$$G \times A \rightarrow A$$

$$(g, a) \mapsto a$$

i.e.  $g \cdot a = a \quad * a \in A$   
 $* g \in G$

This action is called trivial action.

(2)

$$G = S_n$$

$$A = \{1, 2, 3, \dots, n\}$$

$$S_n \times A \rightarrow A$$

$$(g, i) \mapsto g(i)$$

it satisfies both properties  
of being an action.

---

Suppose we are given an  
action. Given  $G$  a group

$A$  a set

$$\begin{aligned} G \times A &\rightarrow A \\ (g, a) &\mapsto g \cdot a \end{aligned}$$

Fix an element  $\underline{g \in G}$ .

Take  $a \in A$ ,  $ga \in A$

This I can do for any  $a \in A$ .

$$\begin{aligned} \delta_g : A &\rightarrow A \\ a &\mapsto g \cdot a \end{aligned}$$

$$\delta_g(a) := g \cdot a$$

•  $\delta_g$  is a well-defined.

$$a_1 = a_2 \Rightarrow g \cdot a_1 = g \cdot a_2$$

• Injective map.

$$\delta_g(a_1) = \delta_g(a_2) \Rightarrow a_1 = a_2$$

$$g(a_1) = g(a_2) \Rightarrow ga_1 = ga_2$$

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

$$\Rightarrow (g^{-1}g) \cdot a_1 = (g^{-1}g) a_2$$

$$\Rightarrow c \cdot a_1 = c \cdot a_2$$

$$\Rightarrow a_1 = a_2.$$

$\tilde{g}$  is surjective ?

Let  $\alpha \in A$

Does  $\exists a \in A$  s.t.  $\tilde{g}(a) = \alpha$  ?

Take  $a = g^{-1}\alpha$

$$\begin{aligned} \tilde{g}(g^{-1}\alpha) &= g \cdot (g^{-1}\alpha) = (gg^{-1})\alpha \\ &= c \cdot \alpha = \alpha \end{aligned}$$

Given an action

Given  $a \in G$  we get

a map  $\delta_a : A \rightarrow A$   
which is a bijection.

In fact, we get

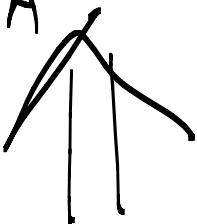
$$G \longrightarrow \text{Bijet}(A)$$

$\sim\!\!\!$

$$\text{Perm}(A) = S_A$$

$$g \mapsto \delta_g$$

$G$  a group,  $A$  a set, an action.

$$G \times A \rightarrow A$$


↓

$\sigma : G \rightarrow \text{Perm}(A)$

This is  
a group  
action  
on A.

$$g \mapsto \sigma_g$$

group homomorphism.

$$\sigma(g_1 g_2) = \sigma(g_1) \circ \sigma(g_2)$$

$$\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$$

$$\begin{aligned}\sigma_{g_1 g_2}(a) &= g_1 g_2 \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \sigma_{g_1}(g_2 \cdot a) = \sigma_{g_1} \sigma_{g_2}(a)\end{aligned}$$

We can also do review?

$$\sigma: G \rightarrow \text{Perm}(A)$$

What is given to us:

- a group  $G$
- a set  $A$
- a group homomorphism  
 $\sigma: G \rightarrow \text{Perm}(A)$

Then, we can have an action.

$$G \times A \longrightarrow A$$

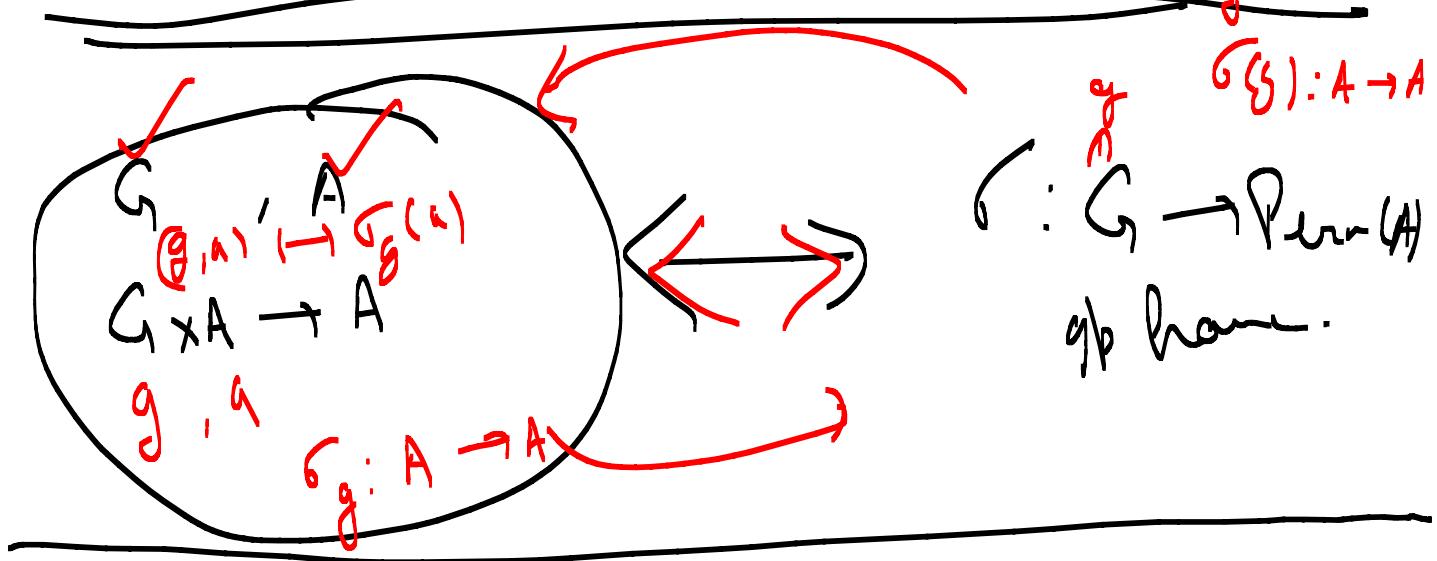
$$(g, a) \mapsto \sigma_g(a)$$

- $c \cdot a = a$  because  $\sigma$  takes identity to identity.

$$\cdot \quad g_1(g_2a) = (g_1g_2)(a)$$

this is equivalent to  $G$  being  
a group homom.

$$g(g)(a) \underset{=} {\equiv} G_g(a)$$



### Example:

① Trivial action.

$$G \times A \rightarrow A$$

$$(g, a) \mapsto a$$

$\begin{array}{ccc} & \uparrow \\ \hookrightarrow: & G \rightarrow \text{Perm}(A) \\ & g \mapsto \text{Identity.} \end{array}$

$\textcircled{2}$        $G = S_n, \quad A = \{1, \dots, n\}$   
 $S_n \times A \rightarrow A$   
 $(g, i) \mapsto g(i)$

$\begin{array}{ccc} & \downarrow \\ \hookrightarrow: & S_n \rightarrow \text{Perm}(A) \\ & g \mapsto g \end{array}$

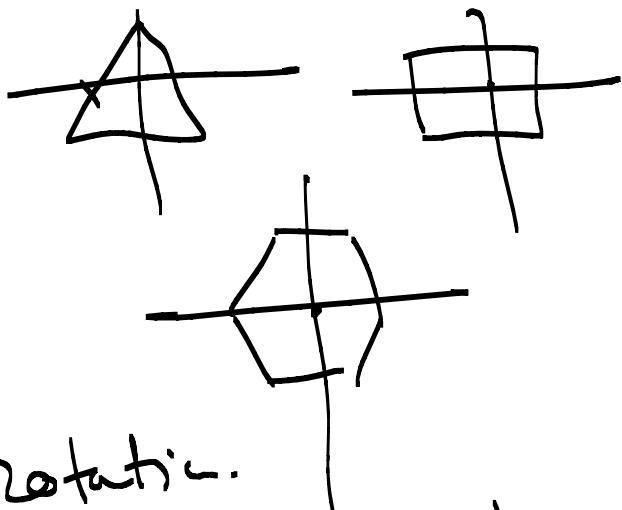
③

Dihedral gp.

$D_{2n}$

$n - \text{gen} \equiv D_n$

$$\left\{ r, s \mid r^n = 1, s^2 = 1, sr = r^{-1} \right\}$$



$r \mapsto \text{rotation.}$

$$\begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

$s \mapsto \text{reflctn.} \quad \theta = \frac{2\pi}{n}$

---

$A \rightsquigarrow \text{Perm}(A)$  gtf

$\cup$   
 $\langle S \rangle$

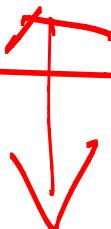
11 March 2021

## Group action

We are given a group  $G$   
given a set  $A$

if  $G \times A \rightarrow A$  is a group action  
(i)  $e \cdot a = a \quad \forall a \in A$

$$(ii) g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$$



$$\text{Bi}_1(A) = S_A$$

$$G \rightarrow \text{Perm}(A)$$

group homomorphism -

#  $G \times A \rightarrow A$  is an action

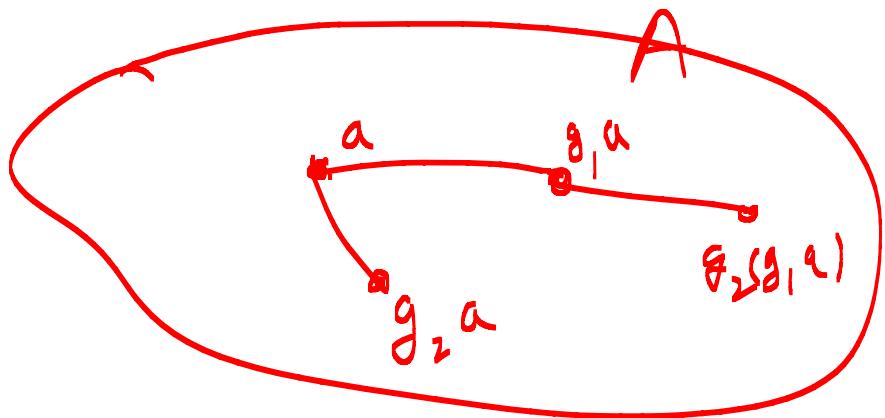


Def.

$$a \in A$$

$$O_a = \{ g \mid g \cdot a \text{ for some } g \in G \}$$

Orbit  
of a



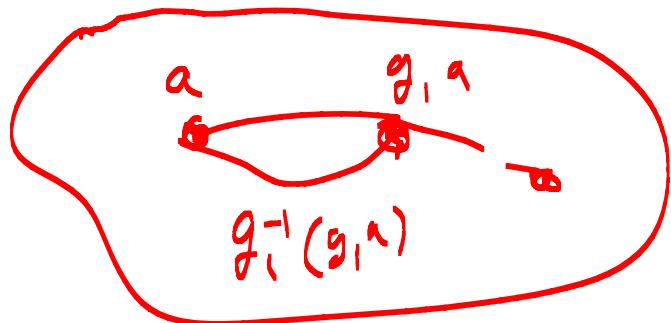
$$\begin{aligned} O_a &= \{ g a \mid g \in G \} \\ &= G \cdot a \end{aligned}$$

Def 2.  $a \in A$

Stabiliser of  $a$  in  $G$  is

$$G_a = \text{Stab}(a)$$

$$:= \{ g \in G \mid g \cdot a = a \}$$



Warning:

$$G_a \subset A$$

$$\text{Stab}(a) = G_a \subset G$$

↗ a subgroup-

Claim:  $G_a$  is a subgroup of  $G$ .

(i)  $g_1, g_2 \in G_a \Rightarrow g_1 g_2 \in G_a$

$$\begin{aligned} g_1 \cdot a = a \\ g_2 \cdot a = a \end{aligned} \quad \Rightarrow \quad \begin{aligned} g_1 g_2 \cdot a \\ g_1 (g_2 \cdot a) \\ \quad \vdots \\ g_1 \cdot (a) = a \end{aligned}$$

(ii)  $g \in G_a \Rightarrow g^{-1} \in G_a$

$$g \cdot a = a$$

$$\begin{aligned} a &= e \cdot a = (g^{-1} \cdot g) a \\ &= g^{-1} (g \cdot a) = g^{-1} a \end{aligned}$$

Def 3 (quotient)

$A/G :=$  A set of representatives  
for each orbit.

---

Def 4 : kernel of an action.

$$\ker = \{ g \in G \mid g \cdot a = a \ \forall a \in A \}.$$

If  $\ker$  of an action is  
trivial then it is called  
a faithful action.

Example  $G = GL_n(\mathbb{R})$

$$A = \mathbb{R}^n$$

$$\begin{aligned} G \times A &\rightarrow A \\ (x, x) &\mapsto xx \end{aligned}$$

this is an action-

What are the orbits?

$$\vec{0} \in A = \mathbb{R}^n$$

$$O_{\vec{0}} = \{0\} \quad \xrightarrow{\textcircled{1}}$$

$$x \in A \setminus \{0\} = \mathbb{R}^n \setminus \{0\} \quad \xrightarrow{\textcircled{2}}$$

$$O_x = \mathbb{R}^n \setminus \{0\}$$

$$\text{Stab}(\bar{o}) = G_{\bar{o}} = \text{GL}_n(\mathbb{K})$$

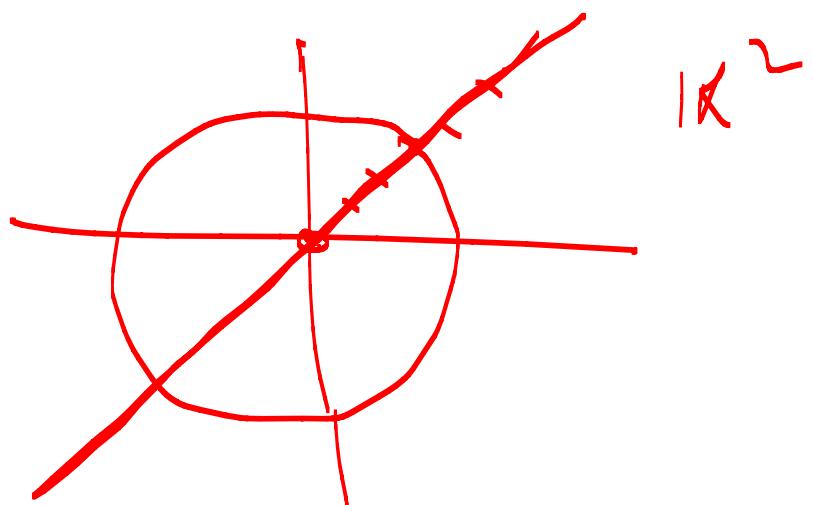
Example:  $\ker = \{I\}$

$$\text{Stab}\left(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right) = \boxed{\begin{array}{c|cc} 1 & * & * \\ 0 & * & * \\ \vdots & & \\ 0 & * & \end{array}}$$

$$G = SO(2), A = \mathbb{R}^2$$

$$G \times A \rightarrow A$$

$$(x, u) \mapsto x(u)$$



Orbit: "Circle"

Stab.  $G_{\bar{o}} = SO(2)$

$$G_{\begin{pmatrix} 1 & \\ 0 & 0 \end{pmatrix}} = I$$

$$\ker = I.$$

---

---

Example. Trivial act.

