Group : A group is an ordered pair $(G, *)$, where G is a set and $*$ is a binary operation on G satisfying the following axioms:

(i) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
[Associative]

(ii) there exists an element e in G such that for all $a \in G$,
[identity] element

$$a * e = e * a = a$$

(iii) for each $a \in G$, there is an element $a^{-1} \in G$.
[inverse of a]

such that

$$a * a^{-1} = a^{-1} * a = e$$

In short; $(G, *)$ with

(i) $*$ being associative

(ii) existence of identity element

(iii) inverse for every element in G

When $*$ is clear from the context; we shall simply say "Group G"
$(G, *)$

Question: Can a group $(G, *)$ be empty set (G) ?

Examples of Groups:

- $(\mathbb{Z}, +)$
  $(\mathbb{R}, +)$
  $(\mathbb{C}, +)$

$$\left.\begin{array}{l}(\mathbb{Z}, +)\\(\mathbb{R}, +)\\(\mathbb{C}, +)\end{array}\right\} \quad \begin{array}{l}e = ?\\a^{-1} =\end{array}$$

$$\left.\begin{array}{l}(\mathbb{Q}-\{0\}, \times)\\(\mathbb{R}-\{0\}, \times)\\(\mathbb{C}-\{0\}, \times)\\(\mathbb{Q}^{+}, \times)\\(\mathbb{R}^{+}, \times)\end{array}\right\} \quad \begin{array}{l}e =\\a^{-1} =\end{array}$$

$(\mathbb{Z}-\{0\}, \times)$

$(G=\{1, i, -1, -i\}, *)$

Suppose V is a finite dimensional vector space over $\mathbb{R}$;

say, $V = \mathbb{R}^n$

$(\mathbb{R}^n, +)$ $\quad e =$

$a^{-1} =$

$(GL_2(\mathbb{R}), \times)$, $\quad e =$

$a^{-1} =$

Recall : $(GL_2(\mathbb{R}), *)$

$\uparrow$ the set of 2x2 matrices, with non-zero determin-ant.

$A, B \in GL_2(\mathbb{R})$, then

$A * B$ is also in $GL_2(\mathbb{R})$

$\uparrow$ usual multiplication

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Given $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we know $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Definition $\rightarrow$ $(G, *)$ is a group, then

(i) $*$ (associative)

(ii) existence of identity element (e) ✓

(iii) existence of inverse for every element in G. ✓

How to check!!

May be we can directy verify

$$(A * B) * C = A * (B * C)$$

for any $A, B, C \in GL_2(\mathbb{R})$.

$\rightarrow$ This is doable but involves too much computation.

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

From where matrices come from ?

Matrix $\longleftrightarrow$ Linear Algebra

$$\dim V = n \qquad \dim W = m$$

$$T : V \longrightarrow W$$

A

there is a matrix of linear transform w.r.t. bases of V & W.

Theorem.

$$\left\{ \begin{array}{c} \text{Linear Transformation} \\ \text{from } V \text{ to } W \end{array} \right\} \xrightarrow[\text{correspondence}]{1-1} \left\{ \begin{array}{c} \text{Set of all} \\ m \times n \\ \text{matrices} \end{array} \right\}$$

$$V \xrightarrow{T_1} W \xrightarrow{T_2} X \xrightarrow{T_3} Y$$

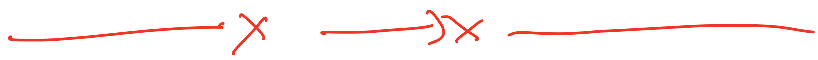
$$T_3 \circ (T_2 \circ T_1) = (T_3 \circ T_2) \circ T_1$$

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$$

$$h \circ (g \circ f) = (h \circ g) \circ f \qquad \underline{\underline{10+2}}$$

Is this true ?

<u>YES</u>



Multiplication

More generally, consider $(GL_n(\mathbb{R}), *)$

$n = 1$; $\quad GL_n(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

$n = 2$; we saw previous case

Let $n > 2$.

$$e = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{pmatrix}$$ is identity element.

Given $A \in GL_n(\mathbb{R})$,

by definition, A is invertible, hence

A^{-1} exists for every A.

Now we come to associativity condition:

$\boxed{(A * B) * C = A * (B * C)}$ for all

$A, B, C \in GL_n(\mathbb{R})$.

When n is large; this verification is too complicated (computational).

Question. Can we think of different way to approach?

