Recall Defn of Groups.

A Group G. is a set with a binary operation.

$$G \times G \longrightarrow G.$$
$$(a, b) \longmapsto a \cdot b = ab$$

(1) Associativity $(ab)c = a(bc)$

(2) Identity $e \in G$, $e \cdot a = a \cdot e = a$.

(3) Inverse $\forall a \in G$, $\exists a^{-1} \in G$, s.t. $a \cdot a^{-1} = a^{-1} \cdot a = e$.

$\forall$: for any; $\exists$: there exists; s.t.: such that

$(\mathbb{R}, +)$

More example (Residue classes)

Fix n positive integer. $(\mathbb{Z}/n\mathbb{Z}, +)$.

$\mathbb{Z}/n\mathbb{Z}$ has n elements $\{\bar{0}, \bar{1}, \bar{2}, \dots \overline{n-1}\}$

$0 \le i, j \le n-1$, $\quad \bar{i}, \bar{j} \in \mathbb{Z}/n\mathbb{Z}$.

Then $\overline{i+j} = \bar{m}$, and $0 \le m \le n-1$.

$i+j \equiv m \mod n$.

Check $(\mathbb{Z}/n\mathbb{Z}, +)$ forms a group.

$(\mathbb{Z}/n\mathbb{Z}, +)$. "$+$" is commutative

More on symmetric groups.

S_n is viewed as bijective maps from the set of $\{1, 2 \dots n\}$ to itself.

S_n is a group under composition of maps

$f \in \mathrm{Perm}(n)$. $g \in \mathrm{Perm}(n)$

$$f \cdot g = f \circ g$$

$S_1 = \{e\}$. $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Multiplication table

	e
e	e

$e \cdot e = e$

$$S_2 = \left\{ e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

$e \cdot a = a \cdot e = a$, $e \cdot e = e$.

$\underline{a\cdot a} = a^2 = e$ $\quad\left(\underbrace{a\cdot a\cdots a}_{n} = a^n \right.$

$\quad$ if $\left. \underbrace{a^{-1}\cdots a^{-1}}_{n} = a^{-n} \right)$

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \\ 1 & 2 \end{array}$$

Multiplication table

	e	a
e	$e\cdot e$	$e\cdot a$
a	$a\cdot e$	$a\cdot a$

element on the right

	e	a
e	e	a
a	a	e

element on the left

S_3 has 6 elements

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $d = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$e\cdot g = g\cdot e = g$.

$$a^2 = c \qquad \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

$$a \cdot c = a^3 = e. \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \hline \end{array}$$

$$(a^4 = a^3 \cdot a = a, \dots)$$

$$b^2 = e \qquad \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \\ \hline 1 & 2 & 3 \\ \hline \end{array}$$

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f. \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$ba = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = d. \qquad b = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

$$a^2 b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = d. \qquad a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$e,\ a,\ a^2 = c,\ a^3 = e$

$b,\ b^2 = e.$

$ab = f. \quad ba = d = \underline{a^2 b}.$

$c \cdot b = a^2 b = d, \quad bc = b \cdot a^2 = b(aa)$

$= (ba) \cdot a = (a^2 b) \cdot a$

$$= a^2(ba) = a^2 \cdot (a^2 \cdot b)$$
$$= a^4 \cdot b = a^3 \cdot (a \cdot b)$$
$$= ab = f.$$

all the elements are in the form of

$a^m \cdot b^n$.

$$(a^m \cdot b^n)(a^i b^j) = a^k b^l.$$

How to find k, l. ($ba = a^2 b$).

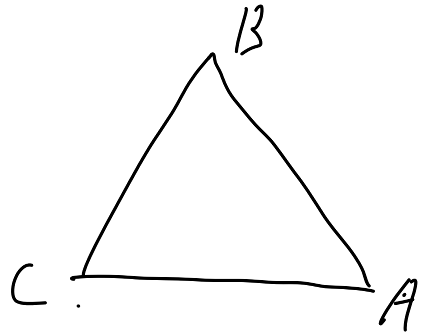
$$\left(a \cdots a\, b \cdots \underbrace{b\, a}_{\downarrow\, a^2 b} \cdots a \cdots b \cdots b \right)$$

In other words. e, $a^3 = e$, $b^2 = e$.

$$\underbrace{e, a, b, ab, a^2b, a^2}_{\text{together with } ba = a^2b.}$$

compare with symmetry of

equiliteral triangle



G = all the rotation and reflection symmetries of

Two groups are "the same".

The elements have different names in the two sets, but the "multiplication structures" are the same.

Defn (Group isomorphism).

Given two groups G_1, G_2.

a map $\rho: G_1 \to G_2$ is called a group isomorphism. if ρ is bijective and $\forall\ g, h \in G_1$,

$$\boxed{\rho(g)\cdot\rho(h) = \rho(gh)}$$

If such ρ exists,

G_1 and G_2 are isomorphic to each other.

