Group Theory
Week #4, Lecture #16

I Generating sets

- Recall a cyclic group G is generated by a single element:

$$\boxed{G = \langle a \rangle = \{e, a, a^2, \dots, a^n, \dots\}}$$

($G \cong \mathbb{Z}_n$ for some n, or $G \cong \mathbb{Z}$)

- Other groups need 2 or more generators.

Def Let $S \subseteq G$ be a subset of a group G. The subgroup of G generated by S is:

$$\boxed{\langle S \rangle := \{g \in G : g = x_1^{\pm 1} \cdots x_n^{\pm 1}, \text{ for some } x_i \in S\}}$$

all possible finite products of elements in S and their inverses

note: $S \subseteq \langle S \rangle$

Check that $\langle S \rangle$ is indeed a subgroup of G:

Let $g = x_1 \cdots x_n$, $h = y_1 \cdots y_m$ $\in \langle S \rangle$.

where $x_i, y_j \in S \to y_j^{-1} \in S$

Then
- $gh = (x_1 \cdots x_n)(y_1 \cdots y_m) = x_1 \cdots x_n y_1 \cdots y_m \in \langle S \rangle$
- $e \in \langle S \rangle$ (the empty product)
- $h^{-1} = y_m^{-1} \cdots y_1^{-1} \in S$ ✓

Remark 1 If G is written additively $\div$ $G = (G, +, 0)$ (something we usually do if G is abelian) — then

$$\begin{aligned}
\langle S \rangle &= \{g \in G \mid g = \pm x_1 \pm \cdots \pm x_n \text{ for } x_i \in S\} \\
&= \{g \in G \mid g = c_1 x_1 + \cdots + c_n x_n \quad x_i \in S, \ c_i = \pm 1\} \\
&= \{g \in G \mid g = k_1 x_1 + \cdots + k_n x_n, \quad x_i \in S, \ k_i \in \mathbb{Z}\}
\end{aligned}$$

all linear combinations of element in S

This is similar with the definition of a vector subspace $W = \langle S \rangle \leq V$ inside a vector space V

Remark 2 $\langle S\rangle$ is the smallest subgroup of G containing S. In fact:

$$\boxed{\langle S\rangle = \bigcap_{\substack{\cdot\, H\le G\\ \cdot\, S\subseteq H}} H}$$

Remark 3. If $G=\langle S\rangle$, we call S a *generating set* for G, and the elements of S are called *generators* of G.

· G is a *finitely generated* group if $G=\langle x_1,\dots,x_n\rangle$ for some $x_i\in G$.

Examples

(1) $G=\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$ is generated by $x=(1,0)$ and $y=(0,1)$ (much the same as $\mathbb{R}^2$ is -nerated by x & y)

i.e.: $\mathbb{Z}^2=\langle x,y\rangle$

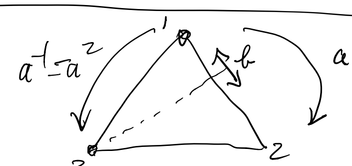
in other words, every pair $(m,n)\in\mathbb{Z}^2$ can be written as

$$(m,n) = \pm(1,0)\pm\cdots\pm(1,0)\pm(0,1)\pm\cdots\pm(0,1)$$

eg:
$$(5,-3) = \underbrace{(1,0)+\cdots+(1,0)}_{5}\underbrace{-(0,1)-\cdots-(0,1)}_{3}$$

---

(2) $G=S_3$



Let $a = 120°$ rotation $= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

b = reflection in dashed axis $= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

Then G is generated by a and b:

$$S_3=\Big\{\underset{e}{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}, \underset{a}{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}}, \underset{a^2}{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}, \underset{b}{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}}, \underset{ba}{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}}, \underset{ba^2}{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}}\Big\}$$

$= \langle \{a, b\} \rangle$

In fact, S_3 has presentation:

$$S_3 = \langle \underset{\uparrow \atop \text{generators}}{a, b} \mid \underbrace{a^3 = e,\ b^2 = e,\ ba = a^2 b}_{\text{relations in the group}} \rangle$$

$$= \underset{\underset{\{e, a, a^2\}}{\langle a \rangle}}{\mathbb{Z}_3} \sqcup \underset{\{b, ba, ba^2\}}{b\mathbb{Z}_3}$$

For a presentation for the dihedral group D_n (symmetries of the n-gon), see notes on webpage.

II Derived subgroup and abelianization

Def Given elements x, y in a group G, their commutator is

$$\boxed{xyx^{-1}y^{-1} \in G}$$

- This is usually denoted by $[x,y]$ (or (x,y))
- Warning: GAP uses $[x,y] = x^{-1}y^{-1}xy$
- Note x and y commute (i.e., $xy = yx$) if and only if their commutator is the identity (i.e., $xyx^{-1}y^{-1} = e$)

"commutator measures failure of commutativity"

Def The derived subgroup (or, the commutator subgroup) of a group G is

$$\boxed{G' = \langle \{ g \in G : g = xyx^{-1}y^{-1} \text{ for some } x, y \in G \} \rangle}$$

i.e., the set of all products of commutators in G.

