S_2 ?

ab
~~ab~~
~~ba~~

Define $(Ha)(Hb) = Hab$
?? well defined
In general this is not well defined

Ex Get all Subgroups of S_3.

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$H_0 = \{e\}$ $\quad H_1 = S_3$

$H_2 = \{e, \tau_1\}$ $\quad H_3 = \{e, \tau_2\}$ $\quad H_4 = \{e, \tau_3\}$

$H_5 = \{e, \sigma_1, \sigma_2\}$ $\quad \cancel{H_6 = \{e, \tau_1}$

Remark: Converse of Lagrange's Theorem is not true in general.

Result: Converse of Lagrange's Theorem is true in case of cyclic groups.

Let $G = \langle a \rangle$ of size n and $d | n$

then $\exists H \leq G$ s.t. $|H| = d$.

Proof $k = n/d$

Set $b = a^k$

$H = \langle b \rangle$ Claim $|H| = d$

In fact, such H is unique.

Suppose $|H_1| = |H_2| = d$

$a^k \qquad a^t$

$\Rightarrow k = t$

- Result: Every subgroup of a cyclic group is cyclic.

$H \le G = \langle a \rangle$

If $H = \langle e \rangle$ then we are done

Else $H \neq \{e\}$ $\qquad a^k \in H$

$a^{-k} \in H$

Consider the set of all the exponents of a in H.

By well ordering let m be the least element in this set $\quad$ claim $H = \langle a^m \rangle$

Let $x \in H$

$\Rightarrow x = a^n$ for some n

$n = mq + r \qquad 0 \le r < m$

$a^r = a^{n-mq} = a^n (a^m)^{-q} \in H$

$\Rightarrow r = 0$

$x = a^n = a^{mq} = (a^m)^q = c^q$

~~$H < \langle c \rangle$~~ $\quad H = \langle c \rangle$

$\cancel{\mathbb{Z}}$

~~$n\mathbb{Z} <$~~ $\quad \mathbb{Z} \le (\mathbb{Q}, +)$

$$S_3 = \{e, \underset{\binom{1\,2\,3}{2\,3\,1}}{\sigma_1}, \underset{\binom{1\,2\,3}{3\,1\,2}}{\sigma_2}, \underset{\binom{1\,2\,3}{1\,3\,2}}{\tau_1}, \underset{\binom{1\,2\,3}{3\,2\,1}}{\tau_2}, \underset{\binom{1\,2\,3}{2\,1\,3}}{\tau_3}\}$$

Consider $H = \{e, \tau_1\} \leq S_3$

$He = \{e, \tau_1\}$

$H\sigma_1 = \{\sigma_1, \tau_2\} = H\tau_2$

$H\sigma_2 = \{\sigma_2, \tau_3\}$

S_3: $\boxed{e, \tau_1 \mid \sigma_1, \tau_2 \mid \sigma_2, \tau_3}$

$H\sigma_1\sigma_2 = He = H$

$H\tau_2\tau_3 = H\sigma_1 \neq H$

Consider $n\mathbb{Z} \leq \mathbb{Z}$

cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are

$\bar{0}, \bar{1}, \bar{2} \; \ldots \; \overline{n-1}$

$a \sim b \Leftrightarrow a - b \in n\mathbb{Z}$

$\Rightarrow a \equiv b \pmod{n}$

Remark: Let $H \leq G$ and G/H the set of all right cosets of H. The operation on G/H defined by $Ha \cdot Hb = Hab$ is not well defined in general.

Normal Subgroup: A non-empty set H of G is said to be normal subgroup of $xHx^{-1} \subseteq H$ $\forall x \in G$. In which case we write $H \trianglelefteq G$

$\{e\}$ & G are normal in G.

Result: Let $H < G$

(1) $H \triangleleft G$

(2) $xHx^{-1} = H \quad \forall x \in G$

(3) $Hx = xH \quad \forall x \in G$

(4) $Hx\, Hy = Hxy \quad \forall x, y \in G$

(1) $\Rightarrow$ (2) for $x \in G$

note $x^{-1} \in G$

$$x^{-1} H x \subseteq H$$

$$\Rightarrow x(x^{-1} H x)x^{-1} \subseteq xHx^{-1}$$

$$\Rightarrow H \subseteq xHx^{-1}$$

(3) $\Rightarrow$ (4)

$$H(xH)y = HHxy = Hxy \quad (\because H \text{ is subgroup})$$

(4) $\Rightarrow$ (1)

- Let G be an abl group. Every subgroup of G is normal.

- Let $H < G$ with $[G : H] = 2$

$$H \quad G - H = Ha, \ a \notin H$$

$$H \quad G - H = aH, \ a \notin H$$

$$H \trianglelefteq G$$

- $f : G_1 \to G_2$ a homomorphism

$\ker f \trianglelefteq G_1$ for $x \in G$ $a \in \ker f$

$xax^{-1} \in \ker f$

- $Z(G) \trianglelefteq G$

- ~~Definition~~ Remark : Let $H \trianglelefteq G$, the set of all (right) cosets of H denoted by G/H is a group w.r.t to operation $HaHb = Hab \ \forall a,b \in G$ is called the quotient group.

$n\mathbb{Z} \trianglelefteq \mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$

- Let $H \trianglelefteq G$
  Define $\varphi : G \to G/H$
  by $\varphi(a) = Ha$
  $\varphi(ab) = H(ab) = HaHb = \varphi(a)\varphi(b)$
  Note that φ is onto.
  Hence φ is an epimorphism.
  ($f : G_1 \to G_2$ is epimorphism we call G_2 homomorphic image of G_1)

- Note that $\ker \varphi = H$