→ 2 families of groups

↳ Group of symmetries for regular n-gon

(Dihedral group D_n, $|D_n| = 2n$)

↳ Free groups generated by n symbols

$F(S)$, where $S = \{a_1, a_2, \dots, a_n\}$

→ $\mathbb{Z}, S_n, \underbrace{\mathbb{Z}_n}$

y-$n = 7$, today = Thu, 10th Aug 2023

What is 10 Aug 2025?

No. of days = $365 \times 2 + 1 = 731$

$731 \% 7 = 3$, so day = thu + 3 = Sunday

→ Suppose H is a subset of group G.

If for $x, y \in H$ we have $xy \in H$, then H is closed under multiplication (or multiplicative subset of G)

Eg: $2\mathbb{Z}$ (even integers) is closed under addition

$2\mathbb{Z}+1$ (odd integers) is not closed under addition.

→ If $H \subset G$ is closed under the operation, and forms a group, then H is called a subgroup of G and we write $H < G$.

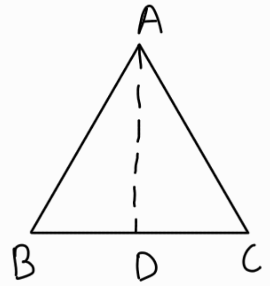
Eg: $2\mathbb{Z} < \mathbb{Z}$, but not $2\mathbb{Z}+1 < \mathbb{Z}$

- $2\mathbb{Z}_n = \{[2x]_n : x \in \mathbb{Z}\}$

Eg: $\mathbb{Z}_5 = \{[0],[1],\dots,[4]\}$

$2\mathbb{Z}_5 = \{[2.0]=[0],[2],[4],[1],[3]\}$
$= \mathbb{Z}_5$

So if n is odd, then $2\mathbb{Z}_n = \mathbb{Z}_n$
if n is even, $2\mathbb{Z}_n < \mathbb{Z}_n$

- 

$\{1, \text{reflection about } AD\} < D_3$

- $\{e\} < G$ (trivial subgroup), and $G < G$

→ Subgroups of $\mathbb{Z}$

- Let $m \in \mathbb{Z}$, then $m\mathbb{Z} = \{mj \mid j \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$
- Let $H < \mathbb{Z}$. Either $H = \{0\}$ or $H = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Let $X = \{x \in H : x > 0\} \neq \phi$, then m can be found as $m = \min(X)$. we know $\min(X)$ exists coz of WOP. By def of m, $m\mathbb{Z} \subset H$.

We just need to prove $H \subset m\mathbb{Z}$
Suppose $x \in H$. By EDA, $x = qm + r$, $0 \le r < m$
then $r \in H$ but m is smallest positive number of H, so r has to be 0. So $m|x$. So $H \subset m\mathbb{Z}$

So finally, $H = m\mathbb{Z}$

→ Subgroups of $\mathbb{Z}_n$

- Every subgroup of $\mathbb{Z}_n$ is of the form $r\mathbb{Z}_n$ for some $r \in \mathbb{Z}$ (Proof of exercise)

  Take HCF

- $r\mathbb{Z}_n = \mathbb{Z}_n$ if $\gcd(n, r) = 1$

Proof: take $[ir] = [jr]$ for some $0 \le i < j < n$

then $n \mid r(j-i)$

but $\gcd(n, r) = 1$

then $n \mid (j-i)$

but $0 \le i < j < n$

So $j - i = 0$

So each subgroup in $\{[0], [r], \dots, [(n-1)r]\}$ is distinct

So, $r\mathbb{Z}_n = \mathbb{Z}_n$

Proposition: Let $H \subset G$, $H \neq \phi$, If "$x, y \in H \Rightarrow xy^{-1} \in H$", then $H < G$

Proof: Suppose $a, b \in H$ (since $H \neq \phi$)

→ take $x = a$, $y = a$, then $xy^{-1} = aa^{-1} = e \in H$

→ take $x = e$, $y = a$, then $a^{-1} \in H$ (closed under inverse)

→ take $x = a$, $y = b^{-1}$, then $a(b^{-1})^{-1} = ab \in H$ (closed under mult)

So $H < G$.

→ Let $H < G$. Define a relation $\sim$ on G as:

For $x, y \in G$, $x \sim y$ if $xy^{-1} \in H$

- Reflexive ✓ (coz $xx^{-1} = e \in H$)
- Symmetric ✓ (coz if $xy^{-1} \in H$, then $(xy^{-1})^{-1} \in H$ i.e., $yx^{-1} \in H$)
- Transitive ✓ (coz if $xy^{-1} \in H$, and $yz^{-1} \in H$, then $xy^{-1}yz^{-1} \in H$. i.e., $xz^{-1} \in H$)

So $\sim_H$ is an equivalence relation.

→ What is the class of $x \in G$ under $\sim_H$?

$y \in [x]_H$ if $y \sim_H x$

i.e., $yx^{-1} \in H$

let $yx^{-1} = h$, $h \in H$

or $y = hx$

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

Hx is called a right coset that contains x.

→ Since $\sim_H$ is equivalence, then

$$G = \bigcup_{x \in G} Hx = \bigcup_{i \in I}^{\cdot} Hx_i$$

disjoint cosets

G is a disjoint union of certain right cosets

→ Consider a finite group G, then $|G|$ is called the order of the group, and is the number of elements in G.

· Suppose $|H| = m$, $|G| = n$

Take the map $H \xrightarrow{m_x} Hx$

$h \longmapsto hx$

by def of Hx, m_x is onto

Also if $hx = h'x$, then $h = h'$ so m_x is one-one,

So m is bijection

So $m = |H| = |Hx|$

So $n = |G| = \left| \biguplus_{i \in I} Hx_i \right| = \sum_{i \in I} |Hx_i| = |I| m$

So $m \mid n$, i.e., $|H| \mid |G|$

morever, # of right cosets is a factor of $|G|$

this number is called index of H in G

→ Define $_H\sim$ as:

for $x, y \in G$, $x \,_H\!\sim y \iff x^{-1}y \in H$

Just like before, define left cosets $H[x] = xH$ then index of left and right cosets is same, number of left and right cosets is same.

Lagrange's Theorem of Group theory

Theorem: The order of subgroup divides the order of the group, if the group is finite.