$$G \times A \rightarrow A$$

$$(g, a) \mapsto a \quad \begin{matrix} g \in G \\ a \in A \end{matrix}$$

What are the orbits?

$$\{a\}$$

$$G_a = G \quad //$$

$$\ker = G. //$$

If  $x_1, x_2 \in G_a$   
then  $G_{x_1}$  &  $G_{x_2}$  are  
related?

$$\exists g, \quad g x_1 = x_2$$

$$g G_{x_1} g^{-1} = G_{x_2}$$

$$g h g^{-1}(x_2) = g h(x_1) = g u = x_2$$

16/03/21

## Group Action

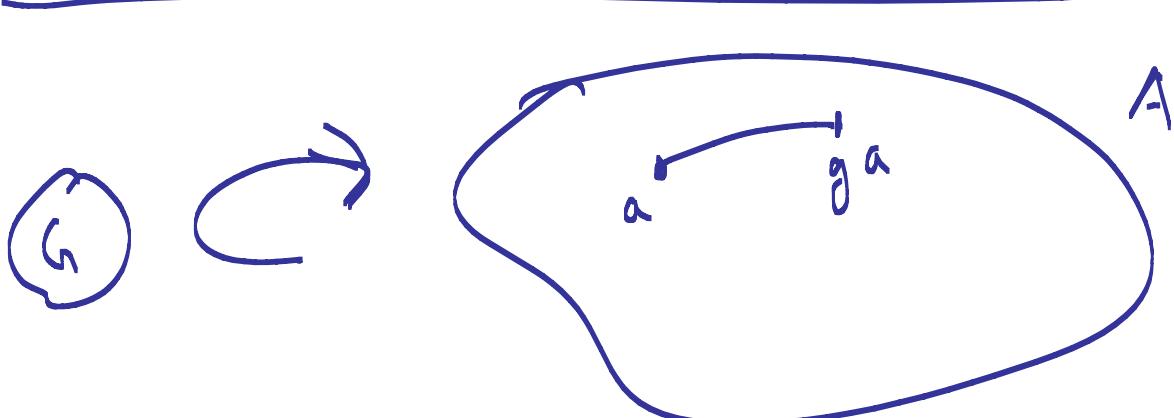
$G$  a group  
 $A$  a set

$$G \times A \rightarrow A$$

$$(i) e \cdot a = a \quad \forall a \in A$$

$$(ii) g_1(g_2 \cdot a) = (g_1 g_2) \cdot a$$

$\forall g_1, g_2 \in G$  and  $\forall a \in A$ .



$\longleftrightarrow$   $\varphi : G \rightarrow \text{Perm}(A)$   
group homomorph.

---

We defined

① Stabiliser of  $a \in A$

$$G_a = \{ g \in G \mid g \cdot a = a \} \subset G$$

② Orbit of an element  $a \in A$

$$\begin{aligned} G_a &= \{ g \cdot a \mid g \in G \} \\ &= G \cdot a \subset A \end{aligned}$$

③ Quotient  $A/G$

= set of representatives of  
each orbit.

Sometimes we think of it  
as a collection of all orbits.

---

Our aim is to see  
usefulness of group action.

---

The usual idea of quotient.

---

of a group, for a subgroup  
of  $\mathfrak{g}$ .

$\mathfrak{g}/\mathfrak{g}_L =$  set of left cosets.

$$G = \mathcal{H}, \quad A = \mathcal{G}$$

$$\begin{matrix} \mathcal{H} \times \mathcal{G} \\ (h, g) \end{matrix} \rightarrow \begin{matrix} \mathcal{G} \\ gh^{-1} \end{matrix}$$

~~Check~~  
this is an action.

$$(i) \quad e \cdot g = g e^{-1} = g$$

$$(ii) \quad h_1 \cdot (h_2 \cdot g) \stackrel{?}{=} (h_1 h_2) \cdot g$$

$$\text{LHS} \quad h_1 \cdot (h_2 \cdot g) = h_1 \cdot (\underbrace{g h_2^{-1}}_{})$$

$$= (g h_2^{-1}) h_1^{-1}$$

$$= g (h_2^{-1} h_1^{-1})$$

$$= g (h_1 h_2)^{-1}$$

$$\underline{\text{RHS}} \quad h_1 h_2 \cdot g = g (h_1 h_2)^{-1}.$$

Orbits of this action.

$$g \in \mathfrak{g}, \quad G_g = \{ h \cdot g \mid h \in \mathcal{H} \}$$

$$= \{ gh^{-1} \mid h \in \mathcal{H} \}$$

$$= g \mathcal{H}$$

Quotient under this action is

$\underset{g \in \mathfrak{g}}{\text{the set of all left const.}}$

$$\text{Stab}(g) = \{ h \in \mathcal{H} \mid h \cdot g = g \}$$

$$= \{ h \in \mathcal{H} \mid gh^{-1} = g \}$$

$$= \{ e \}.$$

Question:  $f: G \times G \rightarrow G$

$$(h, g) \mapsto gh$$

Is this an action?

$$h_1 \cdot (h_2 \cdot g) = h_1 \cdot (gh_2) = gh_2h_1$$

$$(h_1h_2) \cdot g = gh_1h_2$$

---

Now we look at some actions where group acts on itself?

Given a group  $G$ .

Can we have group action?

①  $A = G$ , trivial action

②  $A = G$  Left regular action

$$G \times A \rightarrow A$$

$$(g, a) \mapsto ga$$

is a group action.

$$(i) c \cdot a = a \quad \checkmark$$

$$((ii)) g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$$

this is associativity.

③

Right regular action.

$$G = G, \quad A = G$$

$$G \times A \rightarrow A$$

$$(g, a) \mapsto ag^{-1}$$

this is an action.

④

Conjugacy action

$$G = G, \quad A = G$$

$$G \times A \rightarrow A$$

$$(g, a) \mapsto gag^{-1}$$

this is an action.

$$\checkmark e \cdot a = e^a e^{-1} = a$$

$$\checkmark g_1 \cdot (g_2 \cdot a) \stackrel{?}{=} (g_1 g_2) \cdot a$$

$$\underline{\text{LHS}} \quad g_1 \cdot (g_2 \cdot a)$$

$$= g_1 \cdot (g_2^a g_2^{-1})$$

$$= g_1 (g_2^a g_2^{-1}) g_1^{-1}$$

$$= (g_1 g_2) a (g_2^{-1} g_1^{-1})$$

$$= (g_1 g_2) a (g_1 g_2)^{-1}$$

$$= g_1 g_2 \cdot a = \text{RHS.}$$

Theorem (Cayley's Theorem)

Let  $G$  be a finite group. Then,  
 $\exists n$  such that  $G$  is  
isomorphic to a subgroup of  $S_n$ .

Proof: left regular action of  
 $G$  on itself.

$$A = G$$

$$G \times A \rightarrow A$$



$g : G \rightarrow \text{Perm}(A)$   
group homomorphism

$$n = |G|$$

$$\varrho : G \rightarrow S_n = \text{Per}(A)$$

Claim  $\varrho$  is an injective map.

c.e.  $\ker(\varrho) = e$ .

$$g \in \ker \varrho$$

$\varrho(g) = \text{Id}$

here  $\varrho(g) : A \rightarrow A$

$$\varrho(g)(a) = g \cdot a$$

$\Rightarrow g \cdot a = a \quad \forall a \in A$

$\Rightarrow g = e$ .

$\Rightarrow$   $\ker \varphi$  is full  
hence  $\varphi$  is inj.

Take-  $G' = \text{Im}(\varphi)$

then,  $G'$  is isomorphic

to  $G'$ . This proves  
the theorem.  $\blacksquare$

$N$  normal of  $G$

$\pi: G \rightarrow G/N$  of hom.  
 $g \mapsto gN$

$$\begin{array}{ccc} G & & N \\ \curvearrowright & \circlearrowleft & \curvearrowright \\ \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} & \longrightarrow & \mathbb{Z}/_{2\mathbb{Z}} \\ (a,b) & \mapsto & a \end{array}$$

$$\varrho : \quad \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \mapsto 2n$$

$$\ker \varrho = 0, \quad \text{Im } 2\mathbb{Z}$$

$$\pi : \quad \mathbb{Z} \longrightarrow \mathbb{Z}/_{2\mathbb{Z}}$$

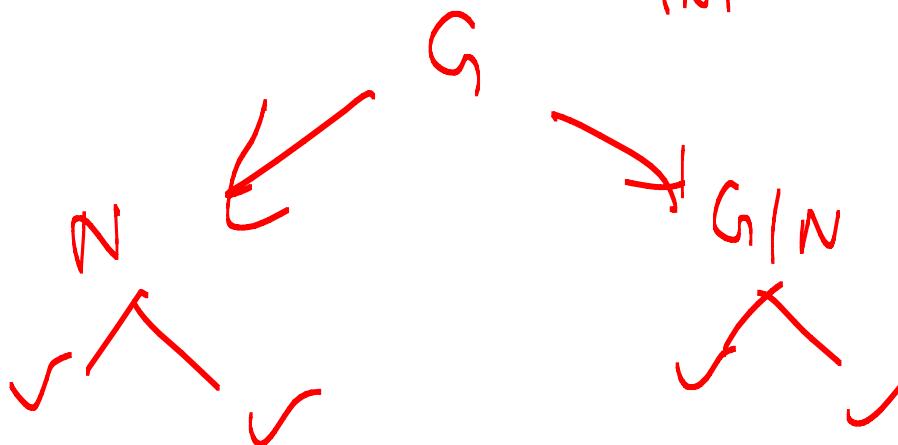
finite:  $G = H_1 \cup H_2 \cup \dots$

$$N \subset G \text{ normal}$$

$$G/N \quad | < |N| < G$$

$$1 < |G/N| < |G|$$

$$\therefore \frac{|G|}{|N|}$$



Similar q/t.

$$\underline{18 \mid 3 \mid 2}$$

We want to define alternating group!

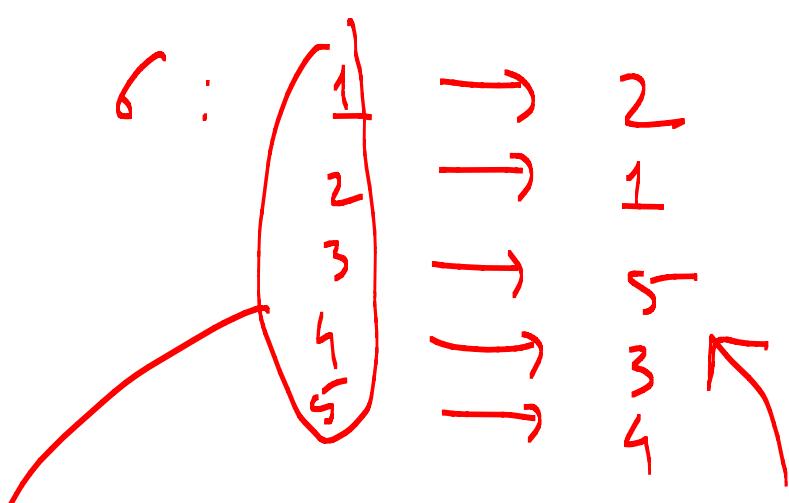
$$G = S_n \quad n \geq 2$$

$$S_n \ni \sigma \quad X = \{1, \dots, n\}$$

$$\sigma : X \rightarrow X$$

We think of  $\sigma$  as a product of disjoint cycles.

$$\underline{\underline{n = 5}}$$



$$G = \underbrace{(1 \ 2)}_{\text{2-cycle}} \underbrace{(3 \ 5 \ 4)}_{\text{3-cycle}}$$

$$G = \underbrace{(1)}_{\text{1-cycle}} \underbrace{(2)}_{\text{1-cycle}} (3 \ 5 \ 4)$$

Def:  $(a_1 \ a_2 \ \dots \ a_n) \in S_n$

is called an  $n$ -cycle,  
and length of this cycle  
is  $n$ .

Warning : not every element  
in  $S_n$  is a cycle.

$$n = 2$$

$$S_2 = \{(1)(2) = e, (12)\}$$

$$\underline{n = 5}$$

$$(12)(345) \in S_5$$

$$(12) \in S_5$$

$$(345) \in S_5$$

---

# Every element of  $S_n$  is  
a product of disjoint cycles.

$(12), (345) \in S_5$

$\begin{array}{c} (12) \\ \equiv \\ (345) \end{array} \in S_5$

Def: Disjoint cycles: no symbol is common.

Example.  $(12), (34) \in S_5$  are disjoint cycles.

$(12), (15) \in S_5$  are not disjoint.

#  $\sigma \in S_n$ ,  $X = \{1, 2, \dots, n\}$

$$H = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$$

$$H \times X \rightarrow X$$

$$(\sigma, i) \mapsto \sigma(i)$$

This is an action.

What are the orbits?

The orbits are the elements

appearing in different cycles

when we write  $\sigma$  as a  
product of disjoint cycles.

Example

$$\sigma = (12) (456) (789) \in S_9$$

$$H = \langle \sigma \rangle, \quad X = \{1, 2, \dots, 9\}$$

$$\begin{array}{l|l} G_1 = \{1, 2\} & G_4 = \{4, 5, 6\} \\ G_2 = \{1, 2\} & = G_5 = G_6 \\ G_3 = \{3\} & G_7 = \{7, 8, 9\} \\ & = G_8 = G_9 \end{array}$$

---

Def.: A cycle of length 2

is called a transposition.

Examp  $(12), (4,5) \in S_5$   
are transposition.

Fact: "disjoint cycles commute".

$$(12)(23) = (123)$$

$$(23)(12) = (132)$$

$$\begin{aligned}
 \underline{\underline{S_4}} : & \left\{ \begin{array}{l} \underline{1}, \\ (12), (13), (14), (23), (24) \\ (34), \end{array} \right. \\
 \rightarrow & (12)(34), (13)(24), (14)(23), \\
 & (123), (124), (234), (134), \\
 & (132), (142), (243), (143), \\
 & (1234), (1324), (1423), \\
 & (1243), (1342), (1432) \left. \right\}
 \end{aligned}$$

\* Every element of  $S_n$  is a product of transpositions.

We need to write a cycle  
as a product of transpositions  
in the view of earlier fact.

$$\checkmark (a_1, \dots, a_n) = (a_1 a_2)(a_1 a_{2-1}), \dots \\ \dots (a_1 a_2).$$

Verify this

$$(356) \stackrel{?}{=} (38)(35) \checkmark$$

Warning - This way of  
writing an element as a  
product of transpositions is

WF unique.

A red arrow points from right to left, indicating the direction of current flow in the circuit diagram.

Fact: When we write an element  $\sigma \in S_n$  as a product of transpositions, the number of transpositions is either even or odd and doesn't depend on writing as a product of transpositions.

Def. Alternating group

$A_n$  = set of all elements  
of  $S_n$  which are a  
product of even number of  
transpositions.

---

$$(357) = \underset{1}{(37)} \underset{2}{(35)}$$

$$= (37)(37)(37)(35)$$

$$= (37)(14)(14)(35)$$

---

$$A_3 = \{1, (123), (132)\}$$

$$A_4 = \{1, (12)(34), (13)(24),$$

$(14)(23), (123), (132) \dots \}$

$$|A_4| = 12$$

$$\overline{|A_n|} = \frac{|S_n|}{2} = \frac{n!}{2}$$

Fact:  $A_n$  is a normal subgroup of  $S_n$  of index 2.

