# Lecture 4 (Introduction to Group Theory)

Jan 11, 2022

## Revision.

$*$

$f : G \times G \to G$

$(a,b) \mapsto f(a,b) \in G$

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

$(a*b)*c = a*(b*c)$

(i) $f(f(a,b),c) = f(a, f(b,c)) \quad \forall\, a,b,c \in G$

(ii) Existence of identity element in $G$

$f(a,e) = f(e,a) = a$

$\exists\, e \in G \ni \forall\, a \in G,\; a * e = e * a = a.$

There exists — such that — for all — identity element

(iii). Existence of inverse element for every element in $G$

$f(a,a^{-1}) = f(a^{-1},a) = e$

$\forall\, a \in G,\; \exists\, a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e.$

For all or for every — There exists — such that — inverse element — identity

**Set-up.** When binary operation $f$ (or $*$) is clear from the context, we shall simply say "Group $G$".

Examples.

1. $(\mathbb{R}, +)$

map (binary operation)

cartesian product

map

$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$(r_1, r_2) \longmapsto +(r_1, r_2)$

defined as $\quad \| $

$r_1 + r_2 \in \mathbb{R}$

usual addition in $\mathbb{R}$

$+$ is binary operation on $\mathbb{R}$

$\mathbb{R}$ is a non-empty set

(i) $+$ is associative

$$+(\underbrace{+(r_1, r_2)}_{r_1+r_2}, r_3) = +(r_1, +(r_2, r_3))$$

$$r_1 + r_2 + r_3 = r_1 + r_2 + r_3$$

(ii) $0 \in \mathbb{R} \ni \forall r \in \mathbb{R}$, we have

Identity element

$$+(r, 0) = +(0, r) = r$$

$$r + 0 = 0 + r = r$$

(iii) $\forall r \in \mathbb{R}, \exists -r \in \mathbb{R} \ni +(r, -r) = +(-r, r) = 0$

Inverse element

$$r + (-r) = (-r) + r = 0$$

$(\mathbb{Z}, +)$, $(\mathbb{C}, +)$ etc.

2. $(\mathbb{R}-\{0\}, \times)$

map

usual multiplication

map (binary operation)

Cartesian Product of set

$$\times : (\mathbb{R}-\{0\}) \times (\mathbb{R}-\{0\}) \longrightarrow \mathbb{R}-\{0\}$$

$$(\alpha, \beta) \longmapsto \times(\alpha,\beta)$$

defined as $\Leftarrow\Big\{ \;\; \overset{\cdot\cdot}{\Vert}$

$\alpha \cdot \beta$

$\in \mathbb{R}-\{0\}$

usual multiplication of real numbers

$\times$ is a binary operation on $\mathbb{R}-\{0\}$.

$\mathbb{R}-\{0\}$ is a non-empty set

(i) $\times$ is associative

$$\times(\times(\alpha,\beta),\gamma) = \times(\alpha, \times(\beta,\gamma))$$

(ii) $1 \in \mathbb{R}-\{0\} \ni \forall\ \gamma \in \mathbb{R}-\{0\}$, we have

$$\times(\gamma,1) = \times(1,\gamma) = \gamma$$

$$\Vert$$

$$\gamma \cdot 1 = 1\cdot\gamma = \gamma$$

(iii) $\forall\ \gamma \in \mathbb{R}-\{0\},\ \exists\ \frac{1}{\gamma} \in \mathbb{R}-\{0\}$

$$\ni \times\left(\gamma, \frac{1}{\gamma}\right) = \times\left(\frac{1}{\gamma},\gamma\right) = 1$$

$(\mathbb{Q}-\{0\}, \times)$, $(\mathbb{C}-\{0\}, \times)$, etc.

3. $(M_n(\mathbb{R}), +)$

$M_n(\mathbb{R})$ is the set of all $n \times n$ matrices

$$+ : M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$$

defined as

map (binary operation)

$$(A, B) \longmapsto +(A,B) := A + B$$

map

Addition of matrices in $M_n(\mathbb{R})$

Check. $(M_n(\mathbb{R}), +)$ is a Group.

$(M_{m,n}(\mathbb{R}), +)$ or $(M_{m,n}(\mathbb{Q}), +)$ etc.

