Group Theory

Lecture 6

19/01/2022

<u>Recall</u>: $f : G_1 \longrightarrow G_2$ is a gp homo if $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$ $\forall\, g_1, g_2 \in G_1$

$\ker f \leq G_1$ and $\operatorname{Im} f \leq G_2$.

$\ker f$ has a special property

let $g \in \ker f$ then $h g h^{-1} \in \ker f$ $\forall\, h \in G_1$ and for all $g \in \ker f$.

<u>Defn</u>. A subgp N of G is called a normal subgp of G $(N \trianglelefteq G)$ if $g h g^{-1} \in N$ $\forall\, g \in G$, $h \in N$.

<u>Examples</u>

(1) If G is an abelian gp then any subgp H of G is a normal subgp.

(2) If $f: G_1 \longrightarrow G_2$ is a gp homo then $\ker f$ is a normal subgp of G_1

(3) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$

$$\ker(\det) = SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R}).$$

(4) $\mathrm{sign} : S_n \longrightarrow \{1, -1\}$.

$$\ker(\mathrm{sign}) = A_n \triangleleft S_n.$$

(5) U be the set of upper triangular invertible matrices in $GL_2(\mathbb{R})$.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin U.$$

U is not a normal subgp of $GL_2(\mathbb{R})$

Centre of a gp:

Defn Let G be a gp. Then its centre is defined as

$$Z(G) := \{ g \in G \mid gh = hg \ \forall h \in G \},$$

Note $Z(G)$ is a subgp of G.
In fact $Z(G)$ is a normal subgp of G.

If G an abelian gp then $Z(G) = G$.

Ex (1) Show that $Z(GL_n(\mathbb{R})) = \{ cI_n \mid c \in \mathbb{R}^{\times} \}$

(2) $$Z(S_n) = \begin{cases} \{(1)\} & \text{if } n \geq 3. \\ S_n & \text{if } n = 1, 2. \end{cases}$$

Let $\phi : S \longrightarrow T$ be a map of sets.
This map defines an equivalance relation on the domain S by the rule $a \sim b$ if $\varphi(a) = \varphi(b)$

For an elt $t \in T$ the inverse image of t is defined as

$$\varphi^{-1}(t) = \{ s \in S \mid \varphi(s) = t \}$$

The inverse images are called the fibers of φ.

Thus $S = \bigsqcup \varphi^{-1}(t)$. where $t \in \operatorname{Im} \varphi$.

For example consider the gp homo $\varphi : \mathbb{C}^{\times} \longrightarrow \mathbb{R}^{\times}_{>0}$ {non-zero real number wrt $\cdot$ }

$$\varphi(z) = |z|$$

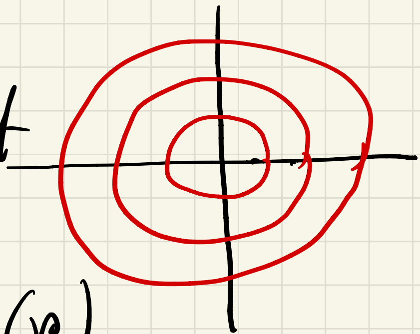
$$\mathbb{C}^\times \longrightarrow \mathbb{R}^\times_{>0}.$$

$$\varphi(z) = |z|.$$

$$\varphi^{-1}(2) = \{ z \in \mathbb{C}^\times \mid |z| = 2 \}.$$

$$\varphi^{-1}(r) = \{ z \in \mathbb{C}^\times \mid |z| = r \}.$$

The fibers of φ are concentric circles about the origin.



and $$\mathbb{C}^\times = \bigsqcup_{r \in \mathbb{R}^\times_{>0}} \varphi^{-1}(r),$$

<u>Propn.</u> Let $\varphi : G \to G'$ be a gp homo with ker N and let $a, b \in G$. Then $\varphi(a) = \varphi(b)$ iff $b = an$ for some $n \in N$ or equivalently if $a^{-1}b \in N$.