Another way to understand

$$S_n \rightarrow GL_n(\mathbb{R})$$

$$\sigma \mapsto \begin{matrix} e_1 \mapsto e_{\sigma(1)} \\ \vdots \\ e_n \mapsto e_{\sigma(n)} \end{matrix}$$

$$A_\sigma = \begin{bmatrix} & \\ & \end{bmatrix}$$

$$\begin{matrix} S_n & \xrightarrow{\quad} & GL_n(\mathbb{R}) & \xrightarrow{\det} & \mathbb{R}^* \\ \hookrightarrow & & A_\sigma & & \\ & \curvearrowright & & & \end{matrix}$$

$\phi = \text{sgn}$

$$\det A_\sigma = \pm 1$$

$\text{ker } \phi = A_n$

This map is also called  
signature or sign map.

Def: Elements of  $A_n$  are called "even" permutations and exist in  $S_n$  but not in  $A_n$  are odd permutations

---

Yet another way to understand this.

---

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix}$$

$x_1, \dots, x_n$  are variables -

$$\Delta = \det V = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

$\sigma \in S_n$

$$\sigma(\Delta) := \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

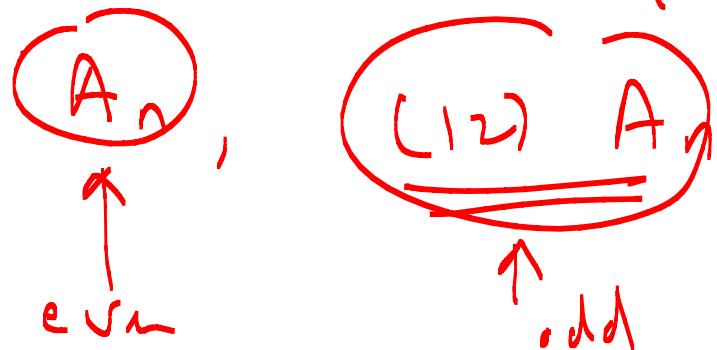
Claim:  $\sigma(\Delta) = \pm \Delta$ .

The elements of  $A_n$  will  
give sign +1 and other  
will give -1.

Example - Any transposition will give sign  $-1$ .

$$\overbrace{\quad}^{n \geq 3} S_n \quad A_n \subset S_n$$

$$(12) \in S_n \setminus A_n$$



Fact:  $A_n$ ,  $n \geq 5$  are simple groups.

(That is, they have no proper normal subgroups).

---

Free group-

Given a group  $G$

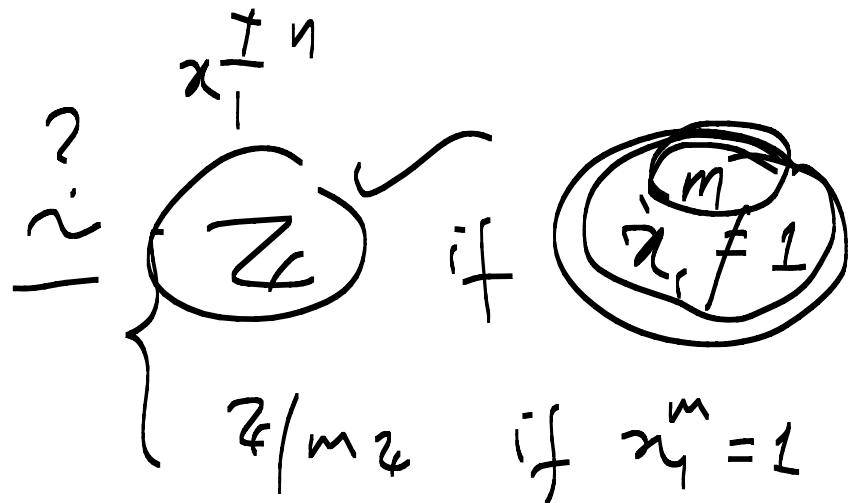
$S \subset G$ ,

$\langle S \rangle \in G$   
A subgp.  
 $s_1, s_2, \dots, s_k$   
 $s_{i_1}, s_{i_2}, \dots, s_{i_k}$

Begin with abstract symbols.

$$\{x_1\}$$

$$G(<x_1>) = \left\{ \begin{array}{l} x_1^0 = 1, x_1, x_1^2, \dots \\ x_1^{-1}, x_1^{-2}, \dots \end{array} \right\}$$



$$G(<x_1, x_2>) = \left\{ 1, x_1^{\pm 1}, x_1^{\pm 2}, \dots \right. \\ \left. x_2^{\pm 1}, x_2^{\pm 2}, \dots \right\}$$

F-wgr. - on 2-symbols.

$x_1 x_2 = x_2 x_1$

not true in  
free  $\mathbb{M}$ .

$$\underline{\underline{x_{i_1}^{r_1} x_{i_2}^{r_2} \dots x_{i_k}^{r_k}}} = 1 \times$$

$$x_1 x_2 x_1 x_2 x_1 x_2 \dots x_1$$

$\overbrace{\quad\quad\quad}$   
 $\overbrace{\quad\quad\quad}$

## **2 Post Midsem**

**2.1 Notes 7**

**2.2 Notes 8**

**2.3 Notes 9**

**2.4 Presentation**

01 April 2021

## Group action.

$G$  a group.

finite

infinite

→ Lie groups

→ Algebraic groups

→ Matrix groups

→ Geometric group Theory

Can we write down all

finite groups?

No

up to isomorphism.

## Groups of order

1

$$\{e\}$$

2

$$\mathbb{Z}/2\mathbb{Z}$$

3

$$\mathbb{Z}/3\mathbb{Z}$$

4

$$\mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad ?$$

5

$$\mathbb{Z}/5\mathbb{Z}$$

6

$$\boxed{\mathbb{S}_3, \mathbb{Z}/6\mathbb{Z}} \quad ?$$

7

$$\mathbb{Z}/7\mathbb{Z}$$

8

$$\mathbb{Q}_8, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{D}_8, \quad \mathbb{Z}/2^3, \quad$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad ?$$

9

$$\mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/3^2 \quad ?$$

Theorem: Any finite group of prime order is cyclic. Hence, there is only one possible group  $\mathbb{Z}/p\mathbb{Z}$  up to isomorphism. ✓

Theorem: (we will prove after a couple of lectures)

Let  $G$  be a group of order  $p^2$  where  $p$  is a prime. Then,  $G$  is Abelian. In fact, there are  $\mathbb{Z}/p^2\mathbb{Z}$  or  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

Recall

Group action

$G$  a group  
 $A$  a set

$$G \times A \rightarrow A$$

$$\textcircled{1} \quad g \cdot a = a \quad \forall a$$

$$\textcircled{2} \quad g_1(g_2 \cdot a) \\ = (g_1 g_2) \cdot a$$

$$\forall g_1, g_2 \in G, \forall a \in A.$$

$$G_a = \{g \in G \mid g \cdot a = a\} \subset G$$

Orbit - Stabiliser Theorem

$G$  a finite group  
 $A$  a finite set

$G$  is acting  
on  $A$ .

Then,

$$\textcircled{1} \quad |A| = \sum_{a \in A/G} |G_a|$$

$$\textcircled{2} \quad |G_a| = [G : G_a]$$

$$= \frac{|G|}{|G_a|}$$

$$\Rightarrow |A| = \sum |G_a| = \sum \frac{|G|}{|G_a|}$$

where sum runs over representatives  
of orbits.

Proof: (1) We define an equivalence relation on  $A$  using the action of  $G$ .

$a \sim b$  if  $b = g \cdot a$  for  
some  $g \in G$ .

This is an equivalence relation.

- ① Reflexive  $a \sim a$ ,  $g = e$
  - ② Symmetric  $a \sim b \Rightarrow b \sim a$   
 $g \cdot a = b \Rightarrow a = g^{-1}b$
  - ③ Transitivity  
 $a \sim b, b \sim c \Rightarrow a \sim c$   
 $b = g_1 a, c = g_2 b$   
 $\Rightarrow c = g_2 b = g_2 g_1 a$
- Now the set  $A$  is disjoint

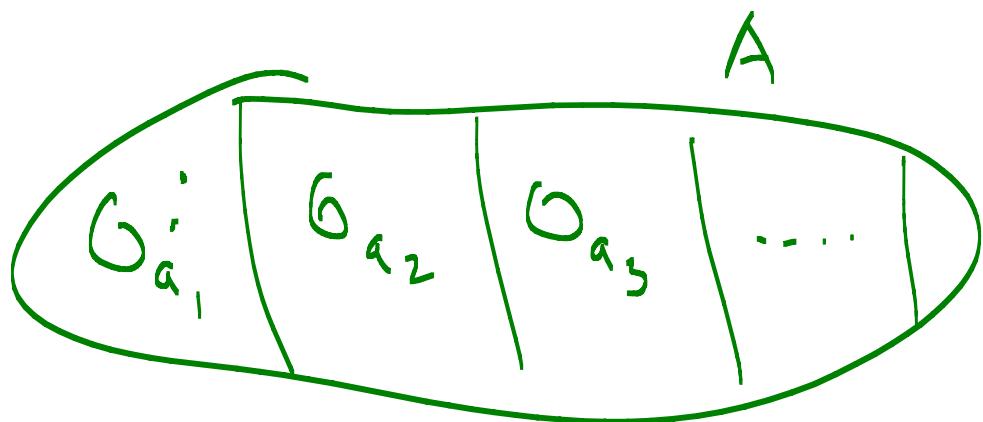
union of equivalence classes.

$$a \in A$$

$$[a] = \{ b \in A \mid b \sim a\}$$

$$= \{ b = g_a \text{ for some } g \}$$

$$= G_a$$



$$|A| = \sum_{\substack{a \\ \text{nb. of } G_a}} |G_a|$$

Recall:

$$A|G = \{G_a \subset A\}$$

$$= \{\bar{a} \mid a \in G_a\}$$

representatives of orbit

$$z \rightsquigarrow z|nz$$

$$= \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$$

$$= \{nz, 1+nz, 2+nz, \dots\}$$

Proof of (2)

We are going to define

$$G/G_a \rightarrow G_a$$

a map which is a bijection.

$$g \cdot G_a \rightarrow g \cdot a$$

Check:

- ① well-defined
- ② one-one
- ③ onto.

①  $\underline{g_1 \cdot g_a = g_2 \cdot g_a} \quad ? \Rightarrow g_1 a = g_2 a$

$$g_1 = g_2 \cdot x$$

where  $x \in G_a$

$$g_1 \cdot a = (g_2 \cdot x) \cdot a = g_2(a) \checkmark$$

②  $\underline{g_1 a = g_2 a} \Rightarrow \boxed{g_1 \cdot g_a = g_2 \cdot g_a}$

$\cancel{\downarrow}$

$$g_1^{-1} g_2 \cdot a = a$$

$g_1^{-1} g_2 \in G_a$

(3)

Sug.

This proves that

$$|G/G_a| = |G_a|$$

$$\text{or } \frac{|G|}{|G_a|}$$

This proves the Thm.

---

$G$  acting on  $A$

If it has only one orbit  
we say " $G$  is acting transitively".

Transitive action.

$$E \times_{\text{affine}} GL_2(\mathbb{R}) \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$\{0\}, \quad (\mathbb{R}^2 \setminus \{0\}).$$

$$GL_2(\mathbb{F}_q) \times \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$$

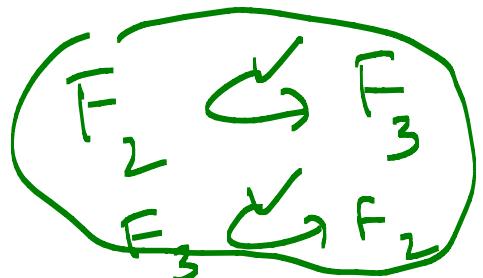
$$\{0\}, \quad \mathbb{F}_q^2 \setminus \{0\}$$

$$G_1, G_2$$

$$\varphi: G_1 \hookrightarrow G_2 \quad \psi: G_2 \hookrightarrow H_1$$

$$G_1 \rightarrow G_2 \quad ?$$

$$G_1 \xrightarrow{\cong} G_2$$





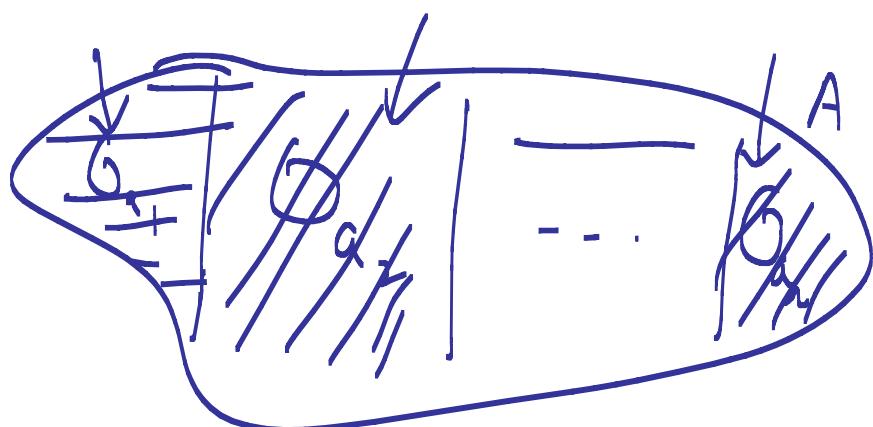
6 April 2021

## Orbit - Stabiliser Theorem:

- | G a group which is finite  
| A a finite set  
| G acting on A

Then,

$$O | A | = \sum_{a \in A/G} |G_a| \rightarrow i$$



$$\textcircled{2} \quad |G_a| = \frac{|G|}{|G_a|}$$

where  $G_a$  stabilizer of  $a$ .

Thus, i becomes

$$|A| = \sum_{a \in A/G} \frac{|G|}{|G_a|}.$$


---

Exercise: Suppose  $a, b \in A$

which are in the same orbit under the action of  $G$ . Then,

$$\exists g \in G \text{ s.t. } \underline{\underline{g G_a g^{-1} = G_b}}.$$

## Conjugation Action -

Given group  $G$ , it acts on itself as follows:

$$G = G, A = G$$

$$G \times A \longrightarrow A$$

$$(g, a) \mapsto gag^{-1}$$

This is an action.

$$\textcircled{1} \quad e \cdot a = e a e^{-1} = a$$

$$\textcircled{2} \quad g_1 \cdot (g_2 \cdot a) \stackrel{?}{=} (g_1 \cdot g_2) \cdot a ?$$

LHS

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

$$\begin{aligned}
 &= (g_1 g_2) \cdot a \cdot (g_2^{-1} g_1^{-1}) \\
 &= (g_1 g_2) \cdot a \cdot (g_1 g_2)^{-1} \\
 &= (g_1 g_2) \cdot a = \text{RHS}.
 \end{aligned}$$

Def:  $G$  a group.  $a, b \in G$

We say that  $a$  and  $b$  are  
conjugate in  $G$  if  $\exists g \in G$   
 s.t.  $g a g^{-1} = b$ .

Remark: Conjugation on  $G$  is an  
 equivalence relation.

---

We want to apply the orbit-stab  
 Theorem for conjugation action.

The orbits here are called Conjugacy classes.  $\rightarrow$  (equivalence class).

