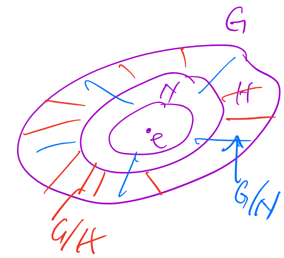
Group Theory
Week #6, Lecture #23

Theorem (2nd Iso Thm) Let H and N be two normal subgroups of G, with $\boxed{N \subseteq H}$. Then

(i) $H/N \triangleleft G/N$

(ii) $\boxed{\dfrac{G/N}{H/N} \cong G/H}$



Proof The canonical projection

$$G \xrightarrow{\pi_H} G/H, \quad g \longmapsto gH \quad \text{(a surj hom)}$$

[makes sense since $H \trianglelefteq G$]

factors through a homomorphism,

$$\boxed{G/N \xrightarrow{\varphi} G/H, \quad gN \longmapsto gH}$$

These maps fit into the diagram

$$\begin{tikzcd} G \arrow[r, two heads, "\pi_H"] \arrow[d, "\pi_N"] & G/H \\ G/N \arrow[ur, dashed, "\varphi"'] & \end{tikzcd} \qquad \begin{tikzcd} g \arrow[r, mapsto, "\pi_H"] \arrow[d, "\pi_N"] & gH \\ gN \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

We claim that φ is a well-defined, surjective homomorphism

- well-defined: Suppose $g_1N = g_2N$. Then:

$$g_2^{-1}g_1 \in N \Longrightarrow g_2^{-1}g_1 \in H \Longrightarrow g_2H = g_1H$$

since $N \subseteq H$

$$\therefore \varphi(g_1N) = \varphi(g_2N) \quad \checkmark$$

- Surj: clear $(\forall gH \in G/H, \ \varphi(gN) = gH)$

- hom

$$\varphi(g_1N \cdot g_2N) = \varphi(g_1g_2N) \quad \text{[by def of * in } G/N]$$

in G/N

$$= g_1g_2H \quad \text{[by def of } \varphi]$$

$\shortparallel$

$$\underset{\uparrow \text{ in } G/H}{\varphi(g_1N)\cdot\varphi(g_2N)} \underset{\uparrow \text{ def of } * \text{ on } G/H}{=} g_1H\cdot g_2H$$

The kernel of φ is:

$$\begin{aligned}\ker(\varphi) &= \{gN : \varphi(gN) = H\} \quad \subseteq G/N \\ &= \{gN : gH = H\} \\ &= \{gN : g\in H\} \\ &= H/N \quad \longrightarrow H/N \trianglelefteq G/N \quad \to \text{proves (i)}\end{aligned}$$

$\leftarrow$ since $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$

By the FTH:, the hom $\varphi: G/N \twoheadrightarrow G/H$ factors through an isomorphism

$$\left. G/N \middle/ H/N \right. \xrightarrow[\varphi]{\cong} G/H \quad \longrightarrow \text{proves (ii)}$$

$\boxed{//}$

Theorem (Decomposition into direct products)

Let G be a group, and let H, K be two subgroups.

Suppose:

(1) $hk = kh$, $\forall h\in H, \forall k\in K$

(2) $G = HK$ $\leftarrow$ product

(3) $H\cap K = \{e\}$

Then:

$$\boxed{G \cong H\times K}$$

$\leftarrow$ direct product

Proof Define a map

$$\begin{aligned}\varphi: H\times K &\longrightarrow G \\ (h,k) &\longmapsto \underset{\text{in } G}{h\cdot k}\end{aligned}$$

Claim This map is an isomorphism.

- hom $\varphi((h_1,k_1)\cdot(h_2,k_2)) = \varphi((h_1\cdot h_2, k_1\cdot k_2))$

$$
\underset{\text{in } G}{\varphi((h_1,k_1)\underset{\text{in } H\times K}{\cdot}(h_2,k_2))} = \underset{\text{def of } * \text{ in } H\times K}{(\underset{\text{in } H}{h_1h_2})(\underset{\text{in } K}{k_1k_2})} \quad [\text{in } G]
$$

$$
\varphi((h_1,k_1))\cdot\varphi((h_2,k_2)) = (h_1k_1)\cdot(h_2k_2) = h_1\cdot(k_1h_2)\cdot k_2 \underset{\text{by (1)}}{=} h_1\cdot(h_2k_1)k_2 \quad \checkmark
$$

[Warning: If we only knew $HK=KH$ that would give us:

$$k_1h_2 = h_3k_3 \quad \text{for some } h_3\in H,\ k_3\in K$$

not good enough!]

- surj: by (2), $\forall g$, $\exists h\in H, k\in H$ st. $g=hk$.
  i.e. $g=\varphi((h,k))$

- inj

$$
\begin{aligned}
(h,k)\in\ker(\varphi) &\iff \varphi((h,k))=e && (\text{def of ker})\\
&\iff h\cdot k=e && (\text{def of } \varphi)\\
&\iff k=h^{-1} && (\text{def of inverse})\\
&\implies k\in K\cap H && (\text{since } k\in K,\ h\in H\Rightarrow h^{-1}\in H)\\
&\implies k=e && (\text{by assumption (3)})\\
&\implies \text{and so } h=e, \text{ also}\\
&\implies (h,k)=(e,e)
\end{aligned}
$$

This shows φ in injective.