Pf: ($\Rightarrow$) Let $\varphi(a) = \varphi(b)$

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

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

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

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

$\Rightarrow a^{-1}b \in N.$

$\Rightarrow a^{-1}b = n$ for some $n \in N.$

$\Rightarrow b = an.$

Conversely if $b = an$ then

$\varphi(b) = \varphi(an) = \varphi(a)\varphi(n) = \varphi(a)$

Cor. A gp homo $\varphi : G \longrightarrow G'$ is inj iff $\ker \varphi = \{1\}.$

Defn. A gp homo $\varphi : G \to G'$ is called an isomorphism if φ is 1-1 and onto.

Moreover $G' = G$ then an isomorphism is called an automorphism.

Example (1) Let $G = \langle x \rangle$ be an infinite cyclic gp. Then $\varphi : \mathbb{Z} \to G$ defined by

$$\varphi(1) = x.$$

$$\varphi(n) = \varphi(\underbrace{1+1\cdots+1}_{n\text{-time}})$$

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

$$= x^n.$$

Then φ is an isomorphism.

(2) Let $G = \langle x \rangle$ be a finite cyclic gp of order n. Then $\varphi : \mathbb{Z}_n \to G$.

defined by $\varphi(T) = x$ is an isomorphism.

(3) Consider the set

$$W = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

Define $\varphi : W \longrightarrow \mathbb{R}$.

$$\varphi\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = x$$

$$\varphi(AB) = \varphi(A) + \varphi(B).$$

$$\underbrace{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}}_{B} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

$$\varphi(AB) = \varphi(A) + \varphi(B).$$

Note that φ is an isomorphism.

I

Ex Is W a normal subgp of $SL_2(\mathbb{R})$?

$W \lhd SL_2(\mathbb{R}) \lhd GL_2(\mathbb{R})$.

Is W a normal subgp of $GL_2(\mathbb{R})$?

(4). Let G be any gp.

Define $Aut(G) := \{ \phi : G \to G \mid \phi$ is an automorphism $\}$.

Check: $Aut(G)$ forms a gp with respect to composition operation.

Inner automorphism :

Let G be a gp and $g \in G$ be a fixed elt. $i_g : G \to G$ by

$$i_g(x) = gxg^{-1}$$

$$i_g(xy) = gxy\,g^{-1}$$
$$= (gxg^{-1})(gyg^{-1})$$
$$= i_g(x) \cdot i_g(y).$$

i_g is injective gp homo.

$$i_g(g^{-1}xg) = g\,g^{-1}xg\,g^{-1}$$
$$= x.$$

Thus i_g is surjective.

Hence i_g is an automorphism.

The elts gxg^{-1} are called conjugates of x for all $g \in G$.

Let G be a gp and H is a subgp of G. We define for $g \in G$ a left coset of H as

$$gH = \{gh \mid h \in H\}.$$

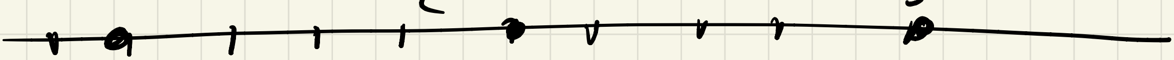
$$\left(g+H = \{g+h \mid h \in H\}\right).$$

Example. $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$.

$g = 1$.

$$1 + 5\mathbb{Z} = \{1 + 5n \mid n \in \mathbb{Z}\}$$

$$2 + 5\mathbb{Z} = \{2 + 5n \mid n \in \mathbb{Z}\}.$$



$$3 + 5\mathbb{Z} = \{3 + 5n \mid n \in \mathbb{Z}\}.$$

$$4 + 5\mathbb{Z} = \{4 + 5n \mid n \in \mathbb{Z}\}.$$

$$5 + 5\mathbb{Z} = 5\mathbb{Z} = H.$$

$$6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$$

(2) S_3, $\quad H = \{(1), (12)\}$.