Def.  $a \in G$ ,

$$Cl(a) = \{ gag^{-1} \mid g \in G \}$$

Conjugacy class of  $a$  in  $G$ .

---

Why conjugacy classes are important?

They appear in representation theory.  
In particular, for a finite group,  
the number of irreducible  
complex representations is equal to  
the number of conjugacy classes.

---

In linear algebra we define

$$A, B \in M_n(F)$$

we say that  $A$  and  $B$  are  
"similar" if  $\exists P \in GL_n(F)$   
s.t.  $P A P^{-1} = B$ .

when  $F = \mathbb{C}$ ,  $G = GL_n(F)$

"similarity"  $\equiv$  conjugacy

and the Jordan canonical form (more generally)  
rational canonical form  
describes the conjugacy classes  
in  $GL_n(\mathbb{C})$ .



Then (Class equation)

$G$  a finite group. Then,

$$|G| = |\mathcal{Z}(G)| + \sum_a \frac{|G|}{|C_G(a)|}.$$

$\uparrow$   
non-central  
conj class.

---

\*  $\mathcal{Z}(G)$  center of  $G$ .

$$g \in \mathcal{Z}(G) \Rightarrow gh = hg \forall h$$

$$\begin{aligned} \text{then, } C_G(g) &= \{hgh^{-1} \mid h \in G\} \\ &= \{g\}. \end{aligned}$$

$$g \in \mathcal{Z}(G) \Leftrightarrow |C_G(g)| = 1$$

$$\mathcal{Z}(G) = G \Leftrightarrow G \text{ is Abelian.}$$

Ques.  $G$  acting on itself  
by conjugation.

$$G \times G \rightarrow G$$
$$(g, a) \mapsto gag^{-1}.$$

Orbits are conjugacy classes.

$$O_a = \{ g \cdot a = gag^{-1} \mid g \in G \}$$
$$= C_G(a)$$

Stabiliser of  $a$  in  $G$ ?

$$G_a = \{ g \in G \mid gag^{-1} = a \}$$
$$= C_G(a) \quad \text{centraliser of } a \text{ in } G.$$

for orbit stabilizer  $\Rightarrow$

$$|G| = \sum_{\substack{a \in A/G \\ \text{Conj class}}} \frac{|G|}{|C_G(a)|}$$

1 iff  $a \in Z(G)$

$$= \sum_{\substack{a \in A/G \\ \text{rep.}}} \frac{|G|}{|C_G(a)|} \cdot$$

representatives  
of conj classes

$$= |Z(G)| + \sum_{\substack{a \text{ non-} \\ \text{central}}} \frac{|G|}{|C_G(a)|}$$

non-central  
elmt.



## Application

Theorem. Let  $G$  be a group of order  $p^2$ , where  $p$  is a prime. Then,  $G$  is Abelian.

(In fact,  $G \cong \mathbb{Z}/p \times \mathbb{Z}/p \cong \text{GL}(2, \mathbb{Z}/p)$ )

Proof:

$$p^2 = |G| = |Z(G)| + \sum_{a \text{ non-}a.l.} \frac{|G|}{|C_G(a)|}$$

We need to show free don't exist.

$$\frac{|G|}{|C_G(a)|} = \frac{b^2}{-} > 1$$

$\Rightarrow$  this is a multiple of  $b$

~~$b$  or  $b^2$~~

$$\Rightarrow b \mid |z(g)|$$

$$\Rightarrow |z(g)| = b \text{ or } b^2$$

If  $|z(g)| = b^2 \Rightarrow z(g) = g$   
 and  $G$  is Abeli. and  
 we are done.

Now suppose  $\{x(g)\} = p$ .

$$\{e\} \subset \mathcal{Z}(G) \subset F_G$$

$g \in G \quad \backslash \quad z(\zeta).$

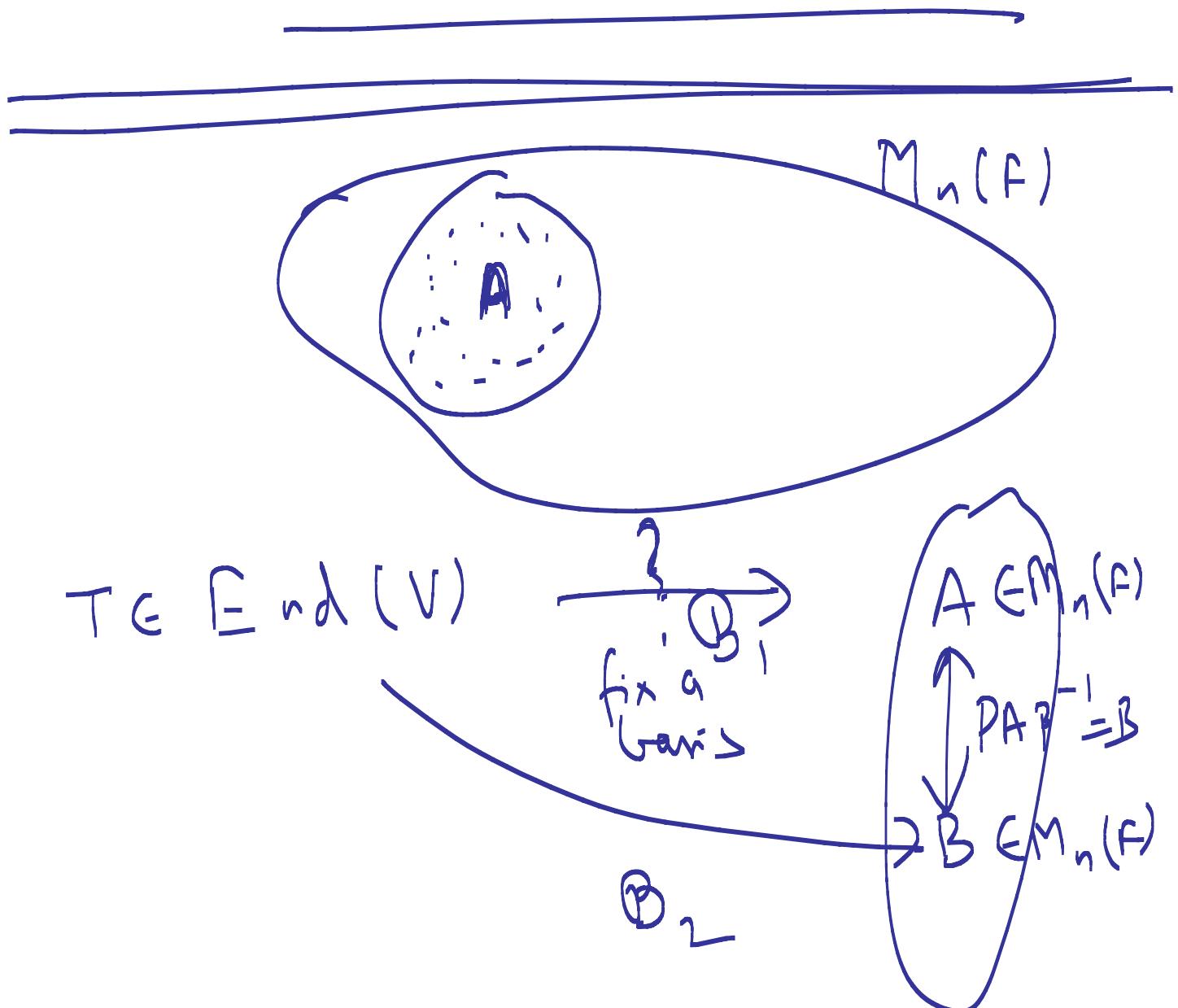
$$G \supset C_G(g) \quad \text{and} \quad z(G)$$

$$\Rightarrow |C_S(g)| = |G|$$

$$\forall g \in z(g) \Rightarrow \text{contradict..}$$

Hence  $\chi(G) = G$ .

Prove to the:



8 April 2021

Given a finite group.

① Can we classify all finite groups?

Direct answer No -

Can we get partial answer?

② Can we find some structural properties?

Question A

$G$  a finite group

$a \mid |G|$ . Does there exist  
a subgroup of size  $a$ ?

Answer # In general this is not  
true for any  $a$  by  $G$ .

# For any cyclic group or  
any Abelian grp answer is yes.

Question B  $p$  a prime,  $p \mid |G|$ .

Does  $\exists$  an element (e.g. a subgrp)  
of order  $p$  in  $G$ ?

Answer Yes, we will prove this.

In fact: Answer to Q(A) is  
yes if  $a \mid |G|$  and  $a = b^n$ , where  
 $n$  is largest.

---

### Sylow's Theorem-

---

Some definitions -

$G$  a finite group  
 $p$  a prime,  $p \mid |G|$ .

$|G| = p^n \cdot m$  where  $p \nmid m$ .

①  $\boxed{p\text{-group}}$  if  $|G| = p^n$  then  
 $G$  is said to be a  $p$ -group.

② If  $G$  has a subgp  
of order  $p^n$  then it is  
called a Sylow  $p$ -subgp.

③  $n_p$  = number of Sylow  
 $p$ -subgp of  $G$ .

---

$$\text{Ex} \quad |S_3| = 6 = 2 \cdot 3$$

How many subgp of order 2 ?

3 such subgp -

$$\{(1), (12)\}, \{(1), (13)\}, \{(1), (23)\}$$

$$\{(1), (12), (132)\} \rightarrow \text{Sylow } 3\text{-subgp.}$$

Theorem (Sylow's Theorem).

$G$  finite gp,  $p \mid |G|$   
 $|G| = p^n \cdot m$ ,  $p \nmid m$ .

Then,

(1) Sylow  $p$ -subgp exists.

(2) All Sylow  $p$ -subgps are conjugate (for fixed  $p$ ).

(3)  $n_p \equiv 1 \pmod{p}$

and  $n_p \mid \frac{|G|}{|N_G(p)|}$  hence,  $n_p \mid m$ .  
when  $P$  is a Sylow  $p$ -subgp.

~~Def~~  $H, K$  are subgps of  $G$ .

If  $\exists g \in G$  s.t  
 $g^{-1} H g = K$  then  
we say  $H$  &  $K$  are conjugate.

---

Examl. Suppose  $|G| = 6 = 2 \cdot 3$

$$2 \mid 6, \quad 3 \mid 6$$

① There is a Sylow 2-subgp of order 2.  
There is a Sylow 3 -                    3.

②  $p = 2$

$$n_2 \equiv 1 \pmod{2}, \quad n_2 \mid 3$$

$$n_2 = \checkmark, \checkmark, 5, 7, \dots$$

$$\Rightarrow n_2 = 1 \text{ or } 3.$$

$$p = 3$$

$$\frac{n_3}{n_3} \equiv 1 \pmod{3}, \quad n_3 \nmid 2.$$

$$n_3 = \cancel{1}, \cancel{2}, \cancel{3}, \dots$$

$\Rightarrow n_3 = 1$  c.e. Sylow 3-subp  
is unique., Call it  $K$ .

$$\Rightarrow N_G(K) = \{g \in G \mid gKg^{-1} = K\}$$

$\Rightarrow$  Sylow 3-subp is normal.

Conclusion.  $|G| = 6$ .

---

① It has a unique normal  
subp of order 3.  
i.e.  $n_3 = 1$

(ii)

$$n_2 = 1 \quad \text{or} \quad n_2 = 3$$

That is,  $G$  has two chains, at most.

$$|H| = 2, \quad |K| = 3$$

$$H K = G.$$

---

$$n_2 = 1, n_3 = 1$$

$H$  is not.

$$G = H \times K$$

$$\cong 2/2 \times 2/3 \cong 2/6$$

$$n_2 = 3, n_3 = 1$$

$$G \cong S_3$$

---

Then       $G$  finite Abelian  $\Leftrightarrow$   
 $b \mid |G|$ .       $b$  - prim.

Then,  $G$  has an element of  
order  $b$ .

Proof:  $\underline{\underline{G = \langle z \rangle}}$  cyclic

Then, generators of  $G$  are  $z^d$  s.t.  
 $(d, |G|) = 1$

$\therefore \langle z^k \rangle$  where  $(k, |G|) \neq 1$   
it's a proper subgp.

$a = z^{\frac{|G|}{b}}$  is an elemt of order  $b$ .

Case 2       $|G| = p$  is Case 1

Take       $|G| > p$ .

If  $G$  has an elemt  $x$

$s + b \mid o(x) \text{ in}$   
 Case (1) splitting to  $\langle x \rangle$   
 gives us the required elt.

Case 3:  $1+x \in G$   
 and  $b + o(x) \text{ for } n$ .  
 $N = \langle x \rangle$ ,  $N$  is a  
 normal subgp of  $G$ .

$G/N$  is a gp of order  $\frac{|G|}{|N|}$ .

induction on  $G/N$  gives us  
 an elt  $yN \in G/N$  of order  $p$ .

(since  $b \mid \frac{|G|}{|N|}$ , hence  $b + |N|$ ).

$$\Rightarrow (yN)^p = N$$

$$\Rightarrow y^p \in N . \quad y \in G \setminus N$$

$$\langle y^p \rangle \subset \underset{\uparrow}{\text{F}} \quad \langle y \rangle \subset G .$$

$$p \mid o(y) \neq \in \text{a contradiction.}$$

This proves the theorem.

---

13 April 2021

## Sylow's Theorem.

$G$  a finite group.

$p$  a prime s.t.  $p \mid |G|$ .

$$|G| = p^n \cdot m, p \nmid m$$

Then,

- (1) There exist a subgroups of  $G$  of order  $p^n$ . (Another way to say this,  $\exists$  Sylow  $p$ -subgroup).
- (2) All Sylow  $p$ -subgroups (for fixed  $p$ ) are conjugate.
- (3)  $n_p \equiv 1 \pmod{p}$ .

Proof of (1) :

Proof is by induction on  $|G|$ .

Hypothesis: Let  $G$  be a group of order  $|G|=2$ . Let  $p \mid 2$ ,  $p$  prime.  
Then  $G$  has a Sylow  $p$ -subgroup.  
(This happens for any prime  $p$ ).

If  $|G|=1$  then this is true.

If  $|G|=2$  the only possible  $p$  is 2.

In this case  $G$  itself is Sylow 2-subgroup.

Now we assume that hypothesis is true for all groups  $H$  s.t.  $|H| < 2$

and all primes dividing  $|H|$ .

To Show:  $G$  a gp.  $|G| = p^n$   
 $p \nmid n$ , prime. Then  $G$  has  
Sylow  $p$ -subgp.

$C := Z(G)$  center of  $G$ .

Case 1:  $p \mid |C|$

$C = Z(G)$  is an Abelian subgp.  
 $C$  has an element of order  $p$ .

Take,  $D$ , as the subgp generated  
by that element.  $|D| = p$ .

Since  $D \subset C \subset G$ ,  $D$  is  
a normal subgp.

$$\text{Take } G/D, \quad |G/D| = \frac{p^m}{p} \\ = p^{m-1}$$

$G/D$  has a Sylow  $p$ -subgroup of order  $p^{m-1}$ .

$$G \rightarrow G/D \text{ surj.}$$

$$H \hookrightarrow H/D$$

$$G \supset H \supset D$$

Let  $P/D$  be the Sylow  $p$ -subgroup of  $G/D$  of order  $p^{m-1}$ .

$$D \subset P \subset G$$

$$|P| = |P/D| \cdot |D| = p^{m-1} \cdot b = p^m$$

$P$  is a required Sylow  $p$ -subgp  
of  $G$ .