4. $(GL_2(\mathbb{R}), \times)$

[In general, we can work with $(GL_n(\mathbb{R}), \times)$]

$GL_2(\mathbb{R})$ is the set of all $2 \times 2$ matrices with non-zero determinant.

$\sim$ set of all $2 \times 2$ invertible matrices over $\mathbb{R}$

Cartesian product

usual multiplication

$$\times : GL_2(\mathbb{R}) \times GL_2(\mathbb{R}) \longrightarrow GL_2(\mathbb{R})$$

map (binary operation)

$$(A, B) \longmapsto \times(A,B) := A \cdot B \in GL_2(\mathbb{R})$$

$\det(AB) = \det(A) \cdot \det(B) \Longrightarrow$

(i) $\times$ is associative

$$\times(\times(A,B),C) = \times(A, \times(B,C))$$

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

(ii) $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) \ni \forall\ \cancel{X}\ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$

we have

map

$$\cancel{\times(X,e)} = \times(A,e) = \times(e,A) = A.$$

$$A\cdot e = e\cdot A = A$$

(iii) $\forall\ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R}),\ \exists\ A^{-1} = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$\in GL_2(\mathbb{R})$

$$\Rightarrow \quad \times(A, A^{-1}) = \times(A^{-1},A) = e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

$(GL_n(\mathbb{R}), \times)$ or $(GL_n(\mathbb{Q}), \times)$ etc.

**Discussion.** $\qquad \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

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

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

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

We can think of $m, n$ as rationals, reals, or complex.

$\neq \phi \qquad f$

**Definition.** Let $(G, *)$ be a group. Let $H$ be a non-empty subset of $G$. We say that <u>$H$ is a subgroup of $G$</u> if the restrictions to $H$ of the rule $*$ and inverse makes $H$ into a group.

Discussion.

1. Let $G = (\mathbb{Z}, +)$.

$(H, +)$

$1+3 \notin H$

Set $H :=$ set of odd integers in $\mathbb{Z}$

$\{\pm 1, \pm 3, \pm 5, \dots\}$

Take $m, n \in \mathbb{Z}$, ~~then~~ with $m, n \in H$,

but $m + n \notin H$

$+$ is not a binary operation on $H$.

$$+ : H \times H \longrightarrow H$$
$$(1, 3) \longmapsto 4 \notin H$$

2. Let $G = (\mathbb{Z}, +)$ and set $H = (\mathbb{Z}_{\geq 1}, +)$

$\mathbb{Z}_{\geq 1} = \mathbb{N}$

$= \{1, 2, 3, \dots\}$

Take $m \in \mathbb{Z}$ such that $m \in H$,

then $-m$ is inverse in $G$,

but $-m \notin H$

$H_2 = (3\mathbb{Z}, +)$

3. $H_1 = (2\mathbb{Z}, +) \leq (\mathbb{Z}, +) = G$

Is this a subgroup? YES


When H is a subgroup?

**Question.** Given a group $(G,*)$, how to check

$(H,*) \subseteq (G,*)$ is a subgroup?

( Setting up language )

**Definition.** Let $(G,*)$ be a group. Let $S$ be a non-empty subset of $G$. We say that

- $S$ is closed under multiplication, if whenever $a, b \in S$, then $a * b \in S$

  $f(a,b) \in S$

- $S$ is closed under taking inverses, if whenever $a \in S$, then $a^{-1} \in S$.

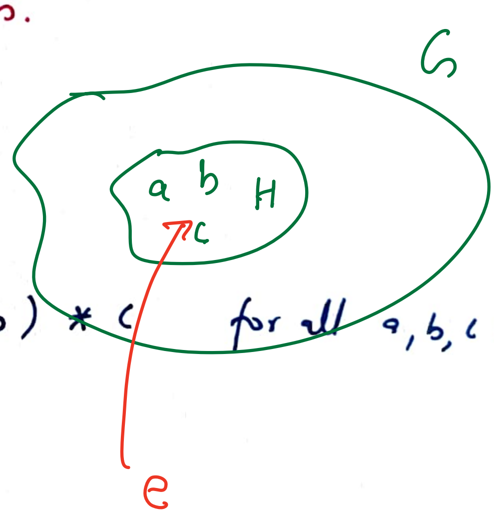
**Proposition.** Let $(G, *)$ be a group, and $H$ be a non-empty subset of $G$. Then

$H$ is a subgroup of $G$ $\iff$ $H$ is closed under multiplication and taking inverses.

