LECTURE 6

02.02.2024

Convention: If the underlying operation is clear from the context, then we will denote a group by its base set, e.g. $GL_n(\mathbb{R})$, SG_n.

A natural subgroup

Let $(G, *)$ be a group. Let $g \in G$. Let us assume $g^0 = e_G$ (the identity element in G). Consider $g^1, g^2, g^3, g^4, \ldots$. We note that all these powers are in G. Let $\langle g \rangle$ denote the set $\{g^n : n \in \mathbb{Z}\}$

H.W.: Show that $(\langle g \rangle, *)$ is a subgroup of $(G, *)$.

We call $\langle g \rangle$ to be a 'cyclic' subgroup of G.

Cyclic group

A group G is said to be a cyclic group if there is some $a \in G$, s.t. for all $g \in G$, $g = a^n$ for some $n \in \mathbb{Z}$.

This 'a' in G will be called a generator of the group G.

Examples:

(1) Consider proper subgroups of SG_3:
$\{e, \tau\}$, $\{e, \tau'\}$, $\{e, \tau''\}$, $\{e, \sigma, \sigma'\}$ are all cyclic subgroups of SG_3.

(2) Consider $(\mathbb{Z}, +)$. It is a cyclic group with generator 1.

Order of an element in a group.

Let $(G, *)$ be a group. and let $g \in G$. with $g \neq e_G$. Order of g is the least positive integer m, s.t. $g^m = e_G$. If no

such n exists then we say that the order of g is infinite. Let $O_G(g)$ denote the order of g in G.

Examples.

(1) SG_3

$O(\tau) = O(\tau') = O(\tau'') = 2$

$O(\sigma) = O(\sigma') = 3$

(2) $\mathbb{Z}$

Take any $z \in \mathbb{Z}$, $z \neq 0$. $O(z)$ is infinite.

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

(a) Consider $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

We have $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

So, order of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is infinite.

(b) Consider $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Now, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

So, order of $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is 2.

Here are some exercises for you:

1. Prove that the identity element of a group is unique.

Proof: Let there be 2 identity elements e_1 and e_2, say. Then we have,

for all $g \in G$, $g * e_1 = e_1 * g = g$ ---- (1)

and, for all $g \in G$, $g * e_2 = e_2 * g = g$ ---- (2)

Now, $e_1 * e_2 = e_1$ from (2)

and $e_1 * e_2 = e_2$ from (1).

Hence, $e_1 = e_2$. □

2. Prove that the inverse of any element of a group is unique.

Proof. Let $g \in G$ has two inverses g_1 and g_2, say. Then we have:

$$g * g_1 = g_1 * g = e \quad \text{—— (1)}$$

and $$g * g_2 = g_2 * g = e \quad \text{—— (2)}$$

Then, $g * g_1 = g * g_2$ from (1) and (2)

So, $g_1 * (g * g_1) = g_1 * (g * g_2)$

or, $(g_1 * g) * g_1 = (g_1 * g) * g_2$

or, $e * g_1 = e * g_2$, by (1)

or, $g_1 = g_2$. □

Identifying certain groups.

$G_1 = (\{1, -1, i, -i\}, \cdot)$

$G_2 = (\{e, \tau, \tau', \tau''\}, \circ)$

For G_1, we are basically talking about

a set of complex numbers.

For G_2, we are basically talking about bijections on $\{1, 2, 3, 4\}$.

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\tau' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \tau'' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Now, let us consider the composition tables:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$\circ$	e	τ	τ'	τ''
e	e	τ	τ'	τ''
τ	τ	τ'	τ''	e
τ'	τ'	τ''	e	τ
τ''	τ''	e	τ	τ'

$i^1 = i$
$i^2 = -1$
$i^3 = -1$
$i^4 = 1$

$f : \{1, -1, i, -i\} \to \{e, \tau, \tau', \tau''\}$
$i^k \mapsto \tau^k$

$f(g \circ g') = f(i^m \cdot i^n)$
$= f(i^{m+n})$
$= \tau^{m+n} = \tau^m \circ \tau^n$
$= f(g) \circ f(g')$

$\tau^1 = \tau$
$\tau^2 = \tau'$
$\tau^3 = \tau''$
$\tau^4 = e$

We say that G_1 and G_2 are isomorphic. Let us define formally.

