Lecture 10 : Introduction to Group Theory

January 29, 2022

Quick Revision.

Group Isomorphism.

A map $\varphi : (G, *_1) \longrightarrow (G', *_2)$ is an isomorphism

if φ is bijective and

$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ [i.e. φ preserves group operation]

Isomorphic Group. Two groups G and G' are isomorphic

if there exists an isomorphism $\varphi : G \to G'$.

$G \cong G'$ or $G \approx G'$

Examples.

1. $G \approx G$ via identity map $id : G \to G$

2. $(\mathbb{Z}, +) \approx \langle a \rangle$ infinite cyclic group generated by a

$\varphi : n \longmapsto a^n$

$\langle a \rangle = \langle \ldots, a^{-1}, a^0, a, a^2, \ldots \rangle$, $a^0 = e$

3. $G = \{1, x, x^2, \dots, x^{n-1}\} = \langle x \rangle$ $\quad$ $\mathrm{ord}(x) = n$

$G' = \{1, y, y^2, \dots, y^{n-1}\} = \langle y \rangle$ $\quad$ $\mathrm{ord}(y) = n$

Then $G \approx G'$ via

$$\varphi : (G, \cdot) \longrightarrow (G', \cdot)$$
$$x \longmapsto y$$

Observation. Cyclic groups of the same order are isomorphic.

4. $(\mathbb{R}, +) \approx (\mathbb{R}_{>0}, \cdot)$

$$\varphi : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$$
$$x \longmapsto e^x$$

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x)\,\varphi(y)$$

5. $(\mathbb{R}, +) \approx \left(\left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \;\middle|\; x \in \mathbb{R} \right\}, \cdot \right)$

 $\| \qquad\qquad\qquad\qquad (G', \cdot)$

$(G, +)$

$$\varphi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

6. $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$

$$x \longmapsto x^n$$

isomorphism if $n = 1$,

otherwise NO

7. Exercises.

(a) $(\mathbb{Q}, +) \overset{?}{\approx} (\mathbb{Q} - \{0\}, \cdot)$

(b) $(\mathbb{R}, +) \overset{?}{\approx} (\mathbb{Q}, +)$

(c) $(\mathbb{R} - \{0\}, \cdot) \overset{?}{\approx} (\mathbb{C} - \{0\}, \cdot)$

(d) $(\mathbb{Z}, +) \overset{?}{\approx} (\mathbb{Q}, +)$

Properties of Isomorphisms.

1. $\varphi : G \longrightarrow G'$ is an isomorphism, then

(a) $\varphi(1_G) = 1_{G'}$

(b) $\varphi(a^n) = \varphi(a)^n$ for all $n \in \mathbb{Z}$

(c) for any $a, b \in G$

$$\boxed{a * b = b * a} \iff \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$$

(d) $$\underset{\text{Cyclic}}{G = \langle a \rangle} \iff \underset{\text{Cyclic}}{G' = \langle \varphi(a) \rangle}$$

(e) $\varphi : G \longrightarrow G'$ isomorphism

then $o(a) = o(\varphi(a))$ for every $a \in G$

(f) Fix $k \in \mathbb{Z}$ and $b \in G$.

$x^k = b$ has same number of solution in G

as $x^k = \varphi(b)$ in G'

(g) If G is finite, then G and G' have exactly

same number of elements of every order.

Lecture 10

Example. Let b be a fixed element of G, then define

$$\varphi : G \longrightarrow G$$
$$a \longmapsto \varphi(a) = bab^{-1}$$

[conjugation by b]

Claim. φ is an isomorphism.

one-one. $\varphi(x) = \varphi(y)$

$\Rightarrow bxb^{-1} = byb^{-1}$

$\Rightarrow x = y$ [Use cancellation law]

onto. Let $y \in G$ be an arbitrary element in G.

Want. $\varphi(\text{—}) = y$

$$\varphi(b^{-1}yb) = bb^{-1}ybb^{-1} = y$$

Assume
$\varphi(x) = y$
$bxb^{-1} = y$
$\Rightarrow x = b^{-1}yb$

φ preserves group operation

$$\varphi(xy) = bxyb^{-1}$$
$$= bxb^{-1}byb^{-1}$$
$$= \varphi(x)\varphi(y)$$

$$\varphi(1_G) = b \cdot 1_G \cdot b^{-1} = 1_G \cdot b \cdot b^{-1} = 1_G$$

Automorphism. An isomorphism $\varphi : G \to G$ (i.e. group to itself) is called an *automorphism* of G.

Example.

1. The identity map $1_G : G \to G$, $a \mapsto a$ is always an isomorphism.

   Hence an automorphism.