Examples: (1) G abelian (or, commutative) $\Rightarrow G' = \{e\}$

(2) $G = S_3 \Rightarrow G' = \{e, a, a^2\} \cong \mathbb{Z}_3$

reason: $ba = a^2 b \Rightarrow a^2 = bab^{-1} \Rightarrow a = bab^{-1}a^{-1} = [b,a]$

Proposition (1) G' is a normal subgroup of G.

(2) G/G' is abelian

(3) If $N \triangleleft G$, then:

G/N is abelian $\iff G' \subseteq N$

Proof (1)(i) G' is a subgroup:

- $g, h \in G' \Rightarrow g = aba^{-1}b^{-1}$, $h = xyx^{-1}y^{-1}$ for some $a, b, x, y \in G$

$\Rightarrow gh = aba^{-1}b^{-1} \cdot xyx^{-1}y^{-1} \in G'$

we need $\langle \ldots \rangle$ here!

- $g \in G' \Rightarrow g = aba^{-1}b^{-1}$ $a, b \in G$

$\Rightarrow g^{-1} = bab^{-1}a^{-1} \in G'$ (i.e., $[a,b]^{-1} = [b,a]$)

- $e = [e,e] \in G'$

(ii) G' is a normal subgroup:

$\underset{aba^{-1}b}{g} \in G'$, $x \in G \Rightarrow xgx^{-1}g^{-1} \in G'$ (by def of G')

$\Rightarrow xgx^{-1} \in G'$ (since G' is a subgroup)

multiply by g on the right

(2) G/G' abelian:

let aG' and bG' be two cosets of G'. Then (*)

$aG' \cdot bG' \cdot (aG')^{-1} \cdot (bG')^{-1} = aG' \cdot bG' \cdot a^{-1}G' \cdot b^{-1}G'$

$$= aba^{-1}b^{-1}\cdot G'$$

since $aba^{-1}b^{-1} \in G'$ $\longrightarrow$ $= G'$

(3) ($\Rightarrow$) If $N \trianglelefteq G$ & G/N is abelian, then, for $\forall\, a,b \in G$:

$$aba^{-1}b^{-1}N = N \qquad \text{(by argument (*1))}$$

$$\therefore\ aba^{-1}b^{-1} \in N$$

$$\therefore\ G' \subseteq N$$

($\Leftarrow$) If $G' \subseteq N \trianglelefteq G$, then, by the $\underline{2^{nd}\text{ Iso Thm}}$ (next week)

The projection $\pi: G \twoheadrightarrow G/N$ factors through a projection $\bar{\pi}: G/G' \twoheadrightarrow G/N$

Hence, since G/G' is abelian by (2), we conclude that G/N is also abelian. $\square$

__Note__ Here at the end we ~~u~~sed:

(exercise!) __Lemma__ Every factor group of an abelian group is again abelian

---

Notation/terminology:

$\boxed{G_{ab} := G/G'}$ is called the __abelianization__ of G

By above Prop (part 3), G_{ab} is the largest abelian quotient of G:

$$\begin{tikzcd} G \arrow[r, two heads, "\pi"] \arrow[dr, "q"'] & G_{ab} = G/G' \arrow[d, dashed, "\varphi"] \\ & H \end{tikzcd}$$

surjective homomorphism

abelian group

a surjective hom. φ exists such that $\varphi \circ \pi = q$

Examples ① G simple group $\Rightarrow G_{ab} = \begin{cases} G & \text{if } G \cong \mathbb{Z}_p \ (p \text{ prime}) \\ \{e\} & \text{otherwise} \end{cases}$

reason: $G' \triangleleft G \underset{G \text{ simple}}{\Longrightarrow} G' = \{e\} \Rightarrow G_{ab} = G$ (this happens when $G = \mathbb{Z}_p$)

or $G' = G \Rightarrow G_{ab} = \{e\}$

eg: · $(A_n)_{ab} = \{e\}$ for $n \geq 5$

· $(S_3)_{ab} = S_3/\mathbb{Z}_3 \cong \mathbb{Z}_2$

Prop Every hom $\varphi: G \longrightarrow H$ takes G' to H'
(This implies the derived subgroup is a "fully characteristic subgroup" of G)

Proof $\forall g, h \in G$:
$$\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})\varphi(h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} \in H' \quad \boxtimes$$

Cor Every hom between two groups induces a hom between their abelianizations:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi_G \downarrow & & \downarrow \pi_H \\ G_{ab} & \xrightarrow{\varphi_{ab}} & H_{ab} \end{array} \qquad \varphi_{ab} \circ \pi_G = \pi_H \circ \varphi$$

$$\varphi_{ab}(x G') := \varphi(x) \cdot H'$$

Cor If $G \cong H$, then $G_{ab} \cong H_{ab}$:

$$\varphi: G \xrightarrow[\text{iso}]{\cong} H \Longrightarrow \varphi_{ab}: G_{ab} \xrightarrow{\cong} H_{ab}$$