[RINKINY]

Group Theory

~~#~~ Def^n:

- **Groups**: $(G, \cdot)$ —

  1) $g, h \in G \Rightarrow g \cdot h \in G$ (closure)

  2) Assosiativity: $(g \cdot h) \cdot w = g \cdot (h \cdot w)$ } $g \cdot h \cdot w$

  way to combine more than two elements

  3) $\exists$ identity element: (1_G)

  $$g \cdot 1 = g \quad \forall g \quad , \quad 1 \cdot g = g \quad \forall g$$

  4) $\exists$ inverse:

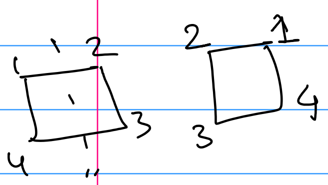
  $\forall g \in G$, we find $g^{-1} \in G$

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

Motivation for group axioms —

- $S_n = \{$ Set of all permutations of n elements $\}$ $1 \quad 2 \quad \cdots \quad n$

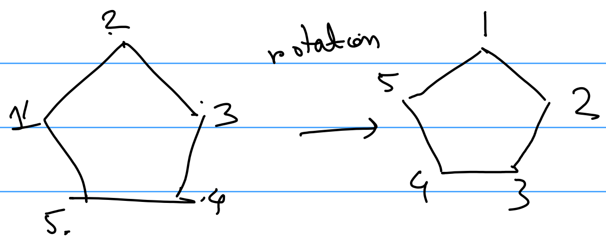
- $D_{2n} = \{$ Set of symmetries of a polygon $\}$



$1 \quad 2 \quad 3 \quad 4 \quad 5$

$\phi : \{1, 2, \ldots, 5\} \rightarrow \{1, 2, \ldots, 5\}$

$5!$



$1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 3$
$4 \mapsto 4$
$5 \mapsto 5$

g, h

$gh = hg$ commutativity

Abelian group

Examples :-

1) $(\mathbb{Z}, +)$ $a + 0 = a = 0 + a$

identity $= 0$

inverse :- (a)

inverse is $(-a)$

$$a + (-a) = 0 = (-a) + a$$

2) $(\mathbb{Z}/n\mathbb{Z}, +)$ [Verify that these are groups]

3) Matrix groups :-

$GL(n, \mathbb{R}) = \{ n \times n$ invertible matrices with entries from $\mathbb{R} \}$

$GL(n, \mathbb{Z}) = \{$ " " " " " " $\mathbb{Z} \}$

binary operation : matrix multi:

$$GL(2, \mathbb{R}) \longrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

identity :- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $AI = A = IA$

inverse :- A^{-1}

3) $SL(n,\mathbb{R}) = \{n \times n$ matrices with det 1 with entries from $\mathbb{R}\}$

$SL(n,\mathbb{Z})$

4) $S_n = \{$ set of permutations $\}$

binary operation here is composition

identity ..

- Exercise : 1) Uniqueness of Id and inverses

(G a group, $1, 1'$ both id $\rightarrow 1 = 1'$)

Show ($\forall g \in G$, h, h' both satisfy $\left.\begin{array}{l} hg = 1 = gh \\ h'g = 1 = gh' \end{array}\right\} \Rightarrow h = h'$

- Exercise 2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

3) $(a^{-1})^{-1} = a$

$\boxed{ab \doteq a \cdot b}$

Subgroups : G group.

$H \leq G$

H is a subset of G

non empty, closed under binary operation and inverses.

i.e. ($[a, b \in H \rightarrow ab \in H]$ $[a \in H, a^{-1} \in H]$

$h_1, h_2, h_3 \in H$
$\in G$)

- This Sub-group Criteria : H is a subset of G.

H is a subgroup $\Leftrightarrow$ $H \neq \phi$ and $\forall g, h \in H$, $gh^{-1} \in H$

Example 5:

$H = \langle 2 \rangle$
$= \{0, 2, -2, 4, -4, 6, -6, \ldots\}$
$= 2\mathbb{Z}$
subgroup.

Pf: H is a subgroup.