Note. For a given group, there can be many automorphisms.

2. For any fixed $b \in G$, define

$$\varphi_b : G \to G$$
$$a \mapsto \varphi(a) = bab^{-1}$$

is an automorphism.

Remark. Assume that G is abelian [$ab = ba$ for all $a, b \in G$]

then

$$\varphi_b(a) = bab^{-1} = abb^{-1} = a$$

$$\Rightarrow \varphi_b = 1_G$$

(conjugation becomes identity in abelian group)

$$1_G : G \longrightarrow G \qquad \text{and} \qquad \varphi_b : G \longrightarrow G$$
$$a \longmapsto a \qquad\qquad\qquad\qquad a \longmapsto bab^{-1}$$

are different isomorphisms provided, the group is non-abelion.

~~non~~

Define.

$$\mathrm{Aut}(G) = \{ \varphi : G \to G \text{ such that } \varphi \text{ is an isomorphism} \}$$

Set consisting of ~~group~~ group isomorphism from G to G

Exercise.

$(\mathrm{Aut}(G), \circ)$ is a group

composition of function

$\varphi \in \mathrm{Aut}(G)$

$\varphi : G \longrightarrow G$ isomorphism

$\varphi^{-1} \in \mathrm{Aut}(G)$

? φ^{-1} an isomorphism

$\varphi^{-1} : G \to G$

$\varphi^{-1}(\alpha\beta) = \varphi^{-1}(\alpha)\varphi^{-1}(\beta)$

Exercise. $\varphi : G \to G'$ is an isomorphism, then

Prove that

(i) $\varphi^{-1} : G' \longrightarrow G$ is also an isomorphism.

(ii) G is cyclic $\iff$ G' is cyclic

$$G = \langle a \rangle \qquad G' = \langle \varphi(a) \rangle$$

Conjugate element. Let G be a group. The element bab^{-1} is called the conjugate of a by b.

Definition. Two elements a and a' of a group G are called conjugate if $a' = bab^{-1}$ for some $b \in G$.

Note. Such conjugate elements define automorphisms.

Examples.

$= \{ A \in M_2(\mathbb{R})$ such that $\det(A) = 1 \}$

$(SL_2(\mathbb{R}), \cdot)$

1. $$\varphi_B : SL_2(\mathbb{R}) \longrightarrow SL_2(\mathbb{R})$$
$$A \longmapsto BAB^{-1}$$ for some fixed $B \in SL_2(\mathbb{R})$

Is φ_B an isomorphism? YES

Yes, $SL_2(\mathbb{R})$ is not relevent here. Any group G with $\varphi_b : G \longrightarrow G$ sending $a \longmapsto bab^{-1}$ is an isomorphism

2. $$\varphi_B : GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$$
$$A \longmapsto BAB^{-1}$$

Homomorphism.

Let $(G, *_1)$ and $(G', *_2)$ be groups. A homomorphism $\varphi : G \longrightarrow G'$ is a map that preserves the group operation, i.e.,

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b) \quad \text{for all } a, b \in G.$$

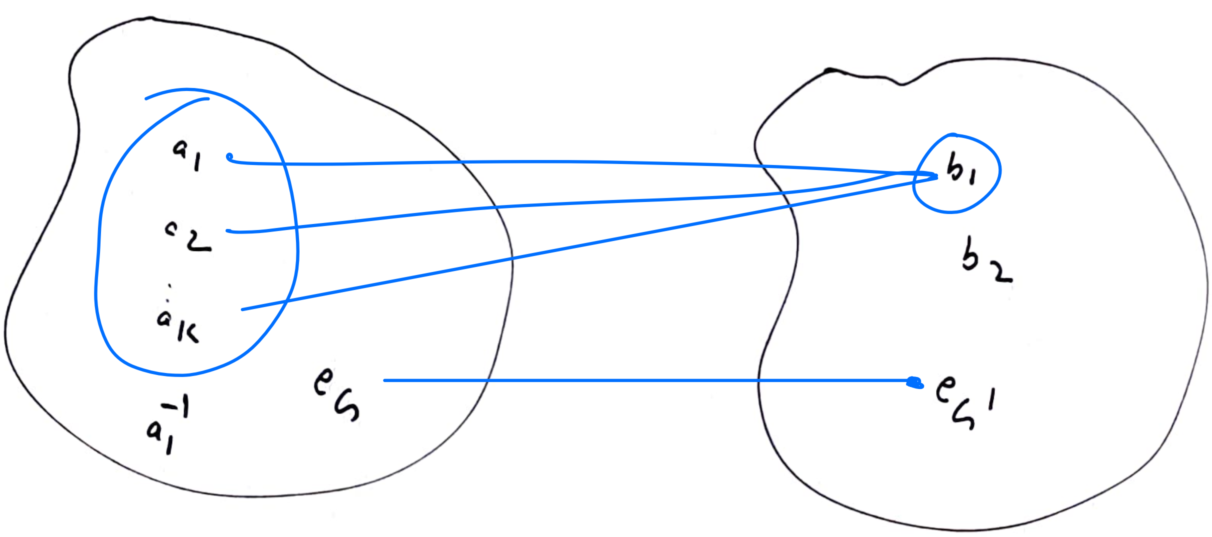
Note.

