Group Theory

Week #4, Lecture 14

Basic tool we discussed last time was the Fundamental Theorem of Homomorphisms:

short version: $\varphi: G \longrightarrow G'$ hom. $\Rightarrow$ $\boxed{G/\ker(\varphi) \cong \mathrm{im}(\varphi)}$

more precise version: Every hom. $\varphi: G \to G'$ factors through an iso $\boxed{\bar{\varphi}: G/\ker(\varphi) \longrightarrow \mathrm{im}(\varphi)}$, where $\boxed{\bar{\varphi}(x \cdot \ker(\varphi)) = \varphi(x)}$

Further remarks:

(1) Every normal subgroup $N \trianglelefteq G$ occurs as the kernel of a homomorphism from G to another group.

Indeed, let $\pi: G \twoheadrightarrow G/N$, $\pi(x) = xN$ be the canonical projection of G onto the factor group. Then $\ker(\pi) = N$ (as we saw last time).
Hence:

$$\boxed{N = \ker(\pi: G \longrightarrow G/N)}$$

(2) Recall that the index of a subgroup $H < G$ is defined as

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

Furthermore, if G is finite, then, by Lagrange's Theorem:

$$\boxed{[G:H] = \frac{|G|}{|H|}}$$

Now suppose $N \trianglelefteq G$ is a normal subgroup, i.e., left & right cosets of N coincide.

Then $\boxed{[G:N] = |G/N|}$ ← the left cosets of N in G

in words: ‖ The index of N in G is the order of the factor group G/N.

For finite groups (and their normal subgroups), Lagrange's theorem can also be written as

$$\boxed{\left|G/N\right| = \frac{|G|}{|N|}}$$

or $$|G| = |N| \cdot |G/N|$$

<u>Example</u> (Problem #24, § 3.8)

Let $G = \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} : \begin{matrix} c, d \in \mathbb{Z}_5 \\ d \neq 0 \end{matrix} \right\} < GL_2(\mathbb{Z}_5)$

and $N = \{ A \in G \mid \det A = 1 \} = \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : c \in \mathbb{Z}_5 \right\}$

(1) Show that $N \trianglelefteq G$.

(2) Identify G/N.

---

note: $|GL_2(\mathbb{Z}_5)| = (5^2-1)\cdot(5^2-5) = 24 \cdot 20 = 480$

observations:

- $|G| = \underset{\substack{\uparrow \\ c}}{5} \cdot \underset{\substack{\uparrow \\ d}}{4} = 20$
- $|N| = 5$
- So, once we show that $N \trianglelefteq G$, we know that

$$|G/N| = \frac{|G|}{|N|} = \frac{20}{5} = 4$$

$\therefore$ $G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$

(1) "Brute force" computation:

$$\underset{\substack{\uparrow \\ B \text{ in } G}}{\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}} \underset{\substack{\uparrow \\ A \text{ in } N}}{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}} \underbrace{\begin{pmatrix} d & 0 \\ -c & 1 \end{pmatrix} \cdot d^{-1}}_{\substack{\uparrow \\ B^{-1}}} = \begin{pmatrix} 1 & 0 \\ c+d & d \end{pmatrix} \begin{pmatrix} d & 0 \\ -c & 1 \end{pmatrix} \cdot d^{-1} = \begin{pmatrix} d & 0 \\ \cancel{cd}+d^2-\cancel{cd} & d \end{pmatrix} \cdot d^{-1}$$

$$= \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \in N \quad \checkmark$$

Shorter proof: $N = \ker(\det : G \twoheadrightarrow \mathbb{Z}_5^\times)$

$\det \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} = d$

so $N \trianglelefteq G$

(2) By shorter proof of (1) and FTH:

$$G/N \cong \operatorname{im}(\det : G \to \mathbb{Z}_5^\times) = \mathbb{Z}_5^\times \cong \mathbb{Z}_4$$

QED

Example (Problem #10, § 3.8)

Let $N \trianglelefteq G$ and suppose $[G:N] = m$. Show that

$$a^m \in N, \quad \text{for all } a \in G$$

Solution: Note that $|G/N| = [G:N] = m$

Now consider the (left) coset aN in G/N. Then, by a corollary to Lagrange's theorem:

$$(aN)^m = N$$

(in general, if $|G|$ is finite and $x \in G$, then $o(x) \mid |G|$, so $x^{|G|} = e$)

$$\underset{a^m N}{\|}$$

(Since $xN \cdot yN = xyN$)

$$\therefore \; a^m \in N$$

$\square$

Question What happens if we drop the assumption that N is normal in G? i.e.,

$$H < G \; \& \; [G:H] = m \overset{?}{\Longrightarrow} a^m \in H, \; \forall a \in G$$

The Center of a group

Def The center of a group G is

(Zentrum) $\to$ $\boxed{Z(G) := \{x \in G : gx = xg, \; \forall g \in G\}}$

Lemma $Z(G)$ is a normal subgroup of G.