Case 2       $p \nmid |C|$ .

$$X = G \setminus C$$

$G$  acts on  $X$  by conjugation.

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\mapsto g^{-1}xg \end{aligned}$$

$X$  is union of conjugacy classes  
of  $G$  of size  $> 1$ .

$$x = \text{cl}_{n_1} \cup \text{cl}_{n_2} \cup \dots \cup \text{cl}_{n_k}$$

$$|\text{cl}_{x_i}| > 1$$

$$\frac{|G|}{|\text{cl}_{x_i}|} \quad (\Rightarrow) \quad |\text{cl}_{x_i}| < |G| \\ \equiv$$

$$|G| = |G \setminus C| + |C|$$

$$b(|G|, \overset{\text{"}}{|x|}) \quad \text{if } b(|x| \Rightarrow b(|C|))$$

$\models$

$$\Rightarrow b + |x|$$

i.e.  $\exists x_i \text{ s.t. } b + |\text{cl}_{x_i}|$

$$H = C_G(u) \overbrace{\subset G}$$

(i)  $H \subsetneq G$

(ii)  $p^n \mid |H|$ .  $\frac{|G|}{|H_{\text{rel}}|}$

$$|H| = p^n \cdot m' < |G|$$

induction hypothesis applied to  $H$

$\Rightarrow H$  has a Sylow  $p$ -subgp

of size  $p^n$ .

$\Rightarrow$  The same Sylow  $p$ -subgp  
is Sylow  $p$ -subgp of  $G$ .

This proves the Theorem.

$$H = C_G(x)$$

$$|H| = |G| / [G : \underline{C_G(x)}]$$

$$\text{But } |G| |C_G(x)| = \frac{|G|}{|C_G(x)|}$$

However

$$|G| = p^n$$

$|G| = p_1^{n_1} p_2^{n_2} \dots$   
 G has  $p$  resp.  
 subgrp.

Def. p a prime.

A Group G is said to be a p-group if  $|G| = p^n$  for some n.

Theorem (for  $p$ -groups)

$G \times \mathbb{F}_p^n$  of order  $p^r$ ,  $b$  apart.

Then,

① The center of  $G$  is non-trivial.

c.c.  $|Z(G)| > 1$ .

②  $G$  has a subgp of order  $p^s$   
for all  $s$ ,  $0 \leq s \leq r$ .

③ If  $G$  acts on  $X$ , then,

$$|X| \equiv |X^G| \pmod{p}$$

where  $X^G$  is the set of fixed  
points.

④  $|Z(G)| \equiv 0 \pmod{p}$ .

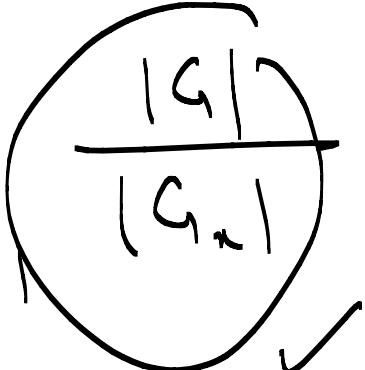
Part.

③

Apply orbit-stab. The.

$$|x| = |x^G| + \sum_{|G_n| > 1} (O_n)$$

$$= |x^G| + \sum_{|G_n| < |G|}$$



$$G_n < G$$

$$b \mid \frac{|G|}{|G_n|}$$

$$|x| = |x^G| \bmod p$$

④

Take  $x = G$  and action

by conjugate

$$O = |G| = |\pi(G)| \bmod p$$

①  $e \in z(G)$

$$\Rightarrow |z(G)| \geq 1$$

$$\nexists |z(G)| > 1.$$

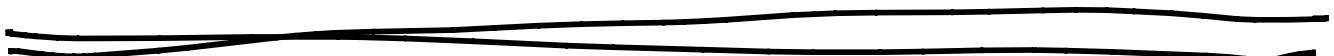
②  $b \mid |z(G)|$ ,  $x \in z(G)$   
upadm b.

$$D = \langle x \rangle$$

$$G \rightarrow G|D$$

$$G \supset H \supset D \hookrightarrow H|D$$

Indukt. gives to rem<sup>ht</sup>.



$G$  a group.  $c \in N$  normal in  $G$   
 $N \trianglelefteq G$ .

$$G \rightarrow G/N$$

$$g \mapsto gN$$

Questi- what are the subps of  
 $G/N$ .

$$\left\{ H \mid \begin{array}{l} H \text{ subp of } G \\ H > N \end{array} \right\} \xleftrightarrow{\text{1-1 Corresp.}} \begin{array}{l} \text{subps of } G/N \\ H \mapsto H/N \end{array}$$

$\pi \in \mathbb{Z}(G)$   
 $\pi$  of order  $p$

$$D = \langle \pi \rangle$$

$$|D| = p$$

$$G \rightarrow G/D \rightarrow \mathbb{Z}_p^{n-1}$$

$H/D$  of ord  $p^{n-1}$

$$|H| = |H(D) \cdot (D)| = p^{8-1} \cdot p = p^8$$

15 April 2021

## Sylow's Theorem (2)

$G$  finite group-

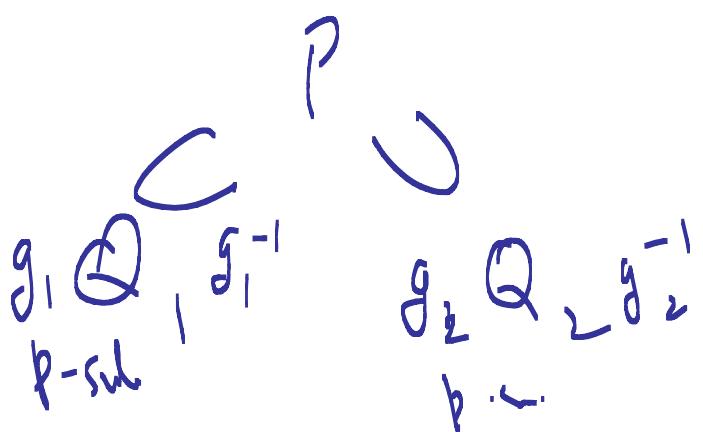
$p$  prime (fix)  
 $p \mid |G|$

$|G| = p^n \cdot m$ ,  $p \nmid m$ . Let  $P$  be a Sylow- $p$ -subgp.  
Let  $Q$  be any  $p$ -subgp of  $G$ . Then.

there exists  $g \in G$  s.t.

$$Q \subset g P g^{-1}.$$

Proof.  $P$  a Sylow  $p$ -subgrp of  $G$ .



$$X = G/P = \{aP \mid a \in G\}$$

$$\begin{array}{ccc} Q & \times & X \\ (g, aP) & \mapsto & (ga)P \end{array}$$

This is an action.

Recall the theorem about  $\mathbb{Z}$ -groups acting on a set.  $\Rightarrow$

$$|X| \equiv |X^Q| \pmod{p}$$

↑↑      ↗      ↘

①

$$|X| = \frac{|G|}{|P|} \quad p \nmid \frac{|G|}{|P|} = n$$

$$\Rightarrow |X^Q| \not\equiv 0 \pmod{p}.$$

$\Rightarrow Q$  has at least one fixed point on  $X$ , say,  $a_0 P$ .

$$q \cdot a_0 P = a_0 P \neq q \in Q$$

$$\Rightarrow q_0^{-1} q a_0 \in P \neq q \in Q$$

$$\Rightarrow Q \subset a_0 P a_0^{-1}.$$

This proves the theorem.

---

$P_1, P_2$  are  $\exists g$  s.t.

$$P_1 \subset g P_2 g^{-1}$$

$$\text{Since } |P_1| = |P_2| = |g P_2 g^{-1}|$$

$$\Rightarrow P_1 = g P_2 g^{-1}.$$

---

Before proving Sylow's (3) we  
need a lemma.

Lemma: Let  $P$  be a Sylow  $p$ -subgp  
 $\nsubseteq G$ . Let  $Q$  be any  $p$ -subgp.

Then,  $Q \cap N_G(P) = Q \cap P$ .

---

### Sylow's Theorem (3)

$n_p :=$  number of Sylow  $p$ -subgps  
 $\nsubseteq G$ .

Then, (i)  $n_p \equiv 1 \pmod{p}$ .

(ii)  $n_p = \frac{|G|}{|N_G(P)|}$  when  $P$  is  
a Sylow  $p$ -subgp  
 $\Rightarrow n_p \mid m$ .

Proof. (i) Let  $P$  be a Sylow- $p$ -subgroup of  $G$ .

$$X = \{P_i^{g, P} \mid P_i \in \dots, P_{n_p}\}$$

$$\begin{array}{ccc} P & \times & X \\ (g, P_i) & \mapsto & gP_i g^{-1} \end{array}$$

this is an action.

Since  $P$  is a  $p$ -group,

$$n_p = |X| \equiv |\{x^P \mid \text{mod } p\}|$$

$$\begin{aligned} X^P &= \{P_i \mid gP_ig^{-1} = P_i \ \forall g \in P\} \\ &= \{P_i \mid P \subset N_G(P_i)\} \end{aligned}$$

$\stackrel{?}{=}$   $\{ P_i = P \}$   
 This follows from the lemma.

$$P_i = P, \quad P_i \text{ and } g \in N_G(P_i)$$

$$\Rightarrow P_i \subset P_i \cap N_G(P_i) = P_i \cap P_i$$

$$\Rightarrow P_i \subset P_i \Rightarrow P_i = P_i$$

$$\Rightarrow n_p \equiv 1 \pmod{p}.$$


---

$$G \times X \longrightarrow X$$

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

Since all Sylow p-subgroups are conjugate, this action is

transitive (single orbit).

$$|X| = \frac{|G|}{|G_P|} = \frac{|G|}{|N_G(P)|}$$

" "



Part of Lemma -

Result

$\{Q\}$  a sylow  $p$ -subgrp. }  
 $\{Q\}$  any  $p$ -subgrp. }

Then,  $Q \cap N_G(P) = \underline{Q \cap P}$ .

Part:

$$H := Q \cap N_G(P)$$

~~Easy~~  $P \cap Q \subset H$  ?

Since  $\varnothing \subset N_G(P)$

$P \cap Q \subset N_G(P) \cap Q := H$

To show

$H \subset P \cap Q$

But

$H \subset Q$

thus, we require to prove  $H \subset P$ .

Claim:  $P|H$  is a  $\overline{p}$ -subgp of  $G$ .

$\{\overline{ph} \mid b \in \mathbb{Z}, h \in H\}$

• Subgp because because  $H \subset N_G(P)$ .

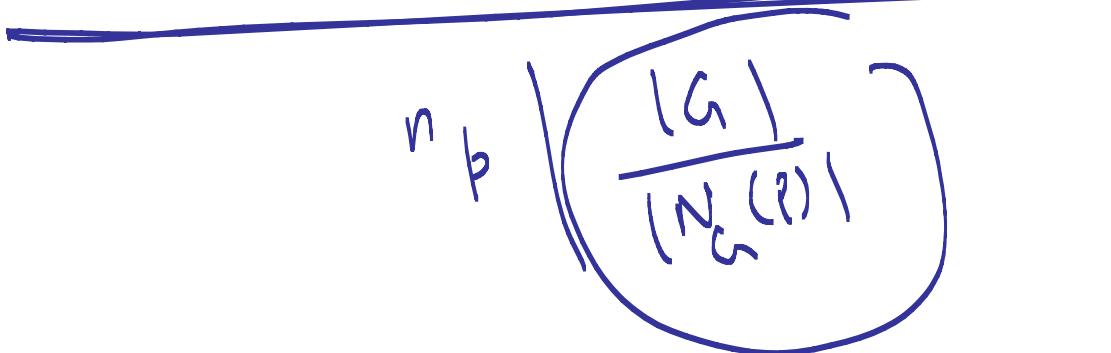
•  $|P|H| = \frac{|P \xrightarrow{f} f(H) \xrightarrow{f} \overline{P}|}{|P \cap H|}$

•  $P|H \supseteq P$

$\boxed{\frac{|P|H| = b^2}{|P|H|}}$

Since  $P$  is a Sylow  $p$ -subgp  
it has largest size among  
 $p$ -subgps.

$$\Rightarrow P \trianglelefteq H \cap P$$



$$\frac{p^n \cdot m}{p^n \cdot s} = \frac{m}{s}$$

# Symmetry via Group Actions

some concrete applications

Anupam Singh

IISER, Pune

*email : anupam@iiserpune.ac.in*



# **Symmetry $\iff$ Groups are ubiquitous**

- Groups are symmetries of an artistic object.
- Groups are fundamental to engineering.
- Groups are tool to explore science.
- Recall: group, and group acting on a set.

