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

Quotient group.

Recall. subgroups. $H \subset G$.

G/H = set of cosets.

Example: $H \subset S_n = G$ $\quad H \overset{\sim}{=} S_{n-1}$

isomorphic

$$X_m = \{\sigma \in S_n \mid \sigma(n) = m\}.$$

$X_1, X_2, \dots X_n.$

$G/H = \{X_1, X_2, \dots X_n\}.$

Normal subgroups

Defn: H is a subgroup of G. We call H a normal subgroup if $\forall g \in G, h \in H$,

$$ghg^{-1} \in H.$$

Defn (Abelian group / commutative group).

G is abelian iff $\forall g, h \in G$, $gh = hg$.

$(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$. ...

Example: (Normal subgroups) If G is abelian. all the subgroups are normal subgroups.

If G is abelian. then

$gh = hg$.

multiply g^{-1} on the right. $ghg^{-1} = hgg^{-1}$

$\Rightarrow ghg^{-1} = h$.

Nonexample: $\underline{\text{Perm}(3)} = G$. $H = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$

H is not a normal subgroup.

$h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in G$.

$\underline{ghg^{-1}}$ $g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. $h = \begin{pmatrix} 1 & 3 & 2 \\ \underline{2} & \underline{3} & \underline{1} \end{pmatrix}$.

$g = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix}$.

$ghg^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$.

H is not a normal subgroup

Prop: TFAE (The following are equivalent)

(I) H is a normal subgroup

(II) Define $Hg = \{ hg \mid h \in H \}$. left H-coset

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

Pf: (I) $\Rightarrow$ (II).

Step 1: $Hg \subset gH$.

$\forall hg \in Hg$, $h \in H$.

$hg = gg^{-1} \cdot hg = g \cdot (g^{-1}hg)$

$$= g\left(\underbrace{(g^{-1})\cdot h\,(g^{-1})^{-1}}_{\text{is in } H}\right) \in gH.$$

Step 2: $gH \subset Hg$.

$\forall\ gh \in gH,\ h \in H.$

$$gh = (ghg^{-1})g \in Hg.$$

(II) $\Rightarrow$ (I)

$\forall\ g \in G,\ h \in H,$

$\underline{ghg^{-1}}$ $\qquad gh \in gH = Hg.$

So $\exists\ h_1 \in H,$ s.t. $gh = h_1 g.$

$$\Rightarrow\ ghg^{-1} = h_1 g \cdot g^{-1} = h_1 (g \cdot g^{-1}) = h_1 \in H.$$

What is good for normal subgroups?

Defn (Quotient group) If H is a normal subgroup of G, G/H has a natural group structure defined by $G/H \times G/H \to G/H$.

$$(g_1 H)\cdot(g_2 H) = g_1 g_2 H. \quad (*)$$

When we write gH, gH as a set does not determine g.

We may have $g_1 \neq g_1'$, but $g_1 H = g_1' H$.

We need to verify $(*)$ is "well-defined":
For any input, we get a unique output.

Pf of "well-defined".

We need to prove,

If $g_1 H = g_1' H$, $g_2 H = g_2' H$,

then $g_1 g_2 H = g_1' g_2' H$.

Example:

We may have $g_1 \neq g_1'$, but $g_1 H = g_1' H$.

$G = (\mathbb{Z}, +)$, $H = 6\mathbb{Z}$.

$g_1 = 0$, $g_1' = 6$. $\boxed{0 + 6\mathbb{Z} = 6 + 6\mathbb{Z}.}$

$g_1 \neq g_1'$.

If we prove if $g_1 H = g_1' H$,

then $g_1 g_2 H = g_1' g_2 H$

and if $g_2 H = g_2' H$. then $g_1 g_2 H = g_1 g_2' H$.

then we can use.

$$g_1 g_2 H = g_1' g_2 H = g_1' g_2' H.$$

Step 1: $g_1 H = g_1' H$.

$g_1 \in g_1 H$. $g_1' \in g_1' H$.

$g_1 = g_1' h_1$. $h_1 \in H$.

compare $\underline{g_1' g_2}$, and $g_1 g_2$.

$$\underline{g_1 g_2} = g_1' h_1 \cdot g_2 = g_1' g_2 g_2^{-1} h_1 g_2$$
$$= \underline{g_1' g_2} \, \underline{(g_2^{-1} h_1 g_2)}$$

is in H because H is normal.

$\Rightarrow$ $g_1 g_2 H = g_1' g_2 H$.

Step 2: $g_2 H = g_2' H \Rightarrow \underline{g_2^{-1} g_2'} \in H$.

compare $\underline{g_1 g_2' H}$, $\underline{g_1 g_2 . H}$. $(g_1 g_2) \cdot (g_1 g_2')^{-1}$

$$= g_1 g_2 \cdot \underbrace{(g_2')^{-1}}_{} g_1^{-1}$$

$$\underbrace{g_2 \cdot (g_2')^{-1}}_{= h \in H}$$

$$= g_1 \, h \, g_1^{-1} \in H \text{ because } H \text{ is normal}$$

$$\Rightarrow \quad g_1 g_2' H = g_1 g_2 H.$$

Example: $\mathbb{Z}$, $n\mathbb{Z}$.

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

$$\{ n\mathbb{Z}, \ 1+n\mathbb{Z}, \ 2+n\mathbb{Z}, \ \cdots \ (n-1)+n\mathbb{Z} \}.$$

$$(i+n\mathbb{Z}) + (j+n\mathbb{Z}) = (i+j) + n\mathbb{Z}$$

Q: What are the normal subgroups of S_3?

(There is a complete answer for all S_n

Ex: $U(1) = \{ z \in \mathbb{C} \mid |z| = 1 \}$

$(U(1), \times)$ is a group

$\mathbb{Z} \subset (\mathbb{R}, +)$ subgroup.

$$\mathbb{R}/\mathbb{Z} \cong U(1)$$

$$\mathbb{R}/\mathbb{Z} \to U(1)$$

$$\theta \longmapsto e^{2\pi\sqrt{-1}\theta} = \cos(2\pi\theta) + \sqrt{-1}\sin(2\pi\theta)$$

use $e^{(a+b)} = e^a \cdot e^b$

A nature source of normal subgroup is from group homomorphism

Defn (homomorphism) $\rho: G_1 \to G_2$ satisfies $\rho(ab) = \rho(a)\cdot\rho(b)$

Prop: $\rho(e_{G_1}) = \rho(e_{G_2})$

Prop: $\rho(a^{-1}) = (\rho(a))^{-1}$

$\Big\}$ $\Rightarrow$ check

Defn: $\ker(\rho) = \{ a \mid \rho(a) = e_{G_2} \}$

Prop: ① $\ker(\rho)$ is normal subgroup of G_1

② $\mathrm{Im}(\rho)$ is a subgroup of G_2

Thm: $\exists\ \underbrace{\bar{\rho} : G_1 / \ker\rho \to \mathrm{Im}\,\rho}_{\text{group isomorphism}}$

s.t. $\bar{\rho}(a \ker\rho) = \rho(a)$

Pf: ⓪ $\bar{\rho}$ "well-defined"

$a \ker\rho = a' \ker\rho$. verify

$\rho(a) = \rho(a')$

① $\bar{\rho}$ surjective.

② $\bar{\rho}$ injective

③ $\bar{\rho}$ preserves group structure. $\square$

Cor: ρ injective iff $\ker \rho = \{e\}$

Ex: $\rho : \mathbb{R} \longrightarrow \mathbb{C}^\times$

$a \longmapsto e^{2\pi\sqrt{-1}\, a}$

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

$\operatorname{Im} \rho = U(1)$