$\dfrac{g \in H}{h \in H \Rightarrow \underline{h^{-1} \in H}}$

$\Rightarrow gh^{-1} \in H$ ☒

Converse: $g, h \in H \Rightarrow gh^{-1} \in H$

$g \in H \Rightarrow gg^{-1} \in H$
$\Rightarrow 1 \in H$

$g \in H,\ 1 \in H \Rightarrow 1 \cdot g^{-1} \in H \Rightarrow g^{-1} \in H \rightarrow$ closed under inverse.

similar: $h^{-1} \in H$

$g \in H,\ h^{-1} \in H \Rightarrow g(h^{-1})^{-1} \in H$
$\Rightarrow gh \in H \longrightarrow$ closed under bin op

$\boxed{\text{\# Exercise: } (g^{-1})^{-1} = g}$

$\Rightarrow$ H is a subgroup. ☒

- Order of groups : $|G|$ = no. of elements in G.
- order of element : $g \in G$

$o(g)$ = smallest +ve int s.t $g^n = 1_G$

- Isomorphisms and homomorphisms :

$1+2=3$

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, 3 \dots \}$$
$$\downarrow \; \downarrow \; \downarrow \; \downarrow \; \downarrow \; \downarrow \; \downarrow \; \downarrow$$
$$5\mathbb{Z} = \{ \dots, -10, -5, 0, 5, 10, 15 \dots \}$$

$5+10=15$.

- Def^n : (homomorphism) $(G, \cdot), (H, *)$ are groups.

function $f : G \longrightarrow H$ is called a homomorphism if -

$$\forall g_1, g_2 \in G, \quad f(g_1 \cdot g_2) = f(g_1) * f(g_2)$$

- Def^n : (Isomorphism) bijective homomorphisms

$G \xrightarrow{\phi} H$ isomorphic. , $G \cong H$ (isomorphic)

$$\mathbb{Z} \cong 5\mathbb{Z}$$

$$\mathbb{Z} \xrightarrow{\phi} 5\mathbb{Z}$$
$$x \longmapsto 5x$$

x, y $\quad \phi(x+y) = 5(x+y) = 5x + 5y$
$\quad = \phi(x) + \phi(y)$

- Automorphism :- $G \xrightarrow{\phi} G$ isomorphism

- $G \xrightarrow{\phi} H$ homomorphism, $\left[\ker\phi = \{g \in G : \phi(g) = 1_H\}\right]$

Exercise :- 1) $\ker\phi$ is a subgroup of G

2) $\operatorname{Im}\phi$ is a subgroup of H

- Group Presentations :

$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$

$\mathbb{Z} = \langle 1 \rangle$

$2\mathbb{Z} = \langle 2 \rangle$ → Subgroup of $\mathbb{Z}$

Subgroup G is generated by $a, b, c \ldots$

$\langle a, b, c \rangle = G$

- Presentation :-

$$G = \langle \underbrace{a, b, c}_{\text{generators}} \mid \underbrace{ab = c, ac = a}_{\text{relations}} \rangle$$

free groups = $\underline{\underline{\langle a, b \rangle}}$

$$\langle a, b \mid a^{-1}ba = b^2, b^{-1}ab = a^2 \rangle = \{1\}$$

Problem: Find all subgroups of $\mathbb{Z}$. } $n\mathbb{Z}$

Answer: **Notice:** Any $n\mathbb{Z}$ is a subgroup.

Claim: Any subgroup is of this form $n\mathbb{Z}$

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

Let n be the smallest (+ve) number in H.

Claim: $H = n\mathbb{Z}$.

Pf:

$n \in H$

$n+n \in H$

$\vdots$

$n\mathbb{Z} \subseteq H$

Remains to prove $H \subseteq n\mathbb{Z}$

Take $h \in H$

$h = nd + r$ where $r < n$, $\cancel{r \neq 0}$

$r = \underbrace{h}_{\in H} - \underbrace{nd}_{\in H}$

$\Rightarrow r \in H$

$r < n \longrightarrow$ contradiction to minimality of n.

$\Rightarrow r = 0$

$\blacksquare$

Coset = left coset

- **Cosets:**

  - Def^n: G is a group, H is a subgroup. Take some $g \in G$.
    Then $gH = \{ g \cdot h : h \in H \}$ is called a left coset

    this is called coset representatives

  - Example: $\mathbb{Z}$
    $n\mathbb{Z}$ are subgroups

    $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

    1) $\{ \ldots, -10, -5, 0, 5, 10, \ldots \}$

    $5\mathbb{Z} + 0$ is another coset.