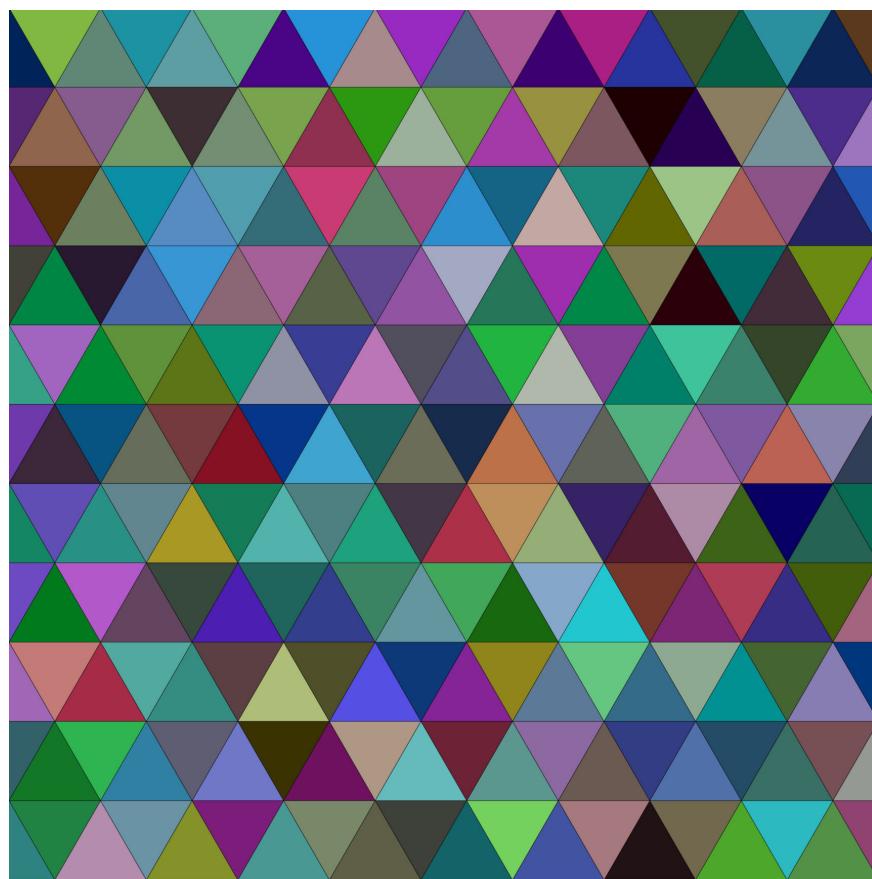
# Symmetry - Tiling of the plane

## Theorem

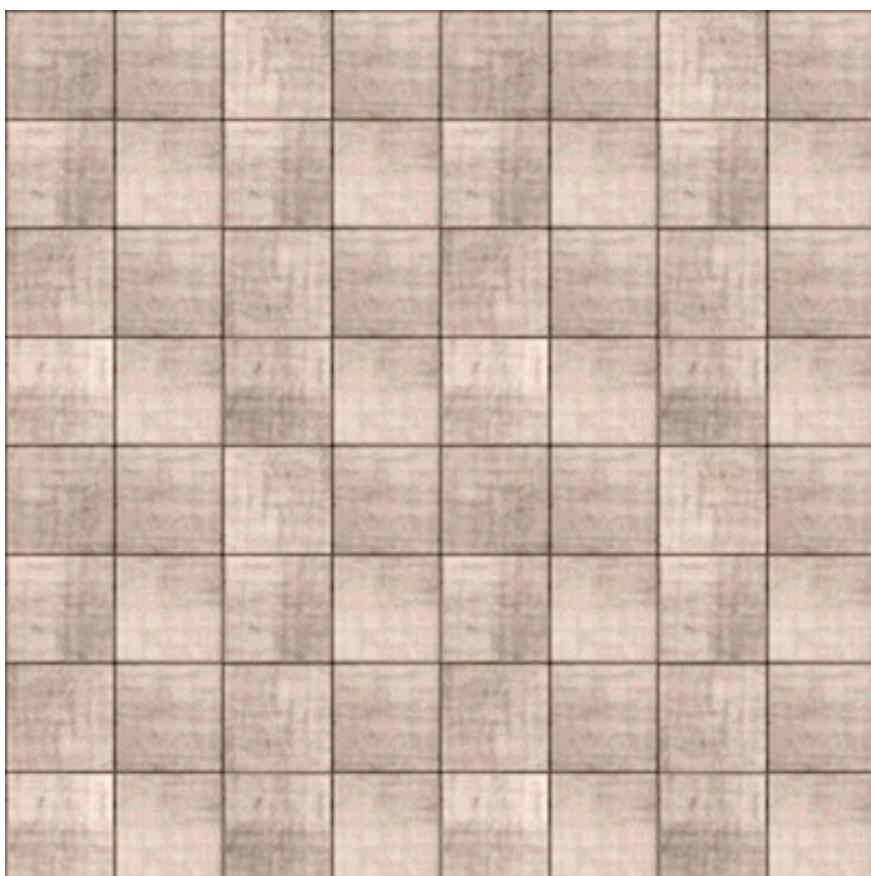
*Only possible  $n$ -gons used to tile the plane, which can fill the whole plane, correspond to  $n = 3, 4$  and  $6$ .*



# Triangular Tiling



# Square Tiling

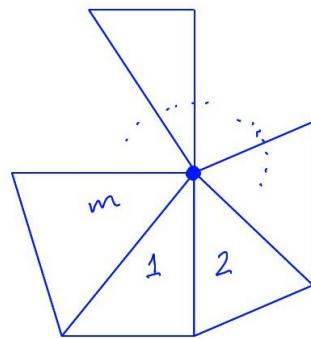


# Hexagon Tiling



## Tiling of the plane

- We fill the plane with tiles which are  $n$ -gons. Let us say  $m$  of them meet at a corner.

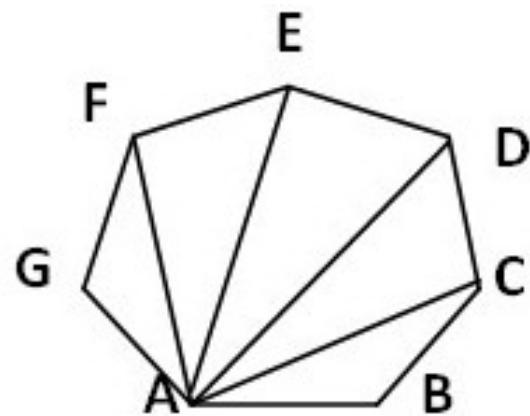


- Tiling condition

$$m \times (\text{Internal angle of } n\text{-gon}) = 2\pi.$$

## Tiling of the plane

- Internal angle of an  $n$ -gon =  $\frac{(n-2)\pi}{n}$ .



- Thus tiling condition,  $m \cdot \frac{(n-2)\pi}{n} = 2\pi$ .

## Tiling of the plane

- Simplifying  $m \cdot \frac{(n-2)\pi}{n} = 2\pi$  gives the equation

$$\frac{1}{n} + \frac{1}{m} = \frac{1}{2}.$$

- Notice the practical condition  $m, n \geq 3$ .
- If either  $n$  or  $m$  is  $\geq 7$  then

$$\frac{1}{n} + \frac{1}{m} \leq \frac{1}{7} + \frac{1}{3} = \frac{10}{21} = .476\dots < \frac{1}{2}.$$

## Tiling of the plane

All possible integer solutions of

$$\frac{1}{n} + \frac{1}{m} = \frac{1}{2}$$

with  $n, m \geq 3$ , are

$$(n, m) = (3, 6), (4, 4), (6, 3).$$

This proves the Theorem.

## What is a symmetry?

- Symmetry is a motion of the plane (an isometry of the plane) which leaves the object invariant!
- Clearly, tiling of a plane has **translational** symmetry. It also has some symmetries coming from that of a individual tile type.
- Thus, we need to look at symmetries of an  $n$ -gon,  $\Delta_n$ , explicitly.

## What measures symmetry?

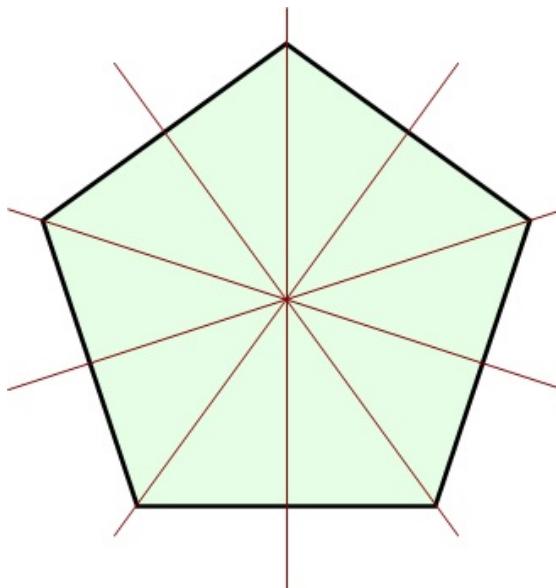
- Given an  $n$ -gon, call it  $\Delta_n$ , we associate symmetry group.

## What measures symmetry?

- Given an  $n$ -gon, call it  $\Delta_n$ , we associate symmetry group.
- More symmetries, the more symmetric an object is!

## What measures symmetry?

- Given an  $n$ -gon, call it  $\Delta_n$ , we associate symmetry group.
- More symmetries, the more symmetric an object is!



- No Translations, 5 Rotations (by multiples of  $\frac{2\pi}{5}$ ) and 5 Reflections.

## What is more symmetric?

- Number of symmetries could be taken as a measure of symmetry.

## What is more symmetric?

- Number of symmetries could be taken as a measure of symmetry.
- Type of symmetries: Translation, Reflection and Rotation and their combinations.

## What is more symmetric?

- Number of symmetries could be taken as a measure of symmetry.
- Type of symmetries: Translation, Reflection and Rotation and their combinations.
- The symmetries of  $\Delta_n$  is the Dihedral group with  $2n$  elements. Why?

## What is more symmetric?

- Number of symmetries could be taken as a measure of symmetry.
- Type of symmetries: Translation, Reflection and Rotation and their combinations.
- The symmetries of  $\Delta_n$  is the Dihedral group with  $2n$  elements. Why?
- It has a rotational symmetry  $\rho_{\frac{2\pi}{n}}$ , and all its powers.
- It has reflection symmetries.

# Symmetry mathematically !!

- $\text{Symm}(\Delta_n) = \{\phi \in \text{Isometry}(\mathbb{R}^2) \mid \phi(\Delta_n) = \Delta_n\} \cong D_{2n} = \{r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1}\}$ , the Dihedral group with  $2n$ -elements. ??

## Symmetry mathematically !!

- $\text{Symm}(\Delta_n) = \{\phi \in \text{Isometry}(\mathbb{R}^2) \mid \phi(\Delta_n) = \Delta_n\} \cong D_{2n} = \{r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1}\}$ , the Dihedral group with  $2n$ -elements. ??
- The orthogonal group  $O(2)$  is at work here.

$$O(2) = SO(2) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . SO(2)$$

where

$$SO(2) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid 0 \leq \theta < 2\pi \right\}.$$

- What is symmetry of the circle?

## Symmetry of $\Delta_n \cong D_{2n}$

- $G := Symm(\Delta_n)$ ,  $D_{2n} \subset G$ , and  $Iso(\mathbb{R}^2) = \mathbb{R}^2 \ltimes O(2)$ .
- Translations do not keep  $\Delta_n$  to itself, implies,  $G \subset O(2)$ .
- $O(2)$  acts on  $\Delta_n$ , and we know,  $D_{2n} \subset G = Symm(\Delta_n)$ .
- $G$  acts transitively on the vertex set  $X_n$  of  $\Delta_n$ . Thus,  
 $|X_n| = \frac{|G|}{|G_v|}$  where  $G_v$  is the stabiliser of one of the verticies, say  $v$ .
- We claim that  $|G_v| = 2$ , given by a reflection. Any element of  $O(2)$  fixing the vertex  $v$ , will fix the line passing through  $v$  and origin, and hence its a reflection.
- Thus,  $|G| = |X_n| \cdot |G_v| = 2|X_n| = 2n$ . Hence,  $G = D_{2n}$ .

## Wall paper group

- A wall paper is infinite tiling of plane with shaded  $n$ -gons.
- The wall paper group contains two independent translations and a finite point group.
- It is a subgroup of  $Iso(\mathbb{R}^2)$ .
- There are 17 wall paper groups. (see Armstrong Chapter 25, 26.) If you are interested in exploring this topic further you should read about Wallpaper groups. The book by Armstrong titled "Groups and Symmetry" is a good source for this topic.

## Three dimensional objects



# Platonic Solids

- The 3-dimensional regular (convex) objects are made of using the  $n$ -gons, called Platonic solids.

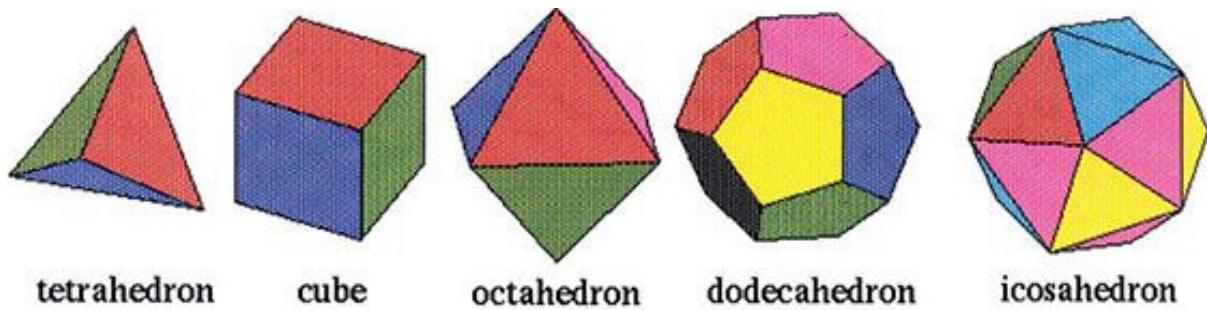
## Platonic Solids

- The 3-dimensional regular (convex) objects are made of using the  $n$ -gons, called Platonic solids.
- There are only FIVE Platonic solids: Tetrahedron, Cube, Octahedron, Dodecahedron, and Icosahedron.

## Platonic Solids

- The 3-dimensional regular (convex) objects are made of using the  $n$ -gons, called Platonic solids.
- There are only FIVE Platonic solids: Tetrahedron, Cube, Octahedron, Dodecahedron, and Icosahedron.
- Demo of models!!!  
See my talk for school children on YouTube channel of IISER Pune Science Activity Center titled "Visualising symmetry through mathematics".  
<https://youtu.be/CcLuv0B7ne8>

# Platonic Solids



## Platonic Solids - mathematical proof

- These correspond to the condition (we want to fold in such way that the resulting object is convex):

$$m \cdot \frac{(n-2)\pi}{n} < 2\pi$$

which gives the equation

$$\frac{1}{n} + \frac{1}{m} > \frac{1}{2}.$$

- All possible integer solutions with  $n, m \geq 3$  are

$$(n, m) = (3, 3), (3, 4), (3, 5), (4, 3), (5, 3).$$

# Classification of Isometries of an Euclidean Space

## Part - II

# Classification of Isometries

## Theorem

*Every isometry of an Euclidean space is a composition of translation and orthogonal transformation (which are composition of reflection and generalised rotation).*

The aim is to make these terminologies concrete and prove this theorem.



# Euclidean Space

The **Euclidean space**  $\mathbb{E}^n = (\mathbb{R}^n, d)$  is a metric space with the distance function

$$d(x, y) := \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

where  $x = (x_1, \dots, x_n)$  and  $y = (y_1, \dots, y_n)$ .

we take  $n \geq 2$ . . Recall the properties of a distance function (for all  $x, y, z \in \mathbb{R}^n$ ):

1.  $d(x, y) \geq 0$ ; and  $d(x, y) = 0 \iff x = y$ .
2.  $d(x, y) = d(y, x)$ .
3.  $d(x, y) \leq d(x, z) + d(z, y)$  (called Triangle inequality).

## What's an Isometry

An **isometry** of Euclidean space is a map on  $\mathbb{R}^n$

$$f : \mathbb{R}^n \rightarrow \mathbb{R}^n \text{ such that}$$
$$d(f(x), f(y)) = d(x, y) \text{ for all } x, y \in \mathbb{R}^n.$$

$Iso(\mathbb{E}^n)$  (or simply  $Iso(\mathbb{R}^n)$ ) is the set of all isometries.

We will prove that isometries are bijection and  $Iso(\mathbb{R}^n)$  is a group.



## Examples of isometry: Translation

Fix  $a = (a_1, \dots, a_n) \in \mathbb{R}^n$ , and define translation by  $a$  as follows:

$$\begin{aligned}\tau_a &: \mathbb{R}^n \rightarrow \mathbb{R}^n \\ \tau_a(x) &= x + a = (x_1 + a_1, \dots, x_n + a_n).\end{aligned}$$

Check  $d(\tau_a(x), \tau_a(y)) = d(x, y)$ .

Thus, translations are isometry but not a linear map if  $a \neq 0$ .

# Orthogonal Linear Transformations



## Symmetric Bilinear Form

- Let  $V$  be a vector space over  $k$ .
- $B: V \times V \rightarrow k$  is a bilinear map which is linear in both coordinate.
- $B$  is symmetric if  $B(x, y) = B(y, x)$  for all  $x, y \in V$ .
- On  $\mathbb{R}^n$  we have a SPECIAL symmetric bilinear form given by

$$B(x, y) := \sum_{i=1}^n x_i y_i = x_1 y_1 + \cdots + x_n y_n.$$

## Normed Vector Space

- We have **norm** on the vector space  $\mathbb{R}^n$  given by

$$\|x\| := \sqrt{x_1^2 + \cdots + x_n^2}.$$

$B_N(v, w) = \frac{N(v+w) - N(v) - N(w)}{2}$  is bilinear.

