Lecture 17

In this lecture, we're going to start the study of isomorphism and homomorphism. In the course, so far, we've tried to devise ways in which we can understand the nature and the structure of a group in more detail. The study of subgroups, provided details about the group by giving us information on what types of subgroups can occur in a group. For cyclic groups, we were able to completely classify the subgroups that a group can have.

Then we were led into the study of cosets and then the Lagrange's Theorem, which put a lot of restriction on the possibilities of a subset to be a subgroup.

Finally, we studied normal subgroups and quotient groups which again led to a better understanding of the group.
The notion of homomorphism and isomorphism are two such notions which help in understanding groups in a better way.

Isomorphism

Suppose we have two groups G and $\overline{G}$. We want to compare them, i.e., how different are G and $\overline{G}$ from each other. We won't care about how the elements in G and $\overline{G}$ "look like" but rather, we are interested in how similar the group-theoretic properties are in G and $\overline{G}$.

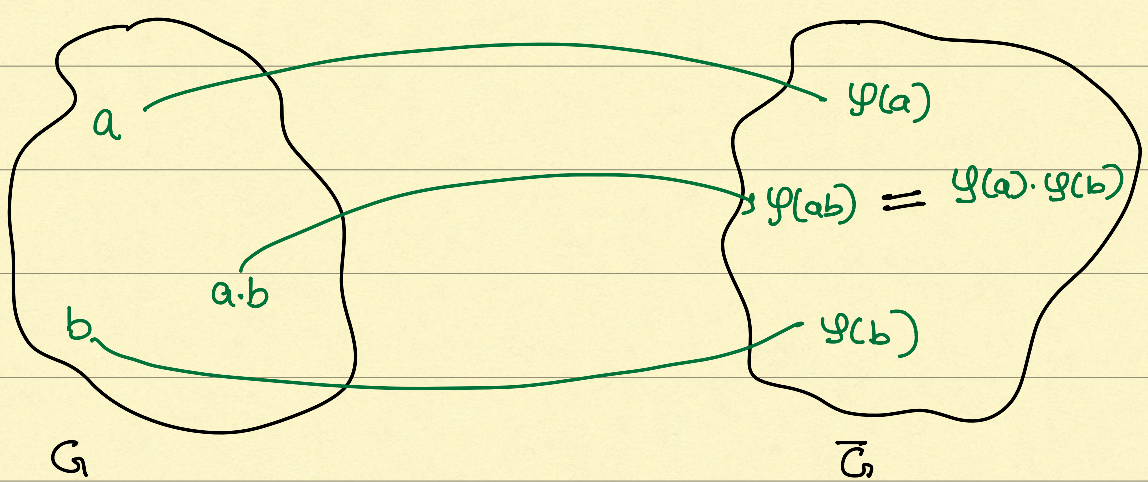
If we want G and $\bar{G}$ to be alike, we first of all want them to have same "number" of elements. This can be achieved by saying that $\exists$ a bijection b/w them, say φ

$$\varphi : G \longrightarrow \bar{G}$$

φ is one-one and φ is onto.

But this just takes care of the set-theoretic properties of G and $\bar{G}$. What about the group-theoretic properties?

Let's understand this via a figure



We have $a, b \in G$ and hence $a \cdot b \in G$.

Now we have the map $\varphi : G \to \overline{G}$, so we can look at $\varphi(a) \in \overline{G}$, $\varphi(b) \in G$ and $\varphi(a \cdot b) \in \overline{G}$.

But $\overline{G}$ is also a group, so we can combine $\varphi(a)$ and $\varphi(b)$ in $\overline{G}$, to get $\varphi(a) \cdot \varphi(b)$

We say that φ preserves the group operation if $\forall\ a, b \in G$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Note that on the LHS, $\cdot$ is the group operation in G while on the RHS $\cdot$ is the group operation in $\overline{G}$.

Def Let G and $\overline{G}$ be groups. We say that a map $\varphi : G \to \overline{G}$ is an isomorphism if

1) φ is a bijection.

2) φ preserves group operation, i.e.,

$\forall\, a, b \in G, \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

If such a φ exist then we say that G and $\overline{G}$ are isomorphic and write $G \cong \overline{G}$.

So in order to prove that two groups G and $\overline{G}$ are isomorphic, one has to follows 3 steps:—

1. Come up with a candidate for $\varphi : G \to \overline{G}$.

2. Show that φ is a bijection. [One also has to show that φ is well-defined if there are more than one representative for elements in G, e.g. when G is a quotient group]

3. Show that φ preserves the group operation, i.e., $\forall\, a, b \in G, \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Examples :-

① Every cyclic group $G = \langle a \rangle$ such that $|G| = \infty$ is isomorphic to $(\mathbb{Z}, +)$.

We know that $\mathbb{Z} = \langle 1 \rangle$. So, whenever we want to study any property of a cyclic group, we should focus only on the generator.

So, a candidate for $\varphi : G \to \mathbb{Z}$ is

$\varphi(a) = 1$, i.e, map the generator for G to the generator of $\mathbb{Z}$.

An arbitrary element of G looks like $a^k, k \in \mathbb{Z}$, so $\varphi(a^k) = k$.

One can check that φ is a bijection.

