Lecture 3: Order of a group & Basic Isomorphism Theorems

Last Time:

- Defined subgroups ($H < G$), normal subgroups ($H \triangleleft G$)
  ($gHg^{-1} = H \ \forall g \in G$)
- (normal) subgroups generated by a set.
- Left cosets $G/H = \{xH : x \in G\} /\sim$ $\quad x \sim y \Leftrightarrow x^{-1}y \in H$
- Right —— $H\backslash G = \{Hx : x \in G\} / \sim'$ $\quad x \sim' y \Leftrightarrow xy^{-1} \in H$
- Thm: If $H \triangleleft G$, then G/H is a group under $gH * g'H = gg'H$
  & $G \twoheadrightarrow G/H$ is gp hom with $\operatorname{Ker} G = H$.
- Cyclic groups & their classification
  - G infinite $\simeq \mathbb{Z}$
  - G finite $\simeq \mathbb{Z}/n\mathbb{Z}$ ($n = \#G$)
- Hamiltonian groups (Example: Quaternions Q_8 via gens & relations)

TODAY: Discuss order of a group & 3 Isomorphisms Thms in Group Theory.

More on cosets of a gp & First counting Lemma

Def $|G| = \#$ elements in G is called the order of G.

Eg: $|S_n| = n!$ $\qquad |\mathbb{Z}/n\mathbb{Z}| = n$.

- If $H < G$, then G breaks into a disjoint union of left cosets

$$\boxed{G = \bigsqcup_{\alpha \in A} g_\alpha H}$$

A = choice of representatives of G/H

In particular, A is in bijection with G/H. This gives us our first counting lemma.

Lemma: Assume G is finite. Then $|G| = |H|\,|G/H|$

Pf/ For each g $\varphi_g : H \longrightarrow gH$ is a bijection.
$h \longmapsto gh$

Corollary: $|H|$ divides $|G|$.

Remark: $|G/H|$ is usually denoted by $(G:H)$ = index of H in G

It is possible for both G & H to be infinite & yet $(G:H)<\infty$.

Example: $G=\mathbb{Z}$, $H=5\mathbb{Z}$ infinite but $(G:H)=5<\infty$

Def: If $(G:H)<\infty$ we say H is a finite index subgroup.

- Any $g\in G$ generated a subgroup $\langle g\rangle$. So we define:

Def The order of an element g of G is the order of $H=\langle g\rangle$

Obs: If $|H|=n<\infty$, then $g^n=e$ $\left(H=\{1,g,\dots,g^{n-1}\}\simeq\mathbb{Z}/n\mathbb{Z}\right)$.

$$g^\ell \longleftarrow\!\shortmid\ \bar{\ell}$$

Corollary: $\mathrm{Order}(g)\mid |G|$ whenever G is finite.

$\boxed{\text{Exponent of a group}}$

Def: Exponent of G = $\boxed{\exp(G)}$ = generator of $\{k \in \mathbb{Z} : g^k = e \ \ \forall g \in G\} \cap \mathbb{Z}_{\geq 0}$

Obs: • If $|G| < \infty$, then $\exp(G) > 0$ $\quad (g^{|G|} = e \ \ \forall g \in G)$

Converse is false: $G = \prod (\mathbb{Z}/2\mathbb{Z}) = \{(a_1, a_2, \dots,) \ \ a_i = 0,1 \ \forall i\}$
with term-by-term multiplication has $\exp(G) = 2$

Prop: • $\exp(G) = 1 \implies G = \{e\}$

• ______ $= 2 \implies G$ is abelian (Exercise)

• ______ $= 3$ need not be abelian

[Ex: Heisenberg gp / $\mathbb{F}_3$: $H_3 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a,b,c \in \mathbb{Z}/3\mathbb{Z} \right\} < GL_3(\mathbb{F}_3)$]

Burnside Problem (1902). Find all $(n, m) \in \mathbb{Z}^2_{>0}$ such that if G is a group with m generators (minimal #) & $\exp(G) = n$, then $|G| < \infty$.

Status: Known cases: $(1, n)$, $(2, n)$ many . . . Still **OPEN**! [$(2,5)$???]
$(m, 3)$, $(m, 4)$, $(m, 6)$ many. (see Wikipedia)

First Isomorphism Theorem

Theorem: Let G, G' be two groups and $\varphi : G \longrightarrow G'$ be a group homomorphism. Write $K = \mathrm{Ker}(\varphi) \lhd G$ & $H' = \mathrm{Im}(\varphi) < G'$.

Then we have a commutative diagram:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/K \arrow[r, "\overline{\varphi}"'] \arrow[ur, "\exists \Psi"] & H' \arrow[u, "i"'] \end{tikzcd}$$

$(\overline{\varphi}(gK) = \varphi(g))$

Here: π = natural projection & i is a natural inclusion.

