Feb11

Thursday, February 11, 2021 12:58 PM

Subgroups generated by multiple elements

2 philosophies in defining sets.

1) In terms of its elements.
2) In terms of its properties.

Lemma G a group $x \in G$. Then $\langle x \rangle$ is the smallest subgroup of G containing x.

Proof
If $x \in H$, then $\langle x \rangle \le H$
But this is clear as H is closed under mult & inv ∅

Prop * Let $\mathcal{A}$ be a collection of subgroups of G.
Then $K = \bigcap_{H \in \mathcal{A}} H \le G$. ✓

Proof Exercise.

Def^n $A \subseteq G$ be a subset.

Then the subgroup generated by A

$$\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subseteq H}} H$$

Notation $A = \{x, y\}$ $\quad \langle \{x, y\} \rangle = \langle x, y \rangle$

A, B 2 subsets

$$\langle A \cup B \rangle = \langle A, B \rangle .$$

Fact Existence & uniqueness comes for free.

Prop Let $A \subseteq G$ subset. $H \leq G$

Then if $A \subseteq H$, $\langle A \rangle \leq H$.

Pf/ 1) Subgroup by $*$

2) $\langle A \rangle = \bigcap\limits_{A \subseteq H' \leq G} H' \leq H.$ $\quad \varnothing$

$\uparrow$ H is one of thes

Construction $A \subseteq G$ subset

Let $$\overline{A} = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \;\middle|\; \begin{array}{l} n \in \mathbb{Z}_{\geq 0},\ a_i \in A \\ \varepsilon_i = \pm 1 \end{array} \right\}$$

Prop $$\overline{A} = \langle A \rangle$$

Proof

① $\overline{A} \leq G$.

$$(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n})(b_1^{\delta_1} \cdots b_m^{\delta_m}) \in \overline{A}$$

$$(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \cdots a_1^{-\varepsilon_1}$$

check (HW2?)

② $a \in A$. $\Longrightarrow a^1 \in \overline{A}$

$$A \subseteq \overline{A}$$

$$\Longrightarrow \langle A \rangle \leq \overline{A} \quad \text{(by def)}$$

③ $a_1, \dots, a_n \in A \rightsquigarrow a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \in \langle A \rangle$

bc closed under mult & inv.

$$\Longrightarrow \overline{A} \leq \langle A \rangle$$ we win

---

Observe

If G abelian. Then $a_1, \dots, a_n \in G$

$$\langle a_1, \dots, a_n \rangle = \{ a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} \mid a_i \in \mathbb{Z} \}$$

$\rightsquigarrow$ If $|a_i| = d_i$

Then writ $0 \le \alpha_i < d_i$

$$\Rightarrow |\langle a_1, \dots a_n \rangle| \le d_1 d_2 \cdots d_n.$$

In a nonabelian setting, much more complicated.

Ex $G = GL_2(\mathbb{R})$

$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$N = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$

Check

$M^2 = N^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$|M| = |N| = 2.$

$(MN) = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$

well $(MN)^n = \begin{pmatrix} 1/2^n & 0 \\ 0 & 2^n \end{pmatrix}$ never $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

But $|MN| = \infty$

& $|\langle M, N \rangle| = \infty$

Moral Subgroups of nonabelian groups may be hard to pin down in terms of properties.

More examples of subgroups

Def^n Let G be a group. $A \subseteq G$ a subset. The centralizer of A in G is the set of elts of g that commute with A.

$$C_G(A) = \{ g \in G \mid ga = ag \quad \forall\, a \in A \}$$

$$= \{ g \in G \mid \underbrace{g\overset{\swarrow}{a}g^{-1}}_{\text{conjugate of } a \text{ by } g.} = \overset{\swarrow}{a} \quad \forall\, a \in A \}$$

Prop $C_G(A) \leq G$

Pf/ $g \in C_G(A) \implies gag^{-1} = a \quad \forall a$

$\implies a = g^{-1}ag \quad \forall a$

$\implies g^{-1} \in C_G(A)$

$g, h \in C_G(A)$

$$(gh)a(gh)^{-1} = (g\underbrace{h)a(h^{-1}}g^{-1})$$

$$= gag^{-1} \qquad \forall\, a \in A$$

$$= a$$

$\implies gh \in C_G(A)$ ⊘

Exercise

$$C_G(A) = C_G(\langle A \rangle) \quad (N_G \text{ as well?})$$

Important Special Case

The center of G is

$$Z(G) = C_G(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$$

Defn ① Let $a \in G$, $g \in G$. Then the congutate of a by g is $gag^{-1} \in G$

② Let $A \subseteq G$ and $g \in G$, then the congugate of A by g is

$$\longrightarrow gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G$$

Exercise Show gAg^{-1} is bijective to A.

Defn The normalizer of A in G is

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

Exercise

1) $N_G(A) \leq G$

2) $Z(G) \leq C_G(A) \leq N_G(A) \leftarrow$

Examples

For any A

① G abelian. Then

$$G = Z(G) = C_G(A) = N_G(A)$$

Exercise G ab
$gag^{-1} = a$ always.