- The norm and symmetric bilinear form are related and can be obtained from each other.

$$\|x\| = \sqrt{B(x, x)}, \quad B(x, y) = \frac{\|x+y\|^2 - \|x\|^2 - \|y\|^2}{2}.$$

- The norm and distance are also related

$$d(x, y) = \|x - y\|.$$

# Orthogonal Linear Transformation

## Definition

A linear transformation  $S: \mathbb{R}^n \rightarrow \mathbb{R}^n$  is called **orthogonal** if

$$B(S(x), S(y)) = B(x, y), \quad \forall x, y \in \mathbb{R}^n.$$

The following are equivalent for a linear transformation  $S: \mathbb{R}^n \rightarrow \mathbb{R}^n$ :

1.  $S$  is orthogonal.
2.  $S$  is an isometry.
3.  $\|S(x)\| = \|x\|$  for all  $x \in \mathbb{R}^n$ .

# Orthogonal Linear Transformation

The following are equivalent for a **linear transformation**  
 $S: \mathbb{R}^n \rightarrow \mathbb{R}^n$ :

1.  $S$  is orthogonal.
2.  $S$  maps an orthonormal basis to an orthonormal basis.
3. The matrix  $A$  of  $S$  with respect to the standard basis satisfies  ${}^tAA = I$ . (That is, if we think of rows (or columns) of  $A$  as vectors in  $\mathbb{R}^n$ , then they form an orthonormal basis.)

## Examples of isometry: orthogonal

**Linear + Isometry = Orthogonal**

Can we write some orthogonal linear transformations explicitly?

## The orthogonal group

The **orthogonal group**  $O(n)$  is the set of all orthogonal linear transformations.

In the matrix form (with respect to the fixed standard basis)

$$O(n) := \{A \in M_n(\mathbb{R}) \mid {}^t A A = I\}.$$

The special orthogonal group (also called rotation group) is

$$SO(n) := \{A \in O(n) \mid \det(A) = 1\}.$$

# Some properties of the orthogonal group

For  $A, B \in O(n)$ :

1.  $\det(A) = \pm 1$ .
2.  $AB \in O(n)$  and  $A^{-1} \in O(n)$ . (Hence  $O(n)$  is a group.)
3. Fix,  $s \in O(n)$  with  $\det(s) = -1$ , then

$$O(n) = SO(n) \bigcup s.SO(n).$$

Why such an  $s$  exist?



## Linear isometries of Plane, $n = 2$ case

- $O(2) = SO(2) \cup s.SO(2)$  where  $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ .
- $SO(2) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid 0 \leq \theta < 2\pi \right\}$ .
- Elements of  $s.SO(2)$  are reflections.
- Elements of  $SO(2)$  are rotations.

## Examples of Isometry: Reflections

- Fix a non-zero vector  $v \in \mathbb{R}^n$ .
- Define a map  $r_v: \mathbb{R}^n \rightarrow \mathbb{R}^n$  by

$$r_v(x) = x - 2 \frac{B(x, v)}{\|v\|^2} v.$$

- $r_v$  is a linear orthogonal transformation and  $r_v^2 = 1$ .
- $r_v(v) = -v$  and  $r_v(w) = w$  if  $w \perp v$ .
- Thus, the fixed  $(n - 1)$  dimensional hyperplane  $v^\perp$  acts like a mirror.

## Examples of Isometry: Rotation in a 2D-plane

- Fix  $\theta \in [0, 2\pi)$  and fix  $1 \leq l \leq n - 1$ .
- Define  $\rho_{l,\theta} : \mathbb{R}^n \rightarrow \mathbb{R}^n$  by

$$\begin{aligned}\rho_{l,\theta}(e_l) &= \cos(\theta)e_l - \sin(\theta)e_{l+1}, \\ \rho_{l,\theta}(e_{l+1}) &= \sin(\theta)e_l + \cos(\theta)e_{l+1}, \\ \rho_{l,\theta}(e_i) &= e_i, \text{ for } i \neq l, l+1.\end{aligned}$$

- Then  $\rho_{l,\theta}$  is a linear isometry, that is, an orthogonal linear transformation.

## Theorem: Classifying elements of $O(n) - SO(n)$

For any fixed reflection  $s$ , every element of  $O(n)$  which is not in  $SO(n)$  is of the form  $s.t$  where  $t \in SO(n)$ .

Warning: In general, these may not be reflection unlike  $n = 2$  case. For example, they have elements of the following form with odd number of  $-1$ :

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \\ & & & & \ddots & \\ & & & & & -1 \end{pmatrix}$$

## Theorem: Classifying elements of $SO(n)$

Every special orthogonal linear transformation, the elements of  $SO(n)$ , up to conjugacy is a composition of 2-dimensional rotations. That is, given  $\tau \in SO(n)$ , there exists a basis of  $\mathbb{R}^n$  such that the matrix of  $\tau$  is as follows:

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \rho_1 \\ & & & & \ddots & \\ & & & & & \rho_l \end{pmatrix}$$

where  $\rho_i$ s are 2-dimensional rotation matrices.

# Classification of isometries and the Isomtery group



# Classification of isometries

## Theorem

Let  $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$  be an isometry. Show that,

$$f(x) = T(x) + a$$

that is,  $f = \tau_a T$  where  $a = f(0)$  and  $T \in O_n(\mathbb{R})$ .

This also proves that every isometry is a bijection.

# Isometry with $(n + 1)$ fixed points

## Lemma

Let  $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$  be an isometry. Suppose  $T$  fixes origin and each of the standard basis vectors, i.e.,  $T(0) = 0$  and  $T(e_i) = e_i \forall i$ . Then  $T$  is identity.

## Proof:

- Let  $x = (x_1, \dots, x_n)$  and  $T(x) = y = (y_1, \dots, y_n)$ .
- We want to prove  $y = x$ .
- We are given that  $T$  is an isometry, i.e., preserves distance.

## Isometry with $(n + 1)$ fixed points

- $d(0, x) = d(T(0), T(x)) = d(0, y) \implies \|x\| = \|y\|.$
- $d(x, e_i) = d(T(x), T(e_i)) = d(y, e_i) \implies \|x - e_i\| = \|y - e_i\|.$
- This gives the equation

$$\begin{aligned} x_1^2 + \cdots + x_{i-1}^2 + (x_i - 1)^2 + x_{i+1}^2 + \cdots + x_n^2 \\ = y_1^2 + \cdots + y_{i-1}^2 + (y_i - 1)^2 + y_{i+1}^2 + \cdots + y_n^2 \end{aligned}$$

- This gives  $x_i = y_i$  for all  $i$ . This proves the required result.

# Isometry fixing origin

## Lemma

Let  $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$  be an isometry. Suppose  $T$  fixes origin. Then  $T$  is an orthogonal **linear** transformation.

## Proof:

- Consider a matrix  $S$  of which columns are  $y_i = T(e_i)$ .
- Then  $S$  defines a linear map  $S: \mathbb{R}^n \rightarrow \mathbb{R}^n$  with the property  $S(e_i) = y_i = T(e_i)$  for all  $i$ .
- We claim that  $S$  is an orthogonal linear transformation.

## Isometry fixing origin

Recall:

$$d(x, y)^2 = \|x - y\|^2 = B(x - y, x - y) = \|x\|^2 + \|y\|^2 - 2B(x, y).$$

This gives,

$$2B(x, y) = \|x\|^2 + \|y\|^2 - \|x - y\|^2.$$

Hence using  $T(0) = 0$ ,

$$\begin{aligned} 2B(T(x), T(y)) &= \|T(x)\|^2 + \|T(y)\|^2 - \|T(x) - T(y)\|^2 \\ &= \|T(x) - T(0)\|^2 + \|T(y) - T(0)\|^2 - \|T(x) - T(y)\|^2 \\ &= d(T(x), T(0))^2 + d(T(y), T(0))^2 - d(T(x), T(y))^2 \\ &= d(x, 0)^2 + d(y, 0)^2 - d(x, y)^2 \quad \text{since } T \text{ is an isometry} \\ &= \|x\|^2 + \|y\|^2 - \|x - y\|^2 = 2B(x, y). \end{aligned}$$

## Isometry fixing origin

- We use this to verify that  $\{y_1, \dots, y_n\}$  is an orthonormal basis, thus  $S$  maps an orthonormal basis to an orthonormal basis.
- Now let us consider the map  $S^{-1}T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ .
- $S^{-1}T$  is an isometry which fixes origin and all of the  $e_i$ .
- Hence from previous Lemma it must be the identity map.
- That is,  $S^{-1}T = Id$  implies  $T = S$ . Proves the Lemma.

## Proof of the main Theorem

- Let  $a = f(0)$ .
- Consider the map  $\tau_{-a}f$  which is an isometry.
- Clearly  $(\tau_{-a}f)(0) = \tau_{-a}(f(0)) = f(0) - a = 0$ .
- Thus, from previous Lemma,  $\tau_{-a}f$  is a linear orthogonal transformation. Say  $\tau_{-a}f = T \in O_n(\mathbb{R})$ .
- Hence,  $f = \tau_a T$ .

## Isometry group

- Now we can talk about Isometry group  $Iso(\mathbb{R}^n)$ .
- Let  $f, f'$  be isometries given by  $f(x) = Ax + a$  and  $f'(x) = A'x + a'$ . Then,

$$(ff')(x) = AA'x + (Aa' + a).$$

- Every isometry is one-one and onto map.
- $Iso(\mathbb{R}^n)$  is closed under composition.
- $f^{-1}(x) = A^{-1}x - A^{-1}a$ .
- Thus,  $Iso(\mathbb{R}^n)$  is a group.

## Return to Symmetries of objects



## Application : Symmetries

- Let  $\Delta$  be a subset of  $\mathbb{E}^n$ .
- $Sym(\Delta) := \{f \in Iso(\mathbb{E}^n) \mid f(\Delta) = \Delta, f|_{\Delta} \text{ is a bijection}\}$ .
- $Sym(\Delta)$  is a group.
- We have computed symmetries of  $n$ -gon in plane. Now we compute the same for Platonic solids in 3 dimensional space.

## 3 dimensional orthogonal group

- $O(3) = SO(3) \cup s.SO(3)$  where  $s = \begin{pmatrix} 1 & & \\ & 1 & \\ & & -1 \end{pmatrix}$ .
- Elements of  $s.SO(3)$  contain reflections and elements of  $SO(3)$  are rotation.
- Every element of  $SO(3)$  has a fixed axis, i.e., 1 is an eigen value.

## Rotation in 3D

**Proof:** Let  $A \in SO(3)$  and  $\lambda_1, \lambda_2, \lambda_3$  be complex eigen-values of  $A$  such that  $\lambda_1\lambda_2\lambda_3 = 1$ . We use the following two facts:

1. Complex eigen values come in pair  $\lambda$  and  $\bar{\lambda}$ .
2. Since  ${}^t A = A^{-1}$ , inverse of every eigenvalue is again an eigenvalue.

We claim that it has at least one real eigenvalue.

On contrary suppose all are strictly complex. Given  $\lambda_1 \in \mathbb{C}$ ,  $\bar{\lambda}_1$  is also an eigenvalue, say it is  $\lambda_2$ . Now  $\lambda_1^{-1}$  is also eigenvalue. If  $\lambda_1^{-1} = \lambda_1$  then  $\lambda_1 = \pm 1$ , a contradiction. Now if  $\lambda_1^{-1} = \lambda_2 = \bar{\lambda}_1$  then determinant condition implies  $\lambda_3 = 1$ , a contradiction.

Thus,  $\lambda_3 = \lambda_1^{-1}$ . But again determinant condition tells us  $\lambda_1 = 1$ , a contradiction.

## Rotation in 3D

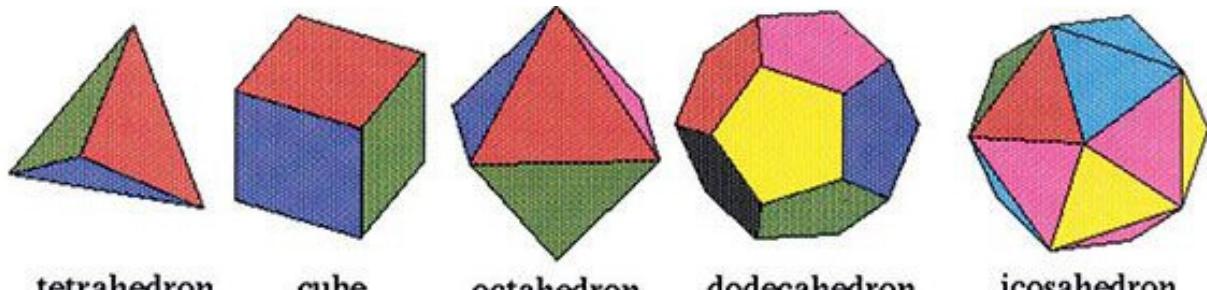
Thus, we may assume, wlg,  $\lambda_1$  is real.

Now, if  $\lambda_2$  is strictly complex then  $\lambda_3 = \bar{\lambda}_2 = \lambda_2^{-1}$  must be complex too. Hence  $\lambda_1 = \lambda_1^{-1}$  implies  $\lambda_1 = \pm 1$  and determinant condition would imply  $\lambda_1 = 1$ .

Now suppose  $\lambda_2$  is also real. Then  $\lambda_3$  is real as well. If at least one of them is 1 we are done.

Suppose none of them are 1. Consider  $\lambda_1^{-1} \neq \lambda_1$ . Then, determinant would imply  $\lambda_3 = 1$ . Thus,  $\lambda_1 = \lambda_1^{-1}$  which gives  $\lambda_1 = -1$ . Now determinant condition would give  $\lambda_2\lambda_3 = -1$ . If  $\lambda_2^{-1} \neq \lambda_2$  then it must be  $\lambda_3$  contradicts the product condition. However if  $\lambda_2^{-1} = \lambda_2$  then it must be  $-1$  and hence  $\lambda_3 = 1$ , again a contradiction.

# Platonic Solids



# Symmetries of Platonic solids

	$V$	$E$	$F$	$Sym$	$Sym^+$
Tetrahedron	4	6	4	$S_4$	$A_4$
Cube	8	12	6	$S_4 \times \mathbb{Z}/2\mathbb{Z}$	$S_4$
Octahedron	6	12	8	$S_4 \times \mathbb{Z}/2\mathbb{Z}$	$S_4$
Dodecahedron	20	30	12	$A_5 \times \mathbb{Z}/2\mathbb{Z}$	$A_5$
Icosahedron	12	30	20	$A_5 \times \mathbb{Z}/2\mathbb{Z}$	$A_5$

## $SO(3)$ Symmetries of Tetrahedron

- Every rotation in 3D fixes an axis.
- We have an identity symmetry.
- Axis passing through a vertex and mid points of the opposite face is order 3 rotation: 4 pairs  $\times (3 - 1) = 8$ .
- Axis passing through two opposite edges:  
3 pairs  $\times (2 - 1) = 3$ .
- Total number of symmetries  $= 1 + 8 + 3 = 12$ .
- By looking at action on vertices and using orbit-stabiliser we get that its a group of order 12. Also, it must be a subgroup of  $S_4$ .

