Lecture III: Quotients & cyclic groups, first counting lemma

Last Time: • Defined subgroups of a gp G: gp structure inherited from G

$(\emptyset \neq H < G$ if and only if $(x, y \in H \Rightarrow x * y^{-1} \in H))$

• Defined normal subgroups: $H \triangleleft G \iff H < G$ & $a^{-1}ba \in H$ $\forall a \in G, b \in H$

• **TODAY**: • quotient groups, first counting lemma.
- classification of cyclic groups
- generators of a group
- exponent / order of a group

§1 Quotient groups

GOAL: Given $H < G$ want to build G/H

Consider the relation $\sim$ on G given by $x \sim y$ if $x^{-1}y \in H$ (equiv: $xH = yH$ as sets)

Lemma: $\sim$ is an equivalence relation.

Pf/ • Symmetry: Say $x \sim y \Rightarrow x^{-1}y \in H \underset{H \text{ subgp}}{\Rightarrow} (x^{-1}y)^{-1} = y^{-1}x \in H$
$\Rightarrow y \sim x$

• Reflexive: $x \sim x \iff x^{-1}x = e \in H$ ✓

• Transitive $x \sim y$ & $y \sim z \overset{?}{\Rightarrow} x \sim z$

$\Rightarrow x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \cdot H \underset{H \text{ subgp.}}{\subseteq} H$ □

Def: $\boxed{G/H}$ = set of equivalence classes in G with respect to $\sim$.
= left cosets (modulo H) $= \{xH \quad x \in G\}$

Similarly: $\boxed{H\backslash G}$ = right cosets (modulo H)
= set of equiv classes in G under
$x \sim' y \iff yx^{-1} \in H$ (equiv $Hy = Hx$)

Q: Do G/H and/or $H\backslash G$ have any algebraic structure?

A: Only when $H \triangleleft G$

Proposition 1: Assume $H \triangleleft G$. Then, G/H has a group structure induced from the one on G. Explicitly: $g_1H \cdot g_2H := g_1g_2H$

($e_{G/H} = 1 \cdot H$ & $(gH)^{-1} = g^{-1}H$).

The natural projection $\pi: G \twoheadrightarrow G/H$, $g \mapsto gH$ is a gp homomorphism with $\mathrm{Ker}(\pi) = H$

Pf/ • Claim 1: Law of composition is well-defined, ie

$$\boxed{g_1 \sim g_1' \ \& \ g_2 \sim g_2' \overset{?}{\Longrightarrow} g_1g_2 \sim g_1'g_2'}$$

Indeed, $g_\ell \sim g_\ell' \Rightarrow g_1^{-1}g_1' \in H$, $g_2^{-1}g_2 \in H$ $(\ell = 1,2)$

Want to show: $(g_1g_2)^{-1}g_1'g_2' \in H$

$$(g_1g_2)^{-1}g_1'g_2' = g_2^{-1}\underbrace{(g_1^{-1}g_1')}_{\in H}g_2' = \underbrace{g_2^{-1}\underbrace{(g_1^{-1}g_1')}_{\in H}g_2}_{\in H \text{ because } H \triangleleft G}\underbrace{g_2^{-1}g_2'}_{\in H} \in H$$

• Claim 2: Law of composition on G/H is associative (This is inherited from G)

• The assertions: $eH = e_{G/H}$ & $(gH)^{-1} = g^{-1}H$ are clear $\square$

§1 Cyclic groups:

Motivating example: $(\mathbb{Z}, +)$ is abelian, so every $N < \mathbb{Z}$ is normal

Q: What does $\mathbb{Z}/N$ look like?

Lemma: Fix $N < \mathbb{Z}$. Then, $\exists\, n \in \mathbb{Z}_{\geq 0}$ st

$$N = n\cdot\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$$

Pf/ • If $N=\{0\}$, then $n=0$ ✓

• Assume $N \neq \{0\}$ & let n = smallest positive integer in N

<u>Claim</u>: $N = n\mathbb{Z}$

Indeed, $n\mathbb{Z} \subseteq N$ because N is a subgroup.