How to think of matrices !!

Recall that matrix corresponds to a (linear) function $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$

Moreover, matrix multiplication corresponds to composition of such functions

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "A", "T_1"'] \arrow[rr, bend right, "T_2 \circ T_1"'] & \mathbb{R}^n \arrow[r, "B", "T_2"'] & \mathbb{R}^n \end{tikzcd} \qquad A \cdot B$$

If we want to check $A * B = B * A$;

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "A", "T_1"'] \arrow[rr, bend right, "T_2 \circ T_1"'] & \mathbb{R}^n \arrow[r, "B", "T_2"'] & \mathbb{R}^n \end{tikzcd} \qquad \begin{tikzcd} \mathbb{R}^n \arrow[r, "B", "T_2"'] \arrow[rr, bend right, "T_1 \circ T_2"'] & \mathbb{R}^n \arrow[r, "A", "T_1"'] & \mathbb{R}^n \end{tikzcd}$$

we are asking whether $T_2 \circ T_1 = T_1 \circ T_2$?

Note : If $A \in GL_n(\mathbb{R})$, then corresponding (linear) function or transformation is an isomorphism.

Question. Can we use the concept of isomorphism ?

Now; $(A * B) * C = A * (B * C)$

$$T_1 : \mathbb{R}^n \longrightarrow \mathbb{R}^n \rightsquigarrow A$$

$$T_2 : \mathbb{R}^n \longrightarrow \mathbb{R}^n \rightsquigarrow B$$

$$T_3 : \mathbb{R}^n \longrightarrow \mathbb{R}^n \rightsquigarrow C$$

$$T_3 \circ (T_2 \circ T_1) \overset{?}{=} (T_3 \circ T_2) \circ T_1$$

Lemma: Let
$$\left.\begin{array}{l} f : X \to Y \\ g : Y \to Z \\ h : Z \to W \end{array}\right\} \text{surjective maps.}$$

Then
$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof. Note that

$$\left.\begin{array}{l} h \circ (g \circ f) \\ (h \circ g) \circ f \end{array}\right\} : X \longrightarrow W$$

Take any element $x \in X$,

$$\begin{aligned} h \circ (g \circ f)(x) &= h((g \circ f)(x)) \\ &= h(g(f(x))) \end{aligned}$$

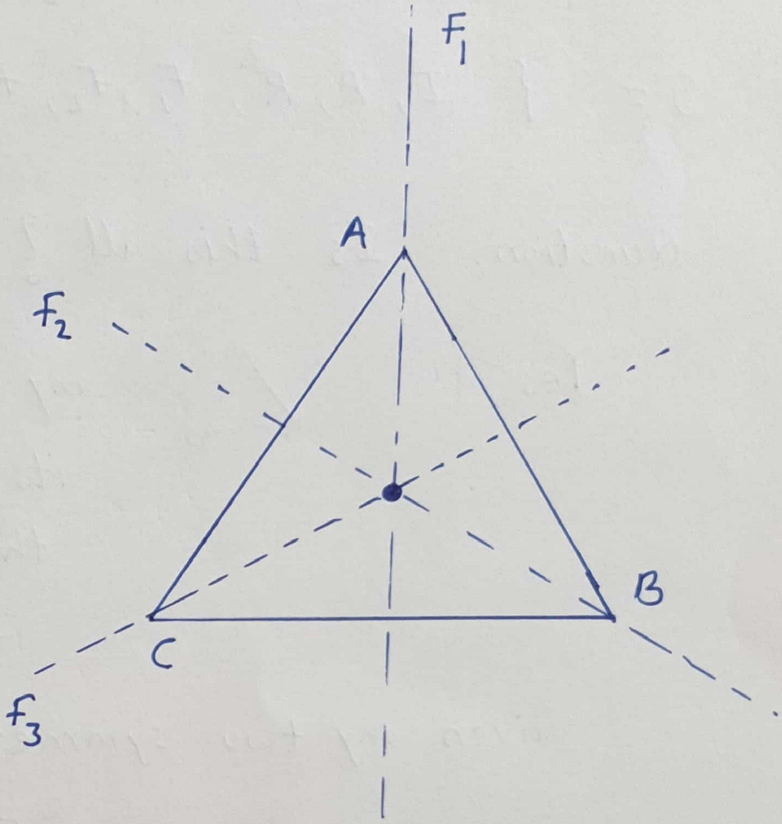
Now,
$$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \end{aligned}$$

This completes the proof.