Moreover, $\overline{\varphi}$ is an isomorphism

Remark: The other two isomorphism theorems will follow from this one.

$$\boxed{\underline{\text{First Iso Thm}}: \quad \frac{G}{\ker\varphi} \xrightarrow{\sim} \operatorname{Im}\varphi}$$

<u>Proof</u>: Define $\psi: G/K \longrightarrow G'$ by $\psi(gK) = \varphi(g)$

<u>Claim 1</u>: ψ is well-defined $(g_1K = g_2K \overset{?}{\Longrightarrow} \varphi(g_1) \overset{?}{=} \varphi(g_2))$

Pf/ $g_1K = g_2K \iff g_2^{-1}g_1 \in K$, so $\varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) = e'$. Thus, $\varphi(g_1) = \varphi(g_2)$ ✓

<u>Claim 2</u>: ψ is a group homomorphism:

Pf/ $\psi(g_1K\, g_2K) = \psi(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1K)\,\psi(g_2K)$ ✓

<u>Claim 3</u>: ψ is injective

Pf/ $\psi(gK) = e' \iff \varphi(g) = e' \iff g \in K \iff gK = K$. ✓

<u>Claim 4</u>: $\overline{\varphi} = \psi$ with range restricted to $H \overset{!}{=} \operatorname{Im}(\varphi)$

By definition $\overline{\varphi}$ is surjective & injective, so it is a bijection. ✓

<u>Exercise</u>: Bijective group homomorphisms are isomorphisms (HW1). $\square$

Second Isomorphism Theorem

Warm-up:

Prop 1: Given any group homomorphism $\varphi : G_1 \to G_2$, if $H_1 < G_1$ is a subgp then $\varphi(H_1) < G_2$ is a subgroup.

Prop 2: For any group homomorphism: if $\varphi : G_1 \to G_2$ & $N_2 \triangleleft G_2$, then $\varphi^{-1}(N_2) \triangleleft G_1$.

Theorem: Let G be a group and $N \triangleleft G$ a normal subgroup. Then

(i) The assignment $H \longrightarrow H/N$ is a bijection between

$$\left\{ \begin{array}{l} \text{Subgroups of} \\ G \text{ containing } N \end{array} \right\} \longleftrightarrow \left\{ \text{Subgroups of } G/N \right\}$$

(ii) Let $H < G$ be a subgroup containing N. Then,

H is normal <u>if and only if</u> H/N is normal in G/N

Furthermore, we have $G/H \xrightarrow{\sim} \dfrac{G/N}{H/N}$ $\quad gH \longmapsto gH/N$

$$\boxed{\text{Proof of } \left\{\begin{matrix}\text{Subgroups of} \\ G \text{ containing } N\end{matrix}\right\} \xleftrightarrow{\text{1-To-1}} \{\text{Subgroups of } G/N\} \qquad \begin{matrix} G & \xrightarrow{\pi} & G/N \\ \triangledown\ \vee & & \vee \\ N \subseteq H & \longleftrightarrow & H/N \end{matrix}}$$

Claim 1 If $N \subseteq H$, then $\pi(H) = \{hN : h \in H\} < G/N$

Pf/ (i) $e_{G/N}$ = identity of G/N $= eN \in \pi(H)$ ✓

(ii) $(h_1N)(h_2N) = h_1h_2N \ \forall h_1, h_2 \in H$ ✓ (iii) $(hN)^{-1} = h^{-1}N \ \forall h \in H$ ✓

For the converse, pick $\bar{H} < G/N$ a subgroup, let $\boxed{H = \pi^{-1}(\bar{H})}$

Claim 2: $H < G$ is a subgroup of G containing N & $\pi(H) = \bar{H}$.

Pf/ $N = \pi^{-1}(\{e_{G/N}\}) = \operatorname{Ker}\pi \subset \pi^{-1}(\bar{H}) = H$

$\boxed{\text{Want to show: } H < G}$ Use $H = \{g \in G : \pi(g) \in \bar{H}\}$

- $e \in H$ is clear since $e \in N \subset H$ ✓
- $g_1, g_2 \in H \Rightarrow \pi(g_1g_2) = \pi(g_1)\pi(g_2) \in \bar{H} \cdot \bar{H} = \bar{H}$. so $g_1g_2 \in H$. ✓
- $g \in H \Rightarrow \pi(g^{-1}) = \pi(g)^{-1} \in \bar{H}^{-1} = \bar{H} \Rightarrow g^{-1} \in H$ ✓

Finally: $\pi(H) = \bar{H}$ by the surjectivity of π $\square$

$$\boxed{N \subseteq H < G : \quad H \triangleleft G \iff H/N \triangleleft G/N}$$

Set $\boxed{\overline{H} := \pi(H) = H/N}$: $H \triangleleft G \iff ghg^{-1} \in H \ \forall g \in G \ \forall h \in H$

$\iff ghg^{-1}N \in \overline{H} \ \forall g \in G \ \forall h \in H \iff (gN)(hN)(g^{-1}N) \in \overline{H} \ \forall g \in G \ \forall h \in H$