1. φ need not be bijective map.

$$\Downarrow$$

φ need not be 1-1 always

Figure for Illustration



Proposition. A group homomorphism caries

$$\varphi : G \longrightarrow G'$$

$$1_G \longmapsto 1_{G'} \quad \text{identity to identity}$$

$$a^{-1} \longmapsto \varphi(a)^{-1} \quad \text{inverse to inverse}$$

Proof.

$1_G = 1_G \cdot 1_G$, then

$$\varphi(1_G) = \varphi(1_G) \cdot \varphi(1_G)$$

$$\Rightarrow \quad \varphi(1_G)^{-1} \cdot \varphi(1_G) = \underbrace{\varphi(1_G)^{-1} \varphi(1_G)}_{} \cdot \varphi(1_G)$$

$$1_{G'} \cdot \varphi(1_G)$$

$$\Rightarrow \quad 1_{G'} = \varphi(1_G).$$

Similarly

$$\varphi(a^{-1})\, \varphi(a) = \varphi(a^{-1} a)$$

$$= \varphi(1_G) = 1_{G'}$$

$$\Rightarrow \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

Examples.

1. Group isomorphisms are always group homomorphisms.

2. Let $G = (\mathbb{R} - \{0\}, \cdot)$

(a) $\varphi_1 : G \longrightarrow G$

$x \longmapsto |x|$

$\varphi_1(xy) = \varphi_1(x) \cdot \varphi_1(y)$

$\ker \varphi_1 = \{1, -1\}$

(b) $\varphi_2 : G \longrightarrow G$

$x \longmapsto x^2$

$\varphi_2(xy) = \varphi_2(x)\varphi_2(y)$

$\|$

$(xy)^2 = x^2 y^2$

3. $\varphi : GL_2(\mathbb{R}) \longrightarrow G = (\mathbb{R} - \{0\}, \cdot)$

$A \longmapsto \det(A)$

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

Let $\varphi : G \longrightarrow G'$ be group homomorphism.

Define

1. $\ker \varphi = \{ a \in G \text{ such that } \varphi(a) = 1_{G'} \} = \varphi^{-1}(1_{G'})$. $\subseteq G$

2. $\operatorname{Im} \varphi = \{ b \in G' \text{ such that } b = \varphi(a) \text{ for some } a \in G \}$

Exercise. $\ker \varphi$ and $\operatorname{Im} \varphi$ are subgroups in G and G' respectively.

$\underline{\underline{\ker \varphi}}$

We will verify $\ker \varphi$ is a subgroup of G.

Recall

$\underline{\underline{\phi \neq H}} \subseteq G$ is a subgroup of G if

(i) If $a \in H, b \in H$, then $ab \in H$

(ii) $1 \in H$

(iii) If $a \in H$, $a^{-1} \in H$

(i) Let $a, b \in \ker \varphi$

$\Rightarrow \varphi(a) = 1_{G'}$ and $\varphi(b) = 1_{G'}$

Now $\varphi(ab) = \varphi(a)\varphi(b) = 1_{G'} \cdot 1_{G'} = 1_{G'}$

$\Rightarrow ab \in \ker \varphi$.

(ii) Is it true that $1_G \in \ker\varphi$?

[We have done this part before, $\varphi(1_G) = 1_{G'}$]

(iii) For every $a \in G$, $a^{-1} \in G$ and

$$\varphi(a \cdot a^{-1}) = \varphi(a)\,\varphi(a^{-1})$$

$$\Rightarrow \quad \varphi(1_G) = \varphi(a) \cdot \varphi(a^{-1})$$

$$\Rightarrow \quad 1_{G'} = \underset{1_{G'}}{\underset{\shortparallel}{\varphi(a)}}\,\varphi(a^{-1})$$

If $a \in \ker\varphi$, then $\varphi(a) = 1_{G'}$

$$\Rightarrow \quad \varphi(a^{-1}) = 1_{G'}$$

Thus, $\ker\varphi$ is a subgroup of G.

Similarly, Prove that $\mathrm{Im}(\varphi)$ is also a subgroup of G'.