    2) $\{ \ldots, -9, -4, 1, 6, 11, \ldots \}$ $5\mathbb{Z}+1$

    3) $\{ \ldots, -8, -3, 2, 7, 12, \ldots \}$ $5\mathbb{Z}+2$

    4) $\{ \ldots, -7, -2, 3, 8, 13, \ldots \}$ $5\mathbb{Z}+3$

    5) $\{ \ldots, -6, -1, 4, 9, 14, \ldots \}$ $5\mathbb{Z}+4$.

    $5\mathbb{Z}+5$

- Cosets have same cardinality.

$$\phi : H \longrightarrow gH \qquad \text{check } \phi \text{ is bijection}$$
$$x \longmapsto gx$$

- Cosets are disjoint: Say not

Say not. $x \in g_1 H$, $x \in g_2 H$

$\Rightarrow x = g_1 h_1$, $x = g_2 h_2$

$g_1 h_1 = g_2 h_2$

$\Rightarrow g_1 = g_2 \underbrace{h_2 h_1^{-1}}_{\in H}$

$g_1 \in g_2 H \longrightarrow g_2 \in g_1 H$

$\Rightarrow g_1 H = g_2 H$

- $\bigcup$ all these cosets $= G$.

(Exercise)

Pf:

gH is a subset of G.

$\bigcup_{g \in H} gH$ is a subset

$\bigcup_{g \in H} gH \subseteq G$

To show: $G \subseteq \bigcup_{g \in H} gH$

Pf: $g \in G$

If $g \in H$ done

If not, chose some $h \in H$

Then, $g = \underbrace{gh^{-1}}_{\in G} \underbrace{h}_{\in H}$

$g \in \underline{(gh^{-1}) H} \to$ coset

- **Lagrange's thm** :- G is group, H any subgroup.

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

Pf :- Look at all the cosets

Quotienting & Normal subgps

G a group, H a subgroup.

G/H = Set of all cosets

Does NOT have to be a group. !

When is this a group? $\longrightarrow$ I'll show that if H is 'normal' subgroup, then G/H is a gp.

Motivation :-

- **Quotienting** :- X, Y are sets

$$X \xrightarrow{f} Y \quad \text{function}$$

Say we have a equiv relation $\sim$ on a set X. equiv class of a -
$[a] = \underbrace{\{b \in X : a \sim b\}}_{\text{subset of } X}$

Define a equivalence relation $\sim$:-

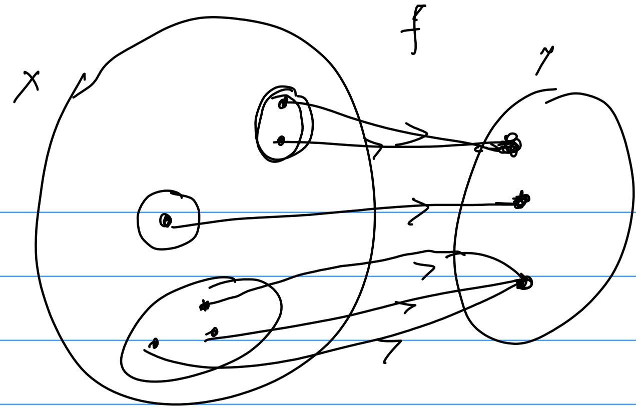
$$a \sim b \text{ if } f(a) = f(b)$$

$$X/\sim \; = \{\text{set of equivalence classes}\}$$

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & Y \\ X/\sim \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

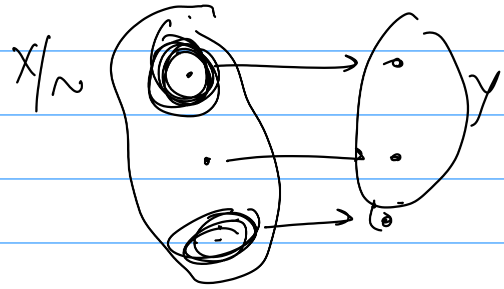
$X \xrightarrow{f} Y$

f is not injective



$\tilde{f} : X/\sim \longrightarrow Y$

$[a] \longmapsto f(a)$



Sticking together

- $\tilde{f}$ is injective

Pf: $f(a) = f(b)$

$\Rightarrow a \sim b$

$\Rightarrow [a] = [b]$ ∎

- **Groups:** $G \xrightarrow{f} H$ homomorphism

$\ker f = N \underset{\text{subgroup}}{\leq} G$

Define equivalence relation $\sim$ this way: $g \sim h$ if $gh^{-1} \in N$

$gh^{-1} \in N$

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

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

$\Rightarrow f(g) = f(h)$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & H \\ G/\sim \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