Proof ~~Z~~ $Z(G)$ is a subgroup:

(a) $\begin{array}{l} x, y \in Z(G) \\ g \in G \end{array} \Rightarrow (xy)\cdot g \underset{\text{assoc}}{=} x(yg) = x(gy) \underset{y \in Z}{}$

$\underset{\text{assoc}}{=} (xg)y \underset{x \in Z}{=} (gx)y = g(xy)$

$\therefore \quad xy \in Z(G)$

$\begin{array}{l} x \in Z \\ g \in G \end{array} \rightarrow g x g^{-1} \underset{\text{since } gx = xg}{=} x \underset{\text{take inverses on both sides}}{\Longrightarrow} g x^{-1} g^{-1} = x^{-1}$

$\therefore \quad g x^{-1} = x^{-1} g$

$\therefore \quad x^{-1} \in Z(G)$

Z is normal:

$\begin{array}{l} x \in Z \\ g \in G \end{array} \Longrightarrow g x = x g \Longrightarrow g x g^{-1} = x \in Z$ ✓

$\boxed{\text{QED}}$

Examples (1) G abelian $\Rightarrow Z(G) = G$

(2) $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ $\quad \left(\begin{array}{l} i^2 = j^2 = k^2 = -1 \\ ij = jk = ki \\ ji = -ij, \text{ etc} \end{array} \right)$

$= \{1, -1\}$

$\cong \mathbb{Z}_2$

$\boxed{\text{Matrix groups}}$

$G = GL_2(F)$, F a field

$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in F, \ ad - bc \neq 0 \right\}$

Lemma $\boxed{Z(G) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in F^{\times} \right\}}$

check: ($\supseteq$) $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x^{-1} \end{pmatrix} = x \cdot x^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

($\subseteq$) Suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(G)$. Then:

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \Rightarrow \begin{cases} a = a+c \\ a+b = b+d \\ c+d = d \end{cases} \Rightarrow \begin{cases} c = 0 \\ a = d \end{cases}$

So A must be of the form $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$

But A must also commute with $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$:

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

$$\begin{pmatrix} a+b & b \\ a & a \end{pmatrix} = \begin{pmatrix} a & b \\ a & b+a \end{pmatrix} \Rightarrow \begin{cases} a+b = a \\ a = b+a \end{cases} \Rightarrow b=0$$

$$\therefore \quad A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

QED

Define $\boxed{PGL_2(F) := GL_2(F) / Z(GL_2(F))}$

projective general linear group of 2×2 matrices w/ entries in F

In particular: $PGL_2(\mathbb{Z}_p) = GL_2(\mathbb{Z}_p)/\text{center}$ (p prime)

$p=2$ $\quad G = GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}_2,\ ad+bc=1 \right\}$

has order $(2^2-1)(2^2-2) = 3\cdot 2 = 6$

$$Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_2^\times \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$\therefore \quad PGL_2(\mathbb{Z}_2) = GL_2(\mathbb{Z}_2)$$

$p=3$ $\quad G = GL_2(\mathbb{Z}_3)$ has order $(3^2-1)(3^2-3) = 8\cdot 6 = 48$

$$Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_3^\times \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\} \cong \mathbb{Z}_2$$

$\therefore$ $PGL_2(\mathbb{Z}_3)$ has order 24

Exercise (Hard!) $\quad PGL_2(\mathbb{Z}_3) \cong S_4$.

$PSL_2(\mathbb{Z}_3) \cong A_4 \cong$ rotations of the tetrahedron

---

Exercise (Problem # 14, § 3.8)

Let N be a subgroup of $Z(G)$.

(a) Show that is a normal subgroup of G

(b) If G/N is cyclic, then G is abelian

Solution (a) Let $x \in N$ and $g \in G$. Then

$$gxg^{-1} \underset{\substack{\uparrow \\ x \in N \subseteq Z(G)}}{=} gg^{-1}x = e \cdot x = x \in N$$

(b) Suppose G/N is cyclic, that is:

$$\boxed{G/N = \langle aN \rangle} \quad \text{, for some } a \in G$$

Let $x, y \in G$. Then

$$\begin{cases} xN = (aN)^k = a^k N \\ yN = (aN)^\ell = a^\ell N \end{cases} \quad \text{, for some } a \in G$$

$$\Rightarrow \begin{cases} x = a^k \cdot u \\ y = a^\ell \cdot v \end{cases} \quad \text{, for some } u, v \in N$$

Hence:

$$\begin{aligned} xy &= (a^k u)(a^\ell v) \\ &= a^k (u a^\ell) v \\ &= a^k (a^\ell u) v \quad \leftarrow \text{since } u \in N \subseteq Z(G) \\ &= a^{k+\ell} u v = yx \end{aligned}$$

QED