Symmetries of an equilateral triangle.

If we rotate the triangle through 120°, denote this by "R".

Set : clockwise rotation as positive direction.



→ rotation by 240°

[It's like R^2,
(think of R^2 as the effect of applying R twice)

→ R^3 (then we are back where we started).

→ So, there is a trivial symmetry (say, $\underline{I}$).

Now; if we rotate by 120° anticlockwise
(may be represted by R^{-1})

So; $R^{-1} = R^2$.

Till Now; we have $\{ \; R, \; \underset{R^{-1}}{\overset{\|}{R^2}}, \; \underset{I}{\overset{\|}{R^3}} \; \}$

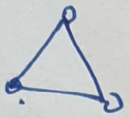
The other set of symmetries comes from flips.
With respect to line F_1, flip the triangle (call it F)
clearly $F^2 = I$ (flipping twice does nothing)

There are two other axes to flip about, corresponding to the fact that there are three corners.

The set of symmetries we have created so far is

$$S = \{ I, R, R^2, F_1, F_2, F_3 \}$$

Question. Is this all ?

Yes;  any symmetry is determined by its action on the vertices of the triangle.

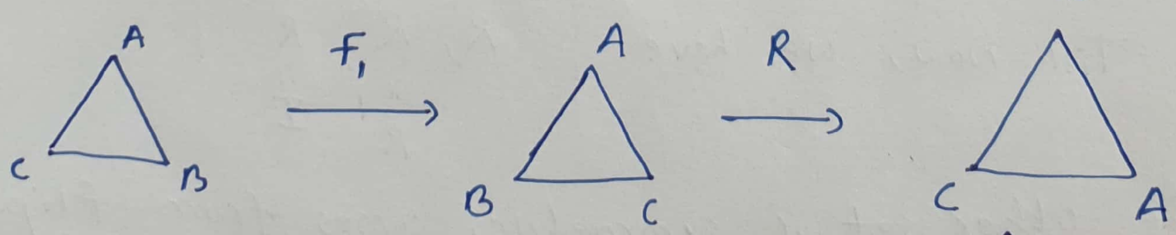
$3! = 6$.

Given any two symmetry in S, how to see

RF_1 or $R^2 F_2$?

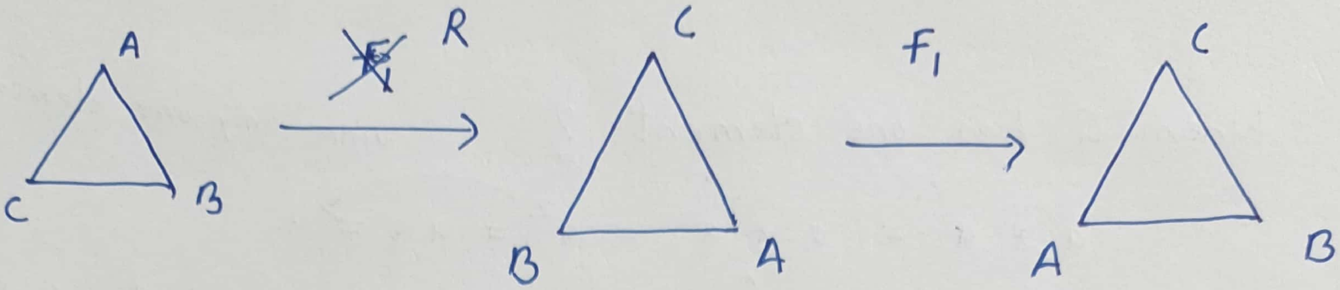
1^{st} we need to adopt the convention that RF means first apply F and then R.

Can you identify RF_1 ? (F_3)



we get this by F_3.

Can you identify $F_1 R$?



This is F_2.

Observe that

$$\underset{\overset{\parallel}{F_3}}{RF_1} \neq \underset{\overset{\parallel}{F_2}}{F_1 R}$$

Think of (algebraic) structure

$(G, *)$

the set of symmetries, operation on a set (how to multiply) in formal sense.

↳ Identity symmetry (I)

– this symmetry does nothing

$I * (\ )$ or $(\ ) * I$ remains unchanged

↳ Given any symmetry, there is an inverse symmetry

(e.g. R then R^{-1})

↳ Associativity !! (check this)

$(G, *)$

Question. Can this G be empty set ?

When G has one element ?