$(23)(12)$

$$\begin{cases} (23)H = \{(23), (132)\}. \\ (12)H = H \\ (13)H = \{(13), (123)\} \end{cases}$$

$$(123)H = \{(123), (13)\}.$$

Let us define an equivalence relation on G as $a, b \in G$ (H is a subgp of G.)

$a \sim b$ if $a = bh$ for some $h \in H$. i.e $a^{-1}b \in H$.

check that $\sim$ is an equivalence relation and the equivalence class of any $g \in G$ is gH.

Therefore any two left cosets are either equal or they are disjoint as left cosets are equivalance classes.

$$G = \bigsqcup_{g \in G} gH$$

i.e G can be written as disjoint union of left cosets of H.

<u>Remark</u>. Let H be a subgp of G and aH be a left coset of H. Then $|H| = |aH|$.

$$f : H \longrightarrow aH$$

$$f(h) = ah.$$

$f(h_1) = f(h_2)$ WTS $h_1 = h_2$.

$\Rightarrow \quad a h_1 = a h_2$

$\Rightarrow \quad h_1 = h_2.$

$\Rightarrow \quad f$ is injective.

$$f(h) = ah \in aH.$$

f is surjective.

Here f is a bijection.

$$|H| = |aH|.$$

Thus all left cosets have same cardinality.

Q. What is the relation between $|G|$ and $|H|$ where H is a subgp of G?

Ans. $\quad |H| \,\big|\, |G|. \quad$ [Lagrange's Thm].

we know that G can be written as disjoint union of left cosets of H. i.e $G = \bigsqcup_{g \in G} gH$.

Say $G = g_1 H \cup g_2 H \cup \cdots \cup g_r H$.

and also we have

$$|g_1 H| = |g_2 H| \cdots = |g_r H| = |H|$$

$\therefore$ $|G| = r \cdot |H|$.

$\Rightarrow$ $|H| \,\big|\, |G|$.

Lagrange's Thm: Let G be a finite gp & H is a subgp of G. Then $|H|$ divides $|G|$ and $|G|/|H|$ = no. of distinct left cosets.

Defn. The number of left cosets of a subgp H of a gp G is called the index of H in G $= [G : H]$.

Remark (1) If G is a finite gp. then the no. of left cosets are finite.

(2) Even if G is infinite but $[G:H]$ can be finite. Consider $G = \mathbb{Z}$, $H = n\mathbb{Z}$. Then the left cosets of H are

$$n\mathbb{Z},\ 1+n\mathbb{Z},\ 2+n\mathbb{Z},\ \ldots,\ n-1+n\mathbb{Z}$$

$$\therefore\ [\mathbb{Z} : n\mathbb{Z}] = n.$$

Cor. Let G be a finite gp and $a \in G$. Then $|a| \mid |G|$ and $a^{|G|} = 1$.

Pf: Let $H = \langle a \rangle$ be the cyclic subgp of G gen by a.

Then $|H| = |a|$.

By Lagrange's Thm $(|H| =) |a| \mid |G|$.

Let $|G| = |a| \cdot r$.

Then $a^{|G|} = a^{|a| \cdot r} = (a^{|a|})^r = 1$.

Cor. Let G be a gp of prime order then G is a cyclic gp.

Pf: Let $1 \neq a \in G$. Consider the cyclic subgp $H = \langle a \rangle$.

Then by Lagenges Thm

$|a| \mid |G|$, but $|G|$ is a prime no say p.

Then $|a| = 1$ or p but $a \neq 1$.

Hence $|a| = p$. Thus $G = \langle a \rangle$

Hence G is a cyclic gp.

Q. If $n \mid |G|$ for a gp G then G need not have a subgp of order n. i.e Converse of Lagrange's Thm is not true.