② $D_8 \supseteq R = \{1, r, r^2, r^3\}$

① $C_{D_8}(R)$

i) $r^i r^j = r^j r^i \quad \forall\, i, j.$

$\rightsquigarrow R \subseteq C_{D_8}(R)$

Exercise $H \leq G$
Show $C_G(H) \supseteq H \iff H$ abelian.

ii) $srs^{-1} = r^{-1}ss^{-1} = r^3 \neq r$
so $s \notin C_{D_8}(R)$.

iii) $sr^i \notin C_{D_8}(R)$ b/c if it were
$(sr^i)(r^{-i}) = s$ would be there ↯

$\Longrightarrow C_{D_8}(R) = R,$

② $N_{D_8}(R)$.

i) $R \subseteq N_{D_8}(R)$

ii) Look at

$sRs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\}$

$= \{1, r^3, r^2, r\} \leftarrow$ check.

$= R.$

$\rightsquigarrow s \in N_{D_8}(R).$

So $r, s \in N_{D_8}(R). \implies \underset{\overset{\|}{D_8}}{\langle r, s\rangle} \subseteq N_{D_8}(R)$

So $N_{D_8}(R) = D_8.$

$\uparrow$ Impt property

This doesn't always happen

③ $N_{D_8}(\langle s\rangle)$ $\quad rsr^{-1} = sr^{-2}$

$= sr^2 \in \underset{}{\langle s\rangle}$ $\quad \overset{\{1, s\}}{\shortparallel}$

$\rightsquigarrow r \notin N_{D_8}(\langle s\rangle) \neq D_8.$

④ $Z(D_8) \subseteq C_{D_8}(R) = R$

$rs \neq sr$ so $r \notin Z(D_8)$

$\rightsquigarrow r^3s \neq sr^3$ so $r^3 \notin Z(D_8).$

(or notice $r^3 \in Z \to \underset{\underset{r}{\psi}}{\langle r^3\rangle} \in \underset{\eta}{Z}$)

$$r^2 s = s r^{-2} = s r^2$$

See $r^2 \in C_{D_8}(r, s) = C_{D_8}(\langle r, s \rangle)$

$$= C_{D_8}(D_8) = Z(D_8)$$

$$\rightsquigarrow \quad Z(D_8) = \{1, r^2\} = \langle r^2 \rangle.$$

Exercise

$$Z(D_{2n}) = \begin{cases} \{1, r^{n/2}\} & n \text{ even} \\ \{1\} & n \text{ odd} \end{cases}$$

Stabilizer of a group action

Let $G \times A \longrightarrow A$ be an action.

Let $a \in A$.

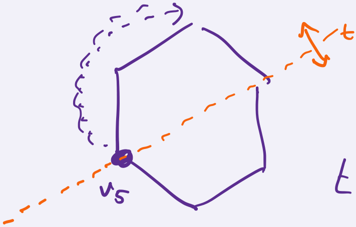
The stabilizer of a in A is

$$G_a = \{g \in G \mid g \cdot a = a\}$$

Exercise $\quad G_a \leq G.$

Example

$$G = D_{12} \circlearrowright \{v_1, v_2, \dots, v_6\}$$



$$G_{v_5} = \{1, t\}$$

$$t = r^{-2} s r^2 = s r^4$$

Quotient Groups

Idea: Dual to subgroups

$K \leq G \longleftrightarrow G \twoheadrightarrow H$

(injective homomorphism) (surjective homomorphism)

3 perspectives

① Images of homomorphisms.

② Fibers of homomorphisms.

③ Cosets (equivalence modulo subgroups).

Example

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ a &\longmapsto \bar{a} \end{aligned}$$

① Image is $\mathbb{Z}/n\mathbb{Z}$

② Fiber $\phi^{-1}(\bar{a}) = \{a, a \pm n, a \pm 2n, \ldots\}$

〃

③ Congruence class of a

How did we add in $\mathbb{Z}/n\mathbb{Z}$?

$\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ ⇝ Lift to $a, b \in \mathbb{Z}$

⇝ Added $a+b \in \mathbb{Z}$

⇝ Mapped to $\overline{a+b}$

Observe: This works for any surjective homomorphism.

Let $\phi : G \longrightarrow H$ surjective homom.

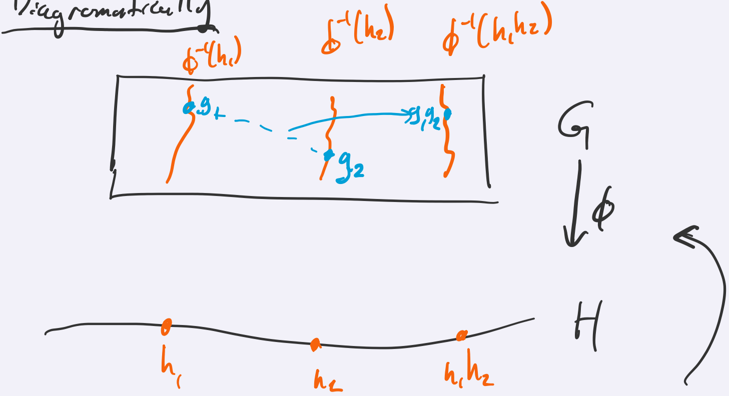
Let $h_1, h_2 \in H$.

