Group Theory

Week #3, Lecture #12

I Normal subgroups

Recall that a subgroup $H < G$ is called normal if

$$\boxed{ghg^{-1} \in H \quad , \forall h \in H, \forall g \in G}$$

Prop The following conditions are equivalent:

(1) $H < G$ is normal

(2) $gHg^{-1} = H \qquad , \forall g \in G$

(3) $gH = Hg \qquad \forall g \in G$

(4) Every left coset of H in G is also a right coset.

Proof $(1) \Longleftrightarrow (2)$: done last time

$(2) \Longleftrightarrow (3)$: clear (multiply both sides on the right by either g or g^{-1})

$(3) \Longrightarrow (4)$: obvious

$(4) \Longrightarrow (3)$ Let gH be a left coset of H in G. By assumption, $gH = Hk$, for some $k \in G$.

Note : • $g = g \cdot e \in gH = Hk$

• $g = e \cdot g \in Hg$

$\Rightarrow g \in Hk \cap Hg$

$\Longrightarrow k = g$ (since cosets either coincide or are disjoint)

$\therefore gH = Hg$

∎

Corollary Every index 2 subgroup is normal.

Proof Let $H < G$ be a subgroup of G, with index $[G : H] = 2$.

Recall $[G:H] = \#\{\text{left cosets of } H \text{ in } G\}$
$\#\{\text{right cosets of } H \text{ in } G\}$

(this came out of the proof of Lagrange's Theorem, where we showed that all cosets of H are in bijection)

- In our situation, there are only 2 cosets:

$$G = H \amalg gH \quad \leftarrow \text{left cosets}$$
$$= H \amalg Hk \quad \leftarrow \text{right cosets}$$

$\therefore \quad gH = Hk$

By the prop $((4) \Rightarrow (1))$, H is normal subgroup of G ▨

Remark. All subgroups of an abelian group G are normal subgroups. $\left(\text{Since } ghg^{-1} = h, \forall h, g \in G \Downarrow ghg^{-1} \in H, \forall h \in H, g \in G\right)$

In particular, left/right cosets coincide in this setting.

Let's illustrate the difference between left/right cosets and normal/non-normal subgroups with an example from linear algebra over finite fields.

Def A field is a commutative ring where every non-zero element is invertible:

$(F, +, \cdot)$
- $(F, +, 0)$ abelian gp
- $(F^\times, \cdot, 1)$ abelian gp
- $a(b+c) = ab + ac$

Eg:
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{Z}_p$, p prime

Let: $GL_n(F) = \{ A \in \underset{\substack{\uparrow \\ n\times n \text{ matrices w/ entries in } F}}{Mat_{n\times n}}(F) : \underset{\substack{\Updownarrow \\ \det A \neq 0}}{A \text{ invertible}} \}$

This is called the General Linear group over F, i.e., the group of invertible linear transformations of the F-vector space $V = F^n$.

This group contains many interesting subgroups such as

$$SL_n(F) = \{ A \in GL_n(F) : \det(A) = 1 \}$$
$$= \ker(\det : GL_n(F) \longrightarrow \{\pm 1\})$$

Simplest nontrivial example: $\qquad \mathbb{Z}_2 = \{0,1\}$

$$GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{matrix} a,b,c,d \in \mathbb{Z}_2 \\ ad+bc=1 \end{matrix} \right\}$$
$$\|$$
$$SL_2(\mathbb{Z}_2)$$
$$= \left\{ \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{H}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} H$$

This group has size 6, and is not abelian, since, eg

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \not\ni$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

In fact: (1) $GL_2(\mathbb{Z}_2) \cong S_3 \cong D_3$ $\qquad$ (exercise!)

(2) This is the only non-abelian group of order 6 (The smallest non-abelian group.)

<u>Exercise</u>: What is the size of $GL_n(\mathbb{Z}_p)$?

<u>Example</u> Let $G = GL_2(\mathbb{Z}_2)$ and $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

Questions: (1) Show that H is a subgroup of G.
(2) Compute all its left and right cosets
(3) What is $[G:H]$?
(4) Is H a normal subgroup?