This rule is for group homomorphism.

$$S_2 = \{ e,\ a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \}. \quad a^2 = e.$$

$$\mathbb{Z}/2\mathbb{Z} = \{ \bar{0},\ \bar{1} \} \quad \bar{1} + \bar{1} = \bar{2} = \bar{0}$$

$$\rho : S_2 \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

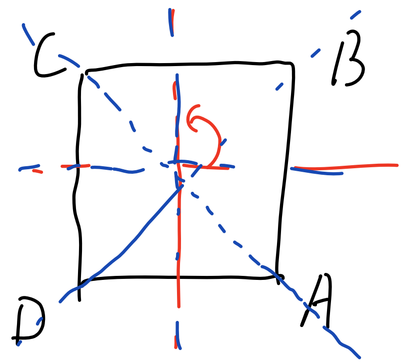
$$e \longmapsto \bar{0}$$

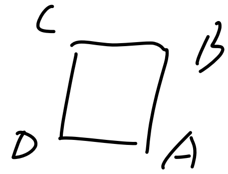
$$a \longmapsto \bar{1}.$$

ρ is a group isomorphism.

More symmetry groups.

Example (Symmetry of a square)



$G = \{$ reflection. rotation symmetries of 

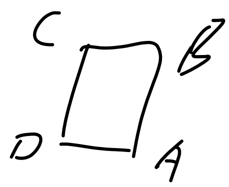
$\}$

4 rotations by $0°$, $90°$, $180°$, $270°$

4 reflections

order of a group

$|G|$ = number of elements in G. $= 8$.

$H = \{$ rotation symmetries of 

$\}$

H is also a group under composition

$|H| = 4$

H is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

$$
\begin{aligned}
\rho: H &\longrightarrow \mathbb{Z}/4\mathbb{Z} \\
e &\longmapsto \bar{0} \\
r_{90^\circ} &\longmapsto \bar{1} \\
r_{180^\circ} &\longmapsto \bar{2} \\
r_{270^\circ} &\longmapsto \bar{3}.
\end{aligned}
$$

ρ is a group isomorphism.

In this case. H is a subset of G.
and with the same multiplication operation.
H is a group itself. (subgroup).

Defn (subgroup). G is a group. $H \subset G$ a non-empty. subset of G, H is called a subgroup
if ① closed under multiplication
$\forall h_1, h_2 \in H$, then $h_1 h_2 \in H$.
② closed under inverse.
$\forall h \in H$, then $h^{-1} \in H$.

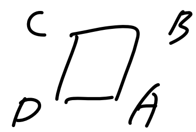
Remark: A subgroup H of a group G is also a group.

Pf: ① Associativity ✓

② Identity element Take $h \in H$, $h^{-1} \in H$

$h \cdot h^{-1} = e \in H$.

③ Inverse. ✓.

Non example: G = symmetries of 

K = all the reflections.

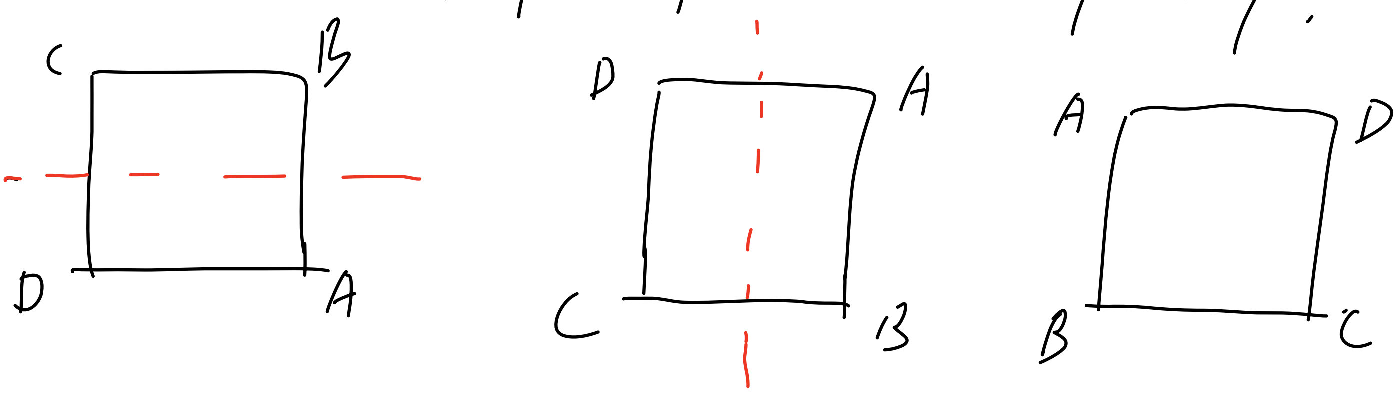
K is not a subgroup

$K \sqcup \{e\}$ is still not a subgroup

$K \sqcup \{e\}$ is closed under inverse.

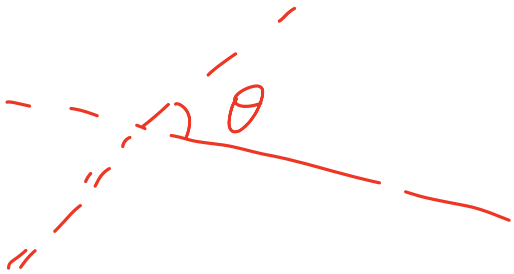
because if f is a reflection,

$$f \cdot f = f^2 = e. \quad f^{-1} = f.$$



Composition of these two reflections is a rotation by 180°.

$K \sqcup \sigma K$ is not closed under multiplication.



any two reflections composed gives a rotation by 2θ