Pick g_i s.t. $\phi(g_i) = h_i$. $(i = 1, 2)$

Multiply $g_1 g_2$

Apply ϕ get $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2$.

Diagrammatically



"Quotients as surjective homomorphisms"

upshot

Multiplication in H is determined by multiplication in G (and ϕ).

Perpective 2 Fibers of surjective hom.

$\phi: G \longrightarrow H$ surjective homomorphism.

HW3 #3(b) $\Longrightarrow$ Fibers partition G.

HW1 $\Longrightarrow$ Get an equivalence relation

$$g_1 \sim g_2 \iff \phi(g_1) = \phi(g_2).$$

Define $F = \mathrm{Fib}(\phi, G) = \{\text{fibers of } \phi\}$.

$$= \{\phi^{-1}(h) \mid h \in H\}$$

Get a natural two natural ways to add equivalence classes.

① $\phi^{-1}(h_1) \cdot \phi^{-1}(h_2) = \phi^{-1}(h_1 h_2)$.

Want to avoid using H to find an intrinsic notion of quotient.

② $g_1 \in \phi^{-1}(h_1)$. $g_2 \in \phi^{-1}(h_2)$

$$[g_1] \cdot [g_2] = [g_1 g_2]$$

Define × w/o H but need the elts.

Proof well defined

$\rightarrow \hat{g}_1 \sim g_1$

$\rightarrow \hat{g}_2 \sim g_2$

$\Longrightarrow \hat{g}_1 \hat{g}_2 \sim g_1 g_2$

i.e. in same fiber.

$$\begin{aligned}\phi(\hat{g}_1 \hat{g}_2) &= \phi(\hat{g}_1)\,\phi(\hat{g}_2)\\ &= \phi(g_1)\,\phi(g_2)\\ &= \phi(g_1 g_2)\end{aligned}$$

✓

Observe $\underline{\mathrm{Fib}(\phi, G)} \xrightarrow{\sim} \underline{\underline{H}} \leftarrow$

$\phi^{-1}(h) \longmapsto h.$

(prove $\mathrm{Fib}(\phi, G)$ a group.

$\mathrm{Id} = \phi^{-1}(1) = \ker\phi$)

$\uparrow$

$\underline{\underline{g_0}} \in \ker\phi$

$$[g_0]\cdot[g] = [g_0 g] = [g].$$

$$\phi(g_0 g) = \underbrace{\phi(g_0)}_{1}\,\phi(g) = \phi(g)$$

$\emptyset$

Right now

Set is classes in G | **BUT**

Mult is in G.

To define equiv classes need ϕ & H.
How do we eliminate this need?

Ex Addition of fibers in $\mathbb{Z}/n\mathbb{Z}$.

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z} \arrow[u, "\pi"] \end{tikzcd}$$

$\bar{a} = \{a \pm kn\} \subseteq \mathbb{Z}$

we didn't say if $\pi(a) = \pi(b)$

$\bar{a} = \bar{b}$

$\iff a \equiv b \mod n$

$\iff a = b + kn.$

$\iff a - b \in n\mathbb{Z}.$

$\ker(\pi) = \{0, \pm n, \pm 2n, \dots\}$
$= n\mathbb{Z}.$

$\phi : G \longrightarrow H.$ ← surjective. Let $K = \ker \phi.$

Defn $a, b \in G.$

Say $a \equiv b \mod K$ if

$\exists\, k \in K$ s.t. $a = bk$

Equivalently, $b^{-1}a \in K.$

Observe

$$\phi(a) = \phi(b) \iff a \equiv b \mod K.$$

Pf/ $\Longrightarrow$ Let $k = b^{-1}a$.

Then $\phi(k) = \phi(b)^{-1}\phi(a) = 1$ b/c $\phi(a) = \phi(b)$

$\Longrightarrow k \in K$

$\Longrightarrow a \equiv b \mod K.$

$\Longleftarrow$ If $a \equiv b \mod k$.

$a = bk$.

$\Longrightarrow \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b)$ Ø

Upshot

Equivalence mod K ARE the fibers of ϕ, defined wrt K not wrt ϕ & H.

Perspective 3: Equivalence classes modulo $K \leq G$.

$$\begin{tikzcd}
\text{Image of } \phi \arrow[rr, Leftrightarrow] & & \text{Fibers of } \phi \\
& \text{Equiv mod } K \arrow[ul, Rightarrow] \arrow[ur, Rightarrow] &
\end{tikzcd}$$

More on this later