## $SO(3)$ Symmetries of Dodecahedron

- Every rotation in 3D fixes an axis.
- Axis passing through mid-points of two opposite faces contribute:  $6 \text{ pairs} \times (5 - 1) = 24$  non-identity symmetries.
- Axis passing through mid points of two opposite sides:  $15 \text{ pairs} \times (2 - 1) = 15$ .
- Axis passing through two opposite vertices:  $10 \text{ pairs} \times (3 - 1) = 20$ .
- Total number of symmetries  $= 1 + 24 + 15 + 20 = 60$ .

# Symmetry of Platonic solids

- Involves the orthogonal group  $O(3)$ .
- Better understood using Hamilton's quaternion  $\mathbb{H}$  which gives the group  $SU(2)$ .
- See youtube video "What are quaternions, and how do you visualize them? A story of four dimensions" by **3Blue1Brown**.

# Quaternions, $SU(2)$ and double cover of rotations in 3D

## Part III



## Hamilton's quaternion

- $\mathbb{H} = \{a = a_0 + a_1i + a_2j + a_3k \mid a_0, a_1, a_2, a_3 \in \mathbb{R}\}$
- For  $a = a_0 + a_1i + a_2j + a_3k$  and  $b = b_0 + b_1i + b_2j + b_3k$ , we have,

$$\begin{aligned} a + b &= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k \\ a.b &= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) \\ &\quad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i \\ &\quad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)j \\ &\quad + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)k. \end{aligned}$$

- $i^2 = -1 = j^2 = k^2$  and  $ij = -ji = k$ .
- $\mathbb{H}$  is an associative algebra (non-commutative ring as well as a vector space over  $\mathbb{R}$ ).

## Hamilton's quaternion

- We define conjugation by  $\bar{a} = a_0 - a_1 i - a_2 j - a_3 k$ .
- Compute and show that  $a\bar{a} = a_0^2 + a_1^2 + a_2^2 + a_3^2 = \bar{a}a$  is a real number.
- Define norm  $N(a) = a\bar{a}$ , and trace  $tr(a) = a + \bar{a} = 2a_0$ .
- For an  $a \in \mathbb{H}$  show that it always satisfies the quadratic equation

$$X^2 - (tr(a))X + N(a) = 0.$$

## Realization of quaternions - Double complex numbers

- $a = a_0 + a_1i + a_2j + a_3k = (a_0 + a_1i) + (a_2 + a_3i)j = z_1 + z_2j$  where  $z_1, z_2$  are in  $\mathbb{C}$ .
- Thus we may think of  $\mathbb{H} = \mathbb{C} + \mathbb{C}j$  with

$$a.b = (z_1 + z_2j).(w_1 + w_2j) = (z_1w_1 - \bar{w}_2z_2) + (w_2z_1 + z_2\bar{w}_1)j$$

where  $a = z_1 + z_2j$  and  $b = w_1 + w_2j$ . where the norm and conjugation on complex numbers are defined in usual way.

## Realization as $2 \times 2$ complex matrices

- $a = z_1 + z_2j$  map it to  $a = \begin{pmatrix} z_1 & -z_2 \\ \bar{z}_2 & \bar{z}_1 \end{pmatrix}$  in  $M_2(\mathbb{C})$ .
- Note that,

$$a.b = \begin{pmatrix} z_1 & -z_2 \\ \bar{z}_2 & \bar{z}_1 \end{pmatrix} \begin{pmatrix} w_1 & -w_2 \\ \bar{w}_2 & \bar{w}_1 \end{pmatrix} = \begin{pmatrix} z_1w_1 - z_2\bar{w}_2 & -z_1w_2 - z_2\bar{w}_1 \\ \bar{z}_2w_1 + \bar{z}_1\bar{w}_2 & -\bar{z}_2w_2 + \bar{z}_1\bar{w}_1 \end{pmatrix}.$$

- Thus  $\mathbb{H} = \left\{ \begin{pmatrix} z_1 & -z_2 \\ \bar{z}_2 & \bar{z}_1 \end{pmatrix} \in M_2(\mathbb{C}) \right\}$ . The multiplication in this case is simply given by the matrix multiplication.
- The norm  $N(a) = \det \begin{pmatrix} z_1 & -z_2 \\ \bar{z}_2 & \bar{z}_1 \end{pmatrix} = z_1\bar{z}_1 + z_2\bar{z}_2$ .

## As $2 \times 2$ complex matrices

Remember the following association of quaternions in the matrix notation:

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

## Four Square Identity

- The map  $N: \mathbb{H}^* \rightarrow \mathbb{R}^*$  defined by  $a \mapsto N(a)$  is a multiplicative group homomorphism. That is,

$$N(ab) = ab \cdot \overline{ab} = ab\bar{b}\bar{a} = aN(b)\bar{a} = N(a)N(b).$$

- Write this in expanded form to get the Four Square Identity.

$$\begin{aligned} & (a_0^2 + a_1^2 + a_2^2 + a_3^2) \cdot (b_0^2 + b_1^2 + b_2^2 + b_3^2) \\ = & (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)^2 \\ & + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)^2 \\ & + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)^2 \\ & + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)^2. \end{aligned}$$

## The group $SU(2)$

- The group  $SU(2) := \{X \in M_2(\mathbb{C}) \mid X^*X = I, \det(X) = 1\}$ .
- Check if  $X \in SU(2)$  then it is of the form  $\begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix}$  for some  $w, z \in \mathbb{C}$  satisfying  $w\bar{w} + z\bar{z} = 1$ .
- $\mathbb{H}^1 := \{a \in \mathbb{H} \mid N(a) = 1\} \cong SU(2)$ .
- Also,  $\mathbb{H}^1 \cong \mathbb{S}^3$ , the sphere (hence simply connected).

## Symmetric bilinear form on $\mathbb{H}$

- Now,  $\mathbb{H}$  is a 4-dimensional vector space over  $\mathbb{R}$ .
- We have a non-degenerate symmetric bilinear form  $B$  on  $\mathbb{H}$  induced from  $N$  given as follows:

$$\begin{aligned} B(x, y) &= \frac{N(x + y) - N(x) - N(y)}{2} \\ &= \frac{1}{2}[(x_0 + y_0)^2 + (x_1 + y_1)^2 + (x_2 + y_2)^2 + (x_3 + y_3)^2 \\ &\quad - (x_0^2 + x_1^2 + x_2^2 + x_3^2) - (y_0^2 + y_1^2 + y_2^2 + y_3^2)] \\ &= x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3. \end{aligned}$$

## The Map

- Let  $V := \text{Im}(\mathbb{H}) = \langle i, j, k \rangle$  be 3 dimensional vector space.
- For  $a \in \mathbb{H}^1$  define a map  $\phi_a: V \rightarrow V$  by

$$\phi_a(x) = axa^{-1} = ax\bar{a}.$$

- $\phi_a$  preserves norm, hence is in  $O(3)$ , in fact in  $SO(3)$ .
- For example, when  $a = \cos(\theta) + \sin(\theta)i$ , the matrix of  $\phi_a: V \rightarrow V$  is

$$\phi_a = \begin{pmatrix} 1 & & \\ & \cos(2\theta) & -\sin(2\theta) \\ & \sin(2\theta) & \cos(2\theta) \end{pmatrix}.$$

## Double cover map

- The map  $a \mapsto \phi_a$  from  $\mathbb{H}^1$  to  $SO(3)$  is a group homomorphism.
- We get the following exact sequence:

$$\{\pm 1\} \hookrightarrow \mathbb{H}^1 \xrightarrow{\phi} SO(3).$$

- The map  $\phi: \mathbb{H}^1 \rightarrow SO(3)$  is a surjective group homomorphism with kernel  $\{\pm 1\}$ .
- Thus,  $\mathbb{H}^1 \cong SU(2) \cong \mathbb{S}^3 \rightarrow SO(3)$  is a double cover.

## Hurwitz Theorem

- The norm  $N: \mathbb{H}^* \rightarrow \mathbb{R}^*$ , defined by  $N(a) = a\bar{a}$ , show that  $\mathbb{H}^1 := \ker(N)$  is a group. Hence, the sphere  $\mathbb{S}^3$  is a group.
- Thus,  $\mathbb{S}^0 = \{\pm 1\}, \mathbb{S}^1, \mathbb{S}^3$  are groups.
- It is an amazing fact that the sphere  $\mathbb{S}^n \subset \mathbb{R}^{n+1}$  is a group if and only if  $n = 1, 3$  or  $7$ .
- This phenomena is related to being able to put composition algebra structure on  $\mathbb{R}^m$  which is possible if and only if  $m = 1, 2, 4$  or  $8$ . The composition algebras of dimension 1 is the field  $\mathbb{R}$ , of dimension 2 is either  $\mathbb{R} \times \mathbb{R}$  or  $\mathbb{C}$ , of dimension 4 is either  $M_2(\mathbb{R})$  or  $\mathbb{H}$  and of dimension 8, two possibilities, called octonions.

# Application of Groups and Computation

## Part - IV



## Maths is Useless

I'm still waiting for the day that I will actually use



$$xy + (4 \cdot 20) > \\ x - 5y[2+9-7]$$

in real life

## **Application to 3D software designing**

- The function of pointer on the desktop, laptop, mobile phone screen is Translation, Rotation and Stretching.
- Any 3D designing software (e.g. BLENDER) is built on these basic movements created by these math formulas. All video games and many (animation) movies are made using these software.
- The basic ROBOTS used in large scale production factories use these basic movements.

## Groups as Galois groups

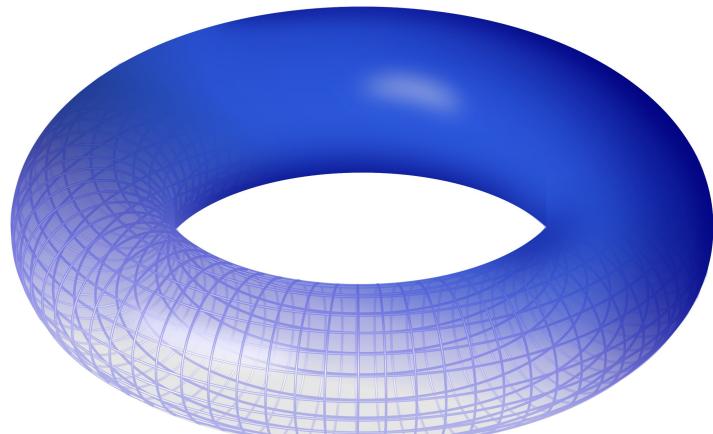
- In Galois theory we associate a group, called Galois group, to a polynomial.
- Example

Polynomial	Field Extension	Galois group $D_8$
$(X^2 - 2)(X^2 - 3)$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$X^4 - 2$	$\mathbb{Q}(\sqrt[4]{2}, i)$	$D_8$
$X^4 - X - 1$	$\mathbb{Q}(????)$	$S_4$ .

- **Inverse Galois Problem:** Given a finite group  $G$ , does there exist a Galois extension  $K$  of  $\mathbb{Q}$  such that  $Gal(K/\mathbb{Q}) \cong G$ ?

# Groups and Topology

- To a topological space  $X$  we associate its fundamental group  $\pi_1(X)$ .
- $\pi_1(\mathbb{S}^1) \cong \mathbb{Z}$ ,  $\pi_1(Torus) \cong \mathbb{Z} \times \mathbb{Z}$ .



- More generally we associate homology and cohomology.

# Computational group theory

- Can we implement a group in computer so that we can do further computations within it?



# Computational group theory

- Can we implement a group in computer so that we can do further computations within it?
- There are computer packages (GAP, SAGEmath, MAGMA etc) where one can work with various groups.

# Computational group theory

- Can we implement a group in computer so that we can do further computations within it?
- There are computer packages (GAP, SAGEmath, MAGMA etc) where one can work with various groups.
- The groups which are implemented are, for example, Symmetric groups  $S_n$ , Alternating groups  $A_n$ , Dihedral groups  $D_n$ ,  $SL(n, q)$ ,  $O(n, q)$  etc.

# Computational Group Theory

## Computations with Groups

Developer's  
point of view

User's  
point of view



# Groups defined by Generators and Relations

- Groups are defined by generators and relations,

$$G = \langle s_1, s_2, \dots \mid r_1, r_2, \dots \rangle$$

instead of the full multiplication table. For example,  
Dihedral group

$$D_{2n} = \langle r, s \mid r^n = 1 = s^2, rs = sr^{-1} \rangle.$$



# Groups defined by Generators and Relations

- Groups are defined by generators and relations,

$$G = \langle s_1, s_2, \dots \mid r_1, r_2, \dots \rangle$$

instead of the full multiplication table. For example,  
Dihedral group

$$D_{2n} = \langle r, s \mid r^n = 1 = s^2, rs = sr^{-1} \rangle.$$

- Thus the main problem is to find a “small” set of generators with a “small” set of relations for a given group.

# Groups defined by Generators and Relations

- Groups are defined by generators and relations,

$$G = \langle s_1, s_2, \dots \mid r_1, r_2, \dots \rangle$$

instead of the full multiplication table. For example,  
Dihedral group

$$D_{2n} = \langle r, s \mid r^n = 1 = s^2, rs = sr^{-1} \rangle.$$

- Thus the main problem is to find a “small” set of generators with a “small” set of relations for a given group.
- This is being done for all finite simple groups.

# Classification of finite simple groups

This is one of the greatest achievement of last century! Any finite simple group belongs to one of the following family:

1. Cyclic group of prime order.
2. Alternating group  $A_n$  for  $n \geq 5$ .
3. Finite groups of Lie type
  - 3.1 Classical groups, for example,  $PSL(n, q)$ , Orthogonal, Symplectic and Unitary groups.
  - 3.2 Exceptional groups, for example,  $G_2(q), F_4(q), E_6(q), E_7(q), E_8(q)$  and their twisted analogues.
4. 26 Sporadic groups.

# Classification of finite simple groups

This is one of the greatest achievement of last century! Any finite simple group belongs to one of the following family:

1. Cyclic group of prime order.
2. Alternating group  $A_n$  for  $n \geq 5$ .
3. Finite groups of Lie type
  - 3.1 Classical groups, for example,  $PSL(n, q)$ , Orthogonal, Symplectic and Unitary groups.
  - 3.2 Exceptional groups, for example,  $G_2(q), F_4(q), E_6(q), E_7(q), E_8(q)$  and their twisted analogues.
4. 26 Sporadic groups.

For example, the Monster group, has order

$$\begin{aligned} & 2^{46} 3^{20} 5^9 7^6 11^2 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ = & 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 \\ \sim & 8 \times 10^{53}. \end{aligned}$$

Watch YouTube video

3Blue1Brown : Group theory, abstraction, and the  
196,883-dimensional monster

<https://youtu.be/mH0oCDa74tE>



## Two generation problem

Guralnick, Kantor, Kassabov and Lubotzky have proved that every non-abelian finite simple group can be generated by 2 generators and at most 80 relations (except one of them).

# **Classification of finite Groups: an approach via Finite Simple Groups**

Please read my article written for IISER Pune Science Club magazine “Helicase”.

# Thank You.

email : anupamk18@gmail.com

<https://sites.google.com/site/anupamk182/>