$\iff \overline{H} \triangleleft G/N$.

$$\boxed{N \subseteq H \triangleleft G \implies G/H \xrightarrow{\sim} \frac{G/N}{H/N} \qquad gH \longmapsto g\,H/N}$$

Write:

$$\begin{tikzcd} G \arrow[r, two heads, "\pi_1"] \arrow[rr, bend right, "\psi = \pi_1 \circ \pi_2"'] & G/N \arrow[r, two heads, "\pi_2"] & \frac{G/N}{H/N} \end{tikzcd}$$

- ψ group hom ✓
- ψ surjective ✓

- $\underline{\operatorname{Ker}\psi = H}$: $\psi(g) = e \iff \pi_1(g) \in H/N \iff gN \in H/N$

$\iff gN = hN$ for some $h \iff g \in hN \subseteq H$.

Now, by 1st Isomorphism Thm: $G/H \underset{\psi}{\cong} \frac{G/N}{H/N}$.

Third Isomorphism Theorem

Theorem: Let G be a group, $H < G$ a subgroup & $N \triangleleft G$. Then:

(i) $H \cap N \subset H$ is a normal subgroup

(ii) $HN := \{ hx : h \in H, x \in N \} \subset G$. Then

$$\begin{cases} \bullet\ HN = NH \\ \bullet\ HN \text{ is a subgroup of } G. \end{cases}$$

(iii) $N \subset HN$ is a normal subgroup.

(iv) $$\begin{aligned} H/H\cap N &\longrightarrow HN/N \\ h(H \cap N) &\longmapsto hN \end{aligned}$$ is an isomorphism

Cartoon encoding (i) — (iii)

$H < G$

$N \lhd G$ $\rightsquigarrow$

$$\begin{tikzcd} & G \arrow[d, dash, "\vee\ \ (ii)"] & \\ & HN = NH \arrow[dl, dash, "<"'] \arrow[dr, dash, "\triangle\ \ (iii)"] & \\ H \arrow[dr, dash, "(i)\ \triangle"'] & & N \arrow[dl, dash, "<"] \\ & H \cap N & \end{tikzcd}$$

<u>Proof of (i)</u>: Want to show $H \cap N \lhd H$. Pick $h \in H$ & $x \in H \cap N$

Then: • $hxh^{-1} \in H$ because $H < G$

• $hxh^{-1} \in N$ —— $N \lhd G$

$\Rightarrow hxh^{-1} \in H \cap N$ $\square$.

<u>Proof of (ii)</u>: We first show $HN \subseteq NH$. Pick $hx \in HN$ ($h \in H$, $x \in N$)

<u>Claim 1</u>: $hx \in NH$ (Pf/ $hx = \underbrace{hxh^{-1}}_{\in N \lhd G} h \in NH$ ✓)

Proof of $NH \subset HN$ is similar.

<u>Claim 2</u>: HN is a subgroup of G

• $e = e \cdot e \in HN$ ✓

• $(h_1 x_1)(h_2 x_2) = h_1 h_2 \overbrace{h_2^{-1} x_1 h_2}^{\in N\ (N \lhd G)} x_2 \in HN$

• $(hx)^{-1} = x^{-1} h^{-1} \in NH \underset{\text{Claim 1}}{=} HN$ $\forall h \in H, x \in N$.

$H < G$
$N \lhd G$ $\rightsquigarrow$

$$\begin{tikzcd}
 & G \arrow[d, dash, "\vee"] \arrow[d, phantom, shift left=6ex, "(ii)"] & \\
 & HN = NH \arrow[dl, dash, "<"'] \arrow[dr, dash, "\rhd\ (iii)"] & \\
H \arrow[dr, dash, "(i)\ \rhd"'] & & N \arrow[dl, dash, "<"] \\
 & H \cap N &
\end{tikzcd}$$

Proof of (iii)

$N \lhd G$ & $N < HN \leq G$

So $N \lhd HN$ ✓

$$\boxed{\begin{array}{lccl} \text{(iv)} & H/H\cap N & \longrightarrow & HN/N \quad \text{is an isomorphism} \\ & h(H \cap N) & \longmapsto & hN \end{array}}$$

Proof Consider $H \overset{\varphi = \pi \circ i}{\xhookrightarrow[\text{inclusion}]{i} HN \xrightarrow[\text{projection}]{\pi}} HN/N$ • φ gp homomorph.

Claim 1: φ is surjective

Pf/ $hxN = hN$ for $h \in H$, $x \in N$

But $hN = i(h)$

$\Rightarrow \varphi(h) = hxN$

Claim 2 $\operatorname{Ker} \varphi = H \cap N$

Pf/ $h \in \operatorname{Ker}\varphi \iff \varphi(h) = \bar{e} \in HN/N$

$(h \in H) \iff hN = N \iff h \in H \cap N$ ✓

$\xRightarrow{\text{1st Iso Thm}}$ $\boxed{H/H\cap N \simeq HN/N}$