$\boxed{\text{QED}}$

Generalization to arbitrarily many subgroups $H_1,\dots,H_n$ of G:

Theorem If

(1) $h_i h_j = h_j h_i$, $\forall h_i\in H_i,\ h_j\in H_j$

(2) $G=H_1\cdots H_n$

(3) $H_i\cap(H_1\cdots H_{i-1}\cdot H_{i+1}\cdots H_n)=\{e\}$ $\forall i\in\{1,\dots,n\}$

Then $G\cong H_1\times\cdots\times H_n$

[Similar proof]
[or, use above thm + induction]

Corollary If N_1 and N_2 are normal subgroups of G such that $N_1 \cap N_2 = \{e\}$, then $N_1 \cdot N_2 \cong N_1 \times N_2$. [Karthik will provide a proof!]

Back to group actions on sets and the Class Equation

Recall: Let G be a finite group acting on a set S

Then: $\boxed{|S| = |S^G| + \sum_{|Gx|>1} [G : G_x]}$

where $S^G = \{ s \in S \mid gs = s \ \forall g \in G \} = \{ s \in S \mid Gs = \{s\} \}$
$= \{ s : |Gs| = 1 \}$

is the fixed point set of the action.

Example 1 $S = G$: Let $H \leq G$ be a subgroup acting on by left multiplication:

$$H \times G \xrightarrow{\mu} G, \quad \mu(h, g) = hg$$
(or: $h * g = hg$)

- H-orbit of $g \in G$ $= Hg$ is the right coset of H
- H-stabilizer of $g \in G$ $= H_g$
  $= \{ h \in H : hg = g \}$
  $= \{e\}$
- Fixed point set $= G^H$
  $= \{ g \in G : hg = g, \ \forall h \in H \}$
  (for $H \neq \{e\}$) $= \emptyset$

$\therefore$ Class eq: (for $H \neq \{e\}$) $\boxed{|G| = |G^H| + \sum_{|Hg|>1} [H : H_g]}$ (for $G \to H$, $S \to G$)

$$= |\emptyset| + \sum_{\substack{\text{right} \\ \text{cosets of } H}} [H : \{e\}]$$

$$= 0 + |H| \cdot [G:H]$$

$$\therefore \quad \boxed{|G| = |H| \cdot [G:H]} \qquad \text{[Lagrange's Theorem]}$$

<u>Example 2</u> (Classical Class Equation)

G acts on $S = G$ by conjugation $x \mapsto gxg^{-1}$

Then:

- orbits $Gx = \{gxg^{-1} : g \in G\} = Cl(x)$ conjugacy class of x
- stabilizers $G_x = \{g \in G : gxg^{-1} = x\} = C(x)$ centralizer of x
- fixed pt set $G^G = \{x \in G : gxg^{-1} = x, \forall g \in G\} = Z(G)$ center of G

Hence, if G is finite:

$$|G| = |Z(G)| + \sum_{|Cl(x)|>1} [G : C(x)]$$

<u>p-Groups</u>

<u>Def</u> A <u>p-group</u> is a finite group whose order is a power of a prime p. That is

For a prime p, G is a p-group if $|G| = p^n$ for some $n \geq 1$

<u>Examples</u>:

(1) $\mathbb{Z}_p, \mathbb{Z}_{p^2}, \mathbb{Z}_{p^3}, \ldots$

(2) $\mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_{p^3}, \ldots$

(3) $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_r}}$ $(k_i \geq 0)$

(4) $D_2, D_4, D_8, \ldots, D_{2^r}, \ldots$

(5) $\overset{\mathbb{Z}_2\times\mathbb{Z}_2}{Q_8}$ & generalized quaternion groups

<u>Remark</u> Most finite groups are p-groups!

In fact, most are 2-groups:

$$\lim_{n\to\infty} \frac{\#\{G : G \text{ 2-group}, |G|\le n\}}{\#\{G : |G|\le n\}} = 1$$

eg: Among all the groups of size $n \le 2000$ in the GAP database, the 2-groups (of size $\le 1{,}024$) are 99%

<u>Prop</u> Let G be a p-group acting on a finite set S. Then:

$$|S| \equiv |S^G| \pmod p$$

<u>Proof</u> Assume $|G| = p^n$. Then, the class eq gives:

$$\boxed{|S| = |S^G| + \sum_{|G_x|>1} [G : G_x]} \quad (*)$$

But, by Lagrange, any subgroup $H \le G$ has

$$|H| \cdot [G:H] = |G| = p^n$$

so $|H| = p^r$ and $[G:H] = p^s$, where $0 \le p, s \le n$ and $p+s = n$

So, in $(*)$: $[G:G_x] = p^s$ for some $0 \le p \le n$

but $|Gx|>1$ is equivalent to $[G:G_x] = \frac{|G|}{|G_x|} > 1$

and so $[G:G_x] > 1$

Hence $[G:G_x]$ is divisible by p

$\therefore$ $|S| = |S^G| \pmod p$ QED

Corollary Every p-group has non-trivial center.