**Proof.**

$\Longrightarrow$ (Holds by definition)

$\Longleftarrow$ Claim. $H$ is a subgroup of $G$. $\qquad *: H \times H \to H$




(i) $*$ is associative on $H$

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

(ii) To show identity element is in $H$.

Pick some element $a \in H$.

Then $a^{-1} \in H$

$\Rightarrow a * a^{-1} \in H$ $\Big\}$ By hypothesis

We know that $a * a^{-1} = e$, hence $e \in H$

[ The same $e$ acts as an identity element in $H$ as it is identity element in $G$

(iii) To show inverse exists for every $h \in H$.

[ Holds by hypothesis ].

Examples.

$$(2\mathbb{Z}, +) \subseteq (\mathbb{Z}, +)$$

$$M_{m,n}(\mathbb{Z}) \underset{+}{\subseteq} M_{m,n}(\mathbb{Q}) \underset{+}{\subseteq} M_{m,n}(\mathbb{R}) \subseteq M_{m,n}(\mathbb{C})$$

$$GL_n(\mathbb{Q}) \subseteq GL_n(\mathbb{R}) \subseteq GL_n(\mathbb{C})$$

$\{g_1, g_2, \dots, g_k\}$

$=$

$H \subseteq G$

**Lemma.** Let $G$ be a finite group and $H$ be a non-empty finite set closed under multiplication. Then $H$ is a subgroup of $G$.

**Discussion.**

$(G, *)$ finite group

[To show given any $a \in H \Rightarrow a^{-1} \in H$]

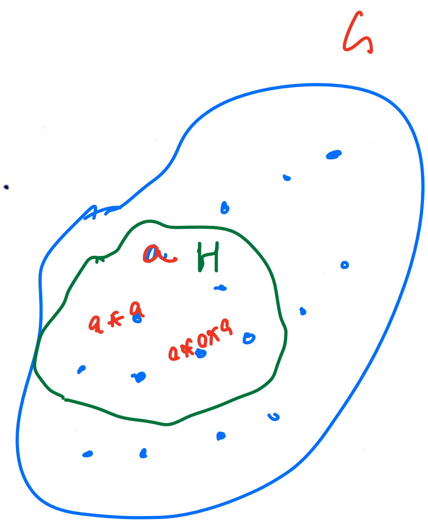
$\Uparrow$

$H$ is a subgroup of $G$ $\Longleftrightarrow$ $H$ is closed under multiplication and taking inverses.

Thus, to prove Lemma, it suffices to prove that $H$ is closed under taking inverses.

**Proof.** Since $H \neq \phi$, let $a \in H$.

If $a = e$, then $a^{-1} = e \in H$.



Assume that $a \neq e$. To show $a^{-1} \in H$

Consider the elements $\{a, \underset{\substack{\| \\ a \times a}}{a^2}, a^3, \dots\dots \}$ finite set

$a^n = a * \cdots * a \in H$ for all $n \geq 1$.

As, $H$ is a finite set and $\{a, a^2, a^3, \dots\}$ has infinitely many collection,

$\exists\ m, n \in \mathbb{Z}$ s.t. $\underline{\underset{\in H \subseteq G}{a^m} = \underset{\in H \subseteq G}{a^n}}$

(Assume $m < n$)

$\underbrace{a^{-m}}_{\text{inverse of } a^m \text{ in } G} \cdot a^m = a^{-m} \cdot a^n$

$\quad\ \ \|$

$\quad\ e = a^{n-m}$

$\quad\ e = \underbrace{a^{n-m-1}}_{\in H} \cdot a$

$a * b = e = b * a$

Similarly, $a \cdot a^{n-m-1} = e$

Hence $a^{n-m-1}$ is inverse of $a$. (in $H$)

Thus $H$ is closed under taking inverses.

$\Rightarrow$ $H$ is a subgroup of $G$.