Also, for $x, y \in G$, $x = a^m, m \in \mathbb{Z}$

$y = a^n, n \in \mathbb{Z}$

$\Rightarrow \varphi(x \cdot y) = \varphi(a^m \cdot a^n) = \varphi(a^{m+n}) = m+n = \varphi(x) \cdot \varphi(y)$

so φ preserves the group operation and hence

$G \cong \mathbb{Z}$.

② Every cyclic group $G = \langle a \rangle$ such that $|G| = n$ is isomorphic to $\mathbb{Z}_n$.

Again, let's look at generators :- $\mathbb{Z}_n = \langle 1 \rangle$ where 1 is mod n.

So, define $\varphi : G \longrightarrow \mathbb{Z}_n$ by $\varphi(a) = 1 \bmod n$ or more generally, $\varphi(a^k) = k \bmod n$.

φ is a bijection. [Check]

for $x = a^m \in G$, $y = a^l \in G$,

$$\varphi(x \cdot y) = \varphi(a^{m+l}) = m + l \bmod n = m \bmod n + l \bmod n$$
$$= \varphi(x) \cdot \varphi(y)$$

and hence φ is a bijection.

Let's see a concrete example of the above

phenomena. Consider the group $U(10) = \{1, 3, 7, 9\}$
Then $U(10) = \langle 3 \rangle$ and $|U(10)| = 4$, so $U(10)$ must be isomorphic to $\mathbb{Z}_4$.

A concrete isomorphism is $\varphi : U(10) \to \mathbb{Z}_4$, $\varphi(3) = 1$ and hence $\varphi(9) = 2$, $\varphi(7) = 3$ and $\varphi(1) = 0$.

7 is also a generator of $U(10)$. So one can also map 7 to 1.

Now, we know many examples of groups, whose order are different and hence there is no chance of them being isomorphic.

Also, it can happen that two groups have same order but any bijection b/w them do not preserve the group operation.

So, it makes sense to weaken the notion of an isomorphism, but still take care of the group theoretic properties. This is precisely the notion of homomorphism.

Defn :- Let G and $\bar{G}$ be groups. A map $\varphi : G \to \bar{G}$ is called a homomorphism if φ preserves the group structure, i.e,

$$\forall\ a, b \in G, \quad \varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$$

So an isomorphism is just a homomorphism which is also a bijection.

Any isomorphism is a homomorphism but the converse is not necesarilly true.

Examples :-

① Consider $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, given by

$\varphi(a) = a \bmod n$.

We see that $\varphi(a+b) = a+b \bmod n$

$= a \bmod n + b \bmod n$

$= \varphi(a) + \varphi(b)$ (or $\varphi(a) \cdot \varphi(b)$

as $\cdot$ is $+$ in $\mathbb{Z}_n$)

So φ is a homomorphism. However, clearly φ is not an isomorphism.

② Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$ under multiplication and let $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ be given by

$\varphi(x) = |x|$. Then for $x, y \in \mathbb{R}$,

$\varphi(x \cdot y) = |x \cdot y| = |x| \cdot |y| = \varphi(x) \cdot \varphi(y)$. So φ is a homomorphism.

③ Consider $\varphi : GL(2, \mathbb{R}) \to \mathbb{R}^*$, given by

$\varphi(A) = \det A$. Then for $A, B \in GL(2, \mathbb{R})$,

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

so φ is a homomorphism.

④ (Non-example) $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$

$\varphi(x) = x^2$ is not a homomorphism as

$\varphi(x+y) = (x+y)^2 = x^2 + y^2 + 2xy \neq \varphi(x) + \varphi(y)$

Related to any homomorphism, there is a very important subgroup called the Kernel of the homomorphism.

Def^n Let $\varphi : G \longrightarrow \overline{G}$ be a homomorphism. The Kernel of φ, written as $\operatorname{Ker} \varphi$ is

$$\operatorname{Ker} \varphi = \{ x \in G \mid \varphi(x) = \overline{e} \}$$

i.e., $Ker(\varphi)$ is the set of all the elements in G which get map to $\bar{e}$ (identity of $\bar{G}$) by φ.

So, $Ker(\varphi) \subseteq G$. Can it be a subgroup?

Theorem (Kernels are Normal Subgroup)

Let $\varphi: G \to \bar{G}$ be a homomorphism. Then $ker(\varphi)$ is a normal subgroup of G.

Proof:- Since φ is a homomorphism, for $a, a^{-1} \in G$

$\varphi(e) = \varphi(a.a^{-1}) = \varphi(a).\varphi(a^{-1}) = \varphi(a).\varphi(a)^{-1} = \bar{e}$

So $e \in Ker(\varphi) \Rightarrow Ker(\varphi) \neq \phi$.

Check that $Ker(\varphi) \leq G$.

To prove $Ker(\varphi) \trianglelefteq G$, we use the normal subgroup test.

Let $g \in G$, $a \in Ker\,\varphi$. We'd like to show that $gag^{-1} \in Ker(\varphi)$.

i.e., $\varphi(gag^{-1}) = \bar{e}$

But $\varphi(gag^{-1}) = \varphi(g)\varphi(a).\varphi(g)^{-1}$

$= \varphi(g)\,\bar{e}\,\varphi(g)^{-1}$ (as $a \in \ker(\varphi)$)

$= \varphi(g).\varphi(g)^{-1} = \bar{e}$

So, $\ker(\varphi) \trianglelefteq G$.

In the next lecture, we'll see various properties of isomorphism and homomorphisms.