Assume $N \not\subseteq n\mathbb{Z}$, then $n \neq 1$ & $\exists\, 0< m \in N \setminus n\mathbb{Z}$

Pick $k \in \mathbb{Z}_{>0}$ s.t $k < \frac{m}{n} < k+1 \implies kn < m < (k+1)n$

$$\implies 0 < \underbrace{\underbrace{m}_{\in N} - \underbrace{nk}_{\in N}}_{\in N \text{ (N subgroup)}} < n$$ Contradicts minimality of n. □

<u>A</u>: $\mathbb{Z}/N = \boxed{\mathbb{Z}/n\mathbb{Z}}$ with law of composition "<u>addition modulo n</u>"

• The above examples are cyclic groups.

<u>Def</u> A group G is <u>cyclic</u> if $\exists\, g \in G$ s.t every element of G is of the form g^m for some $m \in \mathbb{Z}$, that is:

↪ also not unique

$$g^m = \begin{cases} \underbrace{g \cdots g}_{m \text{ times}} & \text{if } m>0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{(-m) \text{ times}} & \text{if } m<0 \end{cases}$$

<u>Name</u>: g = a generator for G (not unique!)

Eg for $\mathbb{Z}$: $\{\pm 1\}$ = set of generators of $\mathbb{Z}$.

<u>Exercise</u>: Number of possible generators of $\mathbb{Z}/n\mathbb{Z} = \Phi(n)$

Here, $\Phi(n) = \#\{\ell \in \{1, \ldots, n-1\} : \gcd(\ell, n) = 1\}$ Euler's Phi function

<u>§3. Subgroups generated by a set</u>:

<u>Lemma</u>: Fix H_1, H_2 subgroups of G. Then

(1) $H_1 \cap H_2$ is a subgroup of G

(2) If $H_1 \lhd G$ & $H_2 \lhd G$, then $H_1 \cap H_2 \lhd G$.

Proof: Easy & works for arbitrary intersections.

Def: Given a set $X \subseteq G$, we define $\langle X \rangle \subset G$ as the smallest subgroup of G containing the set X.

Name: $\langle X \rangle$ subgroup generated by X.

Obs: $\langle \emptyset \rangle = \{e\}$. (trivial subgp)

Similarly: $N\langle X \rangle$ = normal subgroup generated by X
= smallest normal subgp containing X.

Def. G is finitely generated if $\exists$ finite $A \subset G$ with $\langle A \rangle = G$.

For cyclic groups: $G = \langle \{g\} \rangle$ for some $g \in G$

$$= \{e, g, g^2, g^3, \dots, g^{-1}, g^{-2}, g^{-3}, \dots\}$$

$\rightsquigarrow$ 2 options: $\{e, g, g^2, \dots, g^{-1}, g^{-2}, \dots\}$ is infinite (A)

$\{\_\_\_\_\}$ is finite (B)

Option (A): G is isomorphic to $\mathbb{Z}$ $\qquad \mathbb{Z} \xrightarrow{\sim} G \quad n \mapsto g^n$.

Option (B) Pick n = smallest positive integer s.t.

$g^n \in \{e, g, g^2, \dots, g^{n-1}\}$ $\qquad$ ($n > 1$ if $G \neq \{e\}$)

Claim: $g^n = e$

Otherwise, $g^n = g^\ell$ for $0 < \ell < n \Rightarrow g^{n-\ell} = e \in \{e, g, \dots, g^{n-\ell-1}\}$

Then, n was not minimal. Contr!

Then $G = \{e, g, g^2, \dots, g^n\} \simeq \mathbb{Z}/n\mathbb{Z}$

$(g^{-1} = g^{n-1})$ $\qquad g^m \longleftarrow \bar{m} := m(n\mathbb{Z})$ is well def

Classification Thm: All cyclic groups are isomorphic to

$\mathbb{Z}$ (infinite) or $\mathbb{Z}/n\mathbb{Z}$ (finite cyclic) for some $n \in \mathbb{Z}_{>1}$.

These are examples of group presentations (generators & relns)

$\mathbb{Z} = \langle g \rangle = \langle g \mid$ only obvious rules $(g^0 = e,\ g^k g^l = g^{k+l}) \rangle$

$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \bar{n} \} = \langle g \mid g^n = e \rangle$ ← usually omitted

$= \langle g \mid g^n \rangle$

§4. More on cosets & 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 $\varphi_g : H \longrightarrow gH$, $h \longmapsto gh$ is a bijection.

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.