$G/\sim$ = equivalence classes under the equiv relation

$G/\sim \, = G/N \longrightarrow \{\text{set of cosets}\}$

$[g] \longmapsto gN$

<u>Claim</u> :- G/N is a <u>group</u> with the binary operation

$$(g_1 N)\cdot(g_2 N) = \underbrace{(\underbrace{g_1 g_2}_{\in G})\ N}_{\text{coset}}$$

<u>Pf</u> :- <u>well defined</u> :

$$g_1 N = g_1' N \quad , \quad g_2 N = g_2' N$$

<u>To show</u> :- $(g_1 \cdot g_2)\ N = (g_1' \cdot g_2')\ N$

<u>Pf</u> :- $g_1 N = g_1' N$

$g_1^{-1} g_1' \in N \Rightarrow \phi(g_1^{-1} g_1') = 1$

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

$g_2^{-1} g_2' \in N \Rightarrow \phi(g_2) = \phi(g_2')$

$g_1 H = g_2 H$

$\Rightarrow g_1 h_1 = g_2 h_2$

$\Rightarrow h_1 = g_1^{-1} g_2 h_2$

$\Rightarrow g_1^{-1} g_2 = \underbrace{h_1 h_2^{-1}}_{\in H}$

$\Rightarrow g_1^{-1} g_2 \in H$

Now, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$

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

$= \phi(g_1' g_2')$ ■

<u>Exercise</u> :- this is a group.

Closure: obv

Associativity: follows.

Identity: N is the identity

Inverse: $(gN)^{-1} = g^{-1}N$

Exercise: Check this is a grp.

Exercise: $\tilde{f}$ is also homomorphism

▸ Obvious

Also, $\tilde{f} : G/N \to H$ is injectivity

$$G \xrightarrow{f} H \qquad \boxed{N = \ker f}$$

$$G/N \xrightarrow{\tilde{f}} H$$

injective group homomorphism

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

$\boxed{\text{Q commuting}}$

- Def^n: (Normal subgroups) Subgroups of G which are kernel of some homomorphism.

- If N is a normal subgroup of G, then G/N is a group with bin op

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

G/N is called the quotient group.

(Textbooks)

- **Alternate Def^n** : H is a subgroup of G

H is called a normal subgroup if $gHg^{-1} = H$ $\forall g \in G$.

$\forall h \in H$

$ghg^{-1} \in H$

Equivalence of definitions : (N is $\ker \phi$) $\Leftrightarrow$ ($gNg^{-1} = N$)

▶ Pf : $\boxed{\Rightarrow}$ N is kernel of some homomorphism $\phi : G \to H$

Take any $n \in N$, $\phi(n) = 1$

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

So $gng^{-1} \in N$ ☒

$\boxed{\Leftarrow}$ N is a subgroup and $gNg^{-1} = N$

We need to show N is kernel of some homomorphism.

Consider $\phi : G \to G/N$ [prove G/N is a grp] → Exercise

$g \mapsto gN$

Then claim : $N = \ker \phi$

▶ Pf : $n \in N$, then $\phi(n) = N$ So, $N \subseteq \ker\phi$.

Take $x \in \ker\phi$, then $\phi(x) = N$

$\Rightarrow xN = N$

$\Rightarrow x \in N$

$\ker\phi \subseteq N$.

$G \xrightarrow{f} H$

$\underbrace{G/\ker f}_{\text{group}} \xrightarrow{\tilde{f}} \underbrace{H}_{\text{group}}$ is injective

If $G \xrightarrow{f} H$ homomorphism, then $\boxed{G/\ker f \cong \operatorname{Im} f}$ $\longrightarrow$ 1st Isomorphism thm

2nd isomorphism, 3rd isomorphism.