Isomorphism

Let $(G, *)$ and $(G', *')$ be two groups. We say that G and G' are isomorphic as groups if there is $f: G \to G'$ s.t.

(i) f is a bijection

(ii) f is structure-preserving:

$f(a * b) = f(a) *' f(b)$ for all $a, b \in G$.

H.W. Consider $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$. Are they isomorphic? Justify your answer.

Q. Can there be functions from one group to another which is not a bijection but only structure-preserving?

Consider $f: \mathbb{Z} \to S_{G_2}$

$f(n) = e$ if n is even

τ if n is odd.

We have: $f(m+n) = f(m) \circ f(n)$ Check!

Let us now note what kind of properties should two isomorphic groups G and G' preserve:

1. Orders of G and G' should be the same, where order of a group is the number of elements present in the group.
2. If G is commutative then G' should also be commutative and vice versa.
3. If G is cyclic then G' should also be cyclic and vice versa.

(4) $O_G(g)$ and $O_{G'}(f(g))$ should be the same for all $g \in G$, where $f: G \to G'$ is an isomorphism.

H.W. Prove the properties above.

Now, let us get back to our structure-preserving maps which may or may not be bijections. Such maps are called group homomorphisms.

Homomorphism

Let $(G, *)$ and $(G', *')$ be two groups. A map $f: G \to G'$ is said to be a homomorphism if for all $a, b \in G$,

$$f(a * b) = f(a) *' f(b)$$

Examples:

(1) $f: \mathbb{Z} \to SG_2 : n \mapsto \begin{cases} e & \text{if } n \text{ is even} \\ \tau & \text{if } n \text{ is odd} \end{cases}$

is a homomorphism from $(\mathbb{Z}, +)$ to $(SG_2, \circ)$.

② $f : GL_n(\mathbb{R}) \to GL_1(\mathbb{R})$

$A \mapsto \det A$

Now, $f(A \cdot B) = \det(A \cdot B)$

$= \det A \cdot \det B$

$= f(A) \cdot f(B)$.

So, f is a homomorphism.

Is f injective ? NO (Check !)

Is f surjective ? YES (Check !).

Monomorphism : Homomorphism + injective

Epimorphism : Homomorphism + surjective.

Isomorphism : Homomorphism + bijective

Proposition : ① $f(e_G) = e_{G'}$

② $f(g^{-1}) = [f(g)]^{-1}$ for any $g \in G$.

Proof : ① $f(e_G) = f(e_G * e_G) = f(e_G) *' f(e_G)$

So, $f(e_G) *' e_{G'} = f(e_G) = f(e_G) *' f(e_G)$.

Hence, $e_{G'} = f(e_G)$.

(2) $f(e_G) = f(g * g^{-1})$

$= f(g) *' f(g^{-1})$.

So, $f(g) *' f(g^{-1}) = f(e_G) = e_{G'}$

Hence, $f(g^{-1}) = [f(g)]^{-1}$.

Image and Kernel of a homomorphism

Let $(G, *)$ and $(G', *')$ be two groups. Let $f: G \to G'$ be a homomorphism. Then, we define:

$\text{Im } f = \text{Image } f = \{g' \in G' :$ there is $g \in G$ with $f(g) = g'\}$.

$\text{Ker } f = \text{Kernel } f = \{g \in G : f(g) = e_{G'}\}$.

H.W. (1) $\text{Im } f$ is a subgroup of G' } Prove or
$\text{Ker } f$ is a subgroup of G } disprove.