Since only one element

$a * a = a * a = a^2 = aa = a$

in G binary operation [a is identity]

Associativity ✓

Question When $G = \{a, b\}$, and define $*$ by

$a * a = a \qquad a * b = b$

$b * a = b \qquad b * b = a$

Is $(G, *)$ a group ?

Definition. $(G, *)$ is Abelion (commutative) if $a * b = b * a$ for every $a, b \in G$.

Example. Let $M_{m,n}(\mathbb{C})$ denote $m \times n$ matrices, with entries in $\mathbb{C}$.

$*$ is addition of matrices.

claim: $(M_{m,n}(\mathbb{C}), +)$ is a Group.

↪ 0 : zero matrix as identity

↪ $-A$; inverse of matrix A

↪ Associative [check entry by entry]

SUBGROUPS

Discussion. Recall the inclusion of groups

$$(\mathbb{Z},+) \underset{+}{\subsetneq} (\mathbb{Q},+) \underset{+}{\subsetneq} (\mathbb{R},+) \underset{+}{\subsetneq} (\mathbb{C},+)$$

Each subset is a group, and the group laws are obviously compatible.

$m, n \in \mathbb{Z}$,

$m+n$; we can think of m, n as rationals, reals or complex.

Definition. Let G be a group and let H be a subset of G. We say that <u>H is a subgroup of G</u> if the restriction to H of the rule $*$ (of multiplication) and inverse makes H into a group.

Remarks! $\longrightarrow$ (1) Suppose G is $(\mathbb{Z},+)$.

Let $H :=$ set of odd integer's $\subseteq \mathbb{Z}$.

Now, $x, y \in H$, then $\underset{\underset{\text{even}}{\shortparallel}}{x+y} \notin H$.

$\left\{ \text{+ is not a binary operation of arbitrary subset} \right.$

(2) Inverse of H need not be an element of H.

$$(\mathbb{Z}^+, +) \subseteq (\mathbb{Z}, +)$$

$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$

Take $x \in \mathbb{Z}^+$, then $x \in \mathbb{Z}$

so, $-x$ is inverse

but $-x \notin \mathbb{Z}^+$.

Example. $(2\mathbb{Z}, +) \subsetneq (\mathbb{Z}, +)$

Subgroup ?

In General, say given

$$(H, *) \subseteq (G, *)$$

How to check $(H,*)$ is a subgroup?

Definition. Let G be a group and let S be subset of G. We say that (i) S is closed under multiplication if whenever a and b are in S, then there product $(*)$ of a and b is in S.

(ii) S is closed under taking inverses, if whenever a is in S, then the inverse of a is in S.

Proposition. Let H be a non-empty subset of G.

Then H is a subgroup of G if and only if

H is closed under multiplication and taking inverse.

Furthermore, the identity element of H is the identity element of G,

inverse of an element of H is equal to the inverse element in G

Example.

Clearly $\underbrace{(2\mathbb{Z}, +) \subseteq (\mathbb{Z}, +)}_{\text{Subgroup}}$

Proof of Proposition.

$\Rightarrow$ H is a subgroup, then H is closed under multiplication and taking inverses (by defintion)

$\Leftarrow$ Suppose that H is closed under multiplication and taking inverses.

(we will check axioms of a group)

1st note that associativity holds

$$\underbrace{a * (\underbrace{b*c}_{\in H})}_{\in H} \overset{?}{=} \underbrace{(\underbrace{a*b}_{\in H}) * c}_{\in H} \quad \text{for all } \underbrace{a, b, c}_{\in G} \in H$$

(why)

"identity" We have to show that H contains an identity element.

Since $H \neq \phi$, pick some $a \in H$.

Given, H is closed under taking inverses, this implies $a^{-1} \in H$.

But $\underbrace{a a^{-1}}_{\substack{\in H \\ \text{(hypothesis)}}} = \underline{\underline{e \in H}}$

This e acts as an identity element in H as it is identity element in G.

"inverse"

Suppose that $h \in H$.

Then $h^{-1} \in H$ (hypothesis) closed under taking inverses.

This h^{-1} is in fact invert of h in H as it is the inverse in G.

$\square$

Examples of subgroup.

(i) $M_{m,n}(\mathbb{Z}) \subset M_{m,n}(\mathbb{Q}) \subset M_{m,n}(\mathbb{R}) \subset M_{m,n}(\mathbb{C})$

(ii) $GL_n(\mathbb{Q}) \subset GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$