Answers

(1) $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ the identity matrix

$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad A \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

note $\begin{pmatrix} I & A \\ A & I \end{pmatrix}$ mult. table $\qquad$ In fact, $H \cong \mathbb{Z}_2$

$I \leftrightarrow [0]_2$

$A \leftrightarrow [1]_2$

(3) By Lagrange: $[G:H] = \dfrac{|G|}{|H|} = \dfrac{6}{2} = 3$

(2) Left cosets of H:

- $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$
- $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

Right cosets of H

- H
- $H \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$
- $H \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

(4) Left cosets are not right cosets (except for H), so H is not a normal subgroup, by ((4)$\Rightarrow$(1)) in Prop above.

On the other hand, if we take

$K = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \cong \mathbb{Z}_3$

then $[G:K] = 2$, so $K \trianglelefteq G$. (Verify $Kg = gK$, $\forall g \in G$)

II Images & preimages

Let $\varphi : G \to G'$ be a homomorphism

- image of a subset $H \subseteq G$: $\varphi(H) = \{ y \in G' : y = \varphi(x) \text{ for } x \in G \}$
- preimage of a subset $H' \subseteq G'$: $\varphi^{-1}(H') = \{ x \in G : \varphi(x) \in H' \}$

Prop (a) If $H < G$, then $\varphi(H) < G'$.

(b) If $H \trianglelefteq G$, then $\varphi(H) \trianglelefteq \varphi(G)$.

(so, if φ surjective, then $\varphi(H) \trianglelefteq G'$)

(c) If $H' < G'$, then $\varphi^{-1}(H') < G$.

(d) If $H' \trianglelefteq G'$, then $\varphi^{-1}(H') \trianglelefteq G$.

Proof (a) — done in a previous class

(b) let $y \in \varphi(G)$, $x \in \varphi(H)$. Then

$y = \varphi(a)$, $x = \varphi(b)$, for some $a \in G$, $b \in H$.

$$\therefore \quad yxy^{-1} = \varphi(a) \cdot \varphi(b) \cdot (\varphi(a))^{-1}$$
$$= \varphi(a)\,\varphi(b)\,\varphi(a^{-1})$$
$$= \varphi(\underbrace{aba^{-1}}_{\in H \text{ since } H \trianglelefteq G}) \in \varphi(H)$$

$\therefore \varphi(H) \trianglelefteq \varphi(G)$.

(c), (d): exercize

Question Find $\varphi : G \to G'$, $H \trianglelefteq G$ s.t. $\varphi(H) \ntrianglelefteq G'$.

III Cosets of the kernel of a homomorphism

Let $\varphi : G \to G'$ be a homomorphism. Define an equiv. rel. on G by

$$
\begin{aligned}
a \sim_\varphi b &\overset{\text{def}}{\iff} \varphi(a) = \varphi(b) \\
&\iff \varphi(a)\cdot\varphi(b)^{-1} = e' \\
&\iff \varphi(ab^{-1}) = e' \\
&\underset{\substack{\text{def}\\ \text{of ker}}}{\iff} ab^{-1} \in \ker(\varphi)
\end{aligned}
$$

where $K := \ker(\varphi) = \varphi^{-1}(\{e'\}) = \{x \in G : \varphi(x) = e'\}$ is the kernel of φ.

Prop (1) $K = \ker(\varphi)$ is a normal subgroup of G

(2) φ is injective $\iff$ $\ker(\varphi) = \{e\}$.

Proof (1) $x, y \in K \Rightarrow \varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = e' \cdot e' = e'$

$\therefore xy^{-1} \in K$ (so $K < G$)

$x \in K, y \in G \Rightarrow \varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y)^{-1}$

$= \varphi(y)\cdot e' \cdot \varphi(y)^{-1} = e'$

$\therefore yxy^{-1} \in K$ (so $K \trianglelefteq G$)

(2) ($\Rightarrow$) obvious

($\Leftarrow$) Suppose $x, y \in G$ and $\varphi(x) = \varphi(y)$

Then $\varphi(xy^{-1}) = \varphi(x)\cdot\varphi(y^{-1})$

$= \varphi(x)\cdot\varphi(y)^{-1}$

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

$= e'$

$\therefore xy^{-1} \in \ker(\varphi) = \{e\}$

$\therefore x = y$ $\square$

Remark The kernel of a group homomorphism is the analogue of the nullspace of a linear transformation (or of a matrix) in linear algebra.