Math 322, lecture 8, ~~Tue~~ 3/Oct/2017

Today: (1) Subgps
(2) Coset spaces

Subgroups & generating sets

Lemma: The intersection of a (non-empty) family of subgps is a subgp

Pf: Let $\mathcal{H}$ be a set of subgps of G.

Let $H = \bigcap \mathcal{H}$

Then $e_G \in K$ for all $K \in \mathcal{H}$ (they are subgps)

so $e_G \in H$.

Also, if $x, y \in H$ then for all $K \in \mathcal{H}$, $x, y \in K$ so $xy^{-1} \in K$,

so $xy^{-1} \in K$ for all $K \in \mathcal{H}$, so $xy^{-1} \in H$.

Def: Given $S \subset G$, the subgroup generated by S is the subgp

$$\langle S \rangle \overset{\text{def}}{=} \bigcap \{ H < G \mid S \subseteq H \}$$

(note: G is a subgp of G so RHS is non-empty)

Remarks: Note that $S \subset \langle S \rangle$, so $\langle S \rangle$ is the smallest subgp containing S.

Def: A word in S is an expression $\prod_{i=1}^{r} x_i^{\varepsilon_i} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$ where $x_i \in S$, $\varepsilon_i \in \{\pm 1\}$

Aside: Let G be a gp, $S \subseteq G$.

Set Let $\mathrm{Cay}(G;S)$ be the graph with vertex set G, edge set $\{(g, gs)\}_{s \in S \cup S^{-1}}$

S generates G ($\langle S \rangle = G$) iff $\mathrm{Cay}(G;S)$ is cntd

$\mathrm{diam}(G)$ = maximum distance of two vertices

$$= \max_{g \in G} \{ \min_{\substack{w \text{ in } S \cup S^{-1} \\ w \text{ rep'ns } g}} |w|_S$$

Think of S as "efficient" if $\mathrm{diam}(G)$ wrt S is small

Cs: $\mathrm{diam}(S_n;\ \text{transp}) \approx n \log n$ (mergesort)

Open question: how large can $\mathrm{diam}(S_n; S)$ get?

($n \log n \approx \log \# S_n$)

Conj: (Babai) $\mathrm{diam}(S_n; S) \leq (\log \# S_n)^C$ (C fixed)

Best result (Helfgott - Seress) $\leq \exp((\log n)^4 (\log \log n)^C)$

A word in $\{a, b\}$ is something like: $aaba^{-1}bbbaab^{-1}a$

By induction on r, if w is a word in S and $S \subseteq H < G$, ~~...~~, then $w \in H$.

<u>Prop</u>: $\langle S \rangle = \{ g \in G \mid g$ represented by a word in $S \}$

<u>Pf</u>: We just saw RHS $\subseteq$ LHS

Conversely, RHS contains S (as words of length 1) and is a subgp: if $g_1, g_2 \in$ RHS are represented by words w_1, w_2 then $g_1 g_2$ is represented by the concatenation $w_1 w_2$, and g_1^{-1} is represented by word $x_r^{-\epsilon_r} \cdots x_1^{-\epsilon_1}$ if $g_1 = x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$. (Recall that $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$). Also, RHS is non-empty (take empty path)

Since RHS is a subgp containing S, it contains LHS $\langle S \rangle$.

<u>Example</u>: Last time we defined $\langle g \rangle = \langle \{g\} \rangle$

<u>Examples</u> $S_n = \langle \{\text{transpositions}\} \rangle$

$A_n =$ subgp of S_n, generated by 3-cycles

$D_{2n} = \langle r, \rho \rangle$

rotation reflection

Question: Say ~~S~~ $S_G \subset G$, $S_H \subset H$ are generating sets. ~~Does~~ Can you make "$S_G \cup S_H$" generate $G \times H$.

Example: $\mathbb{Z}^2$ not free: any single element generates a copy of $\mathbb{Z}$, if $g \neq h \in S$, $\langle S \rangle = \mathbb{Z}^2$ then $gh = hg$

$\mathbb{Z} \not\to \mathbb{Z}^2$

Coset spaces

Fix a gp G, subgp H.

Define a relation on G: $g \equiv_L g' \ (H) \iff g^{-1}g' \in H \iff \exists h \in H : gh = g'$.

Lemma: This is an equivalence relation. The equivalence class of $g \in G$ is the set $gH = \{gh : h \in H\}$.

Pf: $g^{-1}g = e_G \in H$ so $g \equiv_L g \ (H)$

if $g^{-1}g' \in H$ then $(g')^{-1}g = (g^{-1}g')^{-1} \in H$ so $g' \equiv_L g \ (H)$

if $g^{-1}g' \in H$, $(g')^{-1}g'' \in H$ then $g^{-1}g'' = (g^{-1}g')((g')^{-1}g'') \in H$

so $g \equiv_L g' \ (H) \wedge g' \equiv_L g'' \ (H) \Rightarrow g \equiv_L g'' \ (H)$

~~Remarks~~ ~~Claim~~ Def: The equivalence classes are called the left cosets of H in G

Remark: The right cosets Hg are the equivalence classes of relation $g \equiv_R g' \ (H) \iff g'g^{-1} \in H$.

Def: Write G/H (say G mod H) for the coset space $G/\equiv_L(H)$

Examples $\mathbb{Z}/n\mathbb{Z}$ ($G=\mathbb{Z}$, $H=n\mathbb{Z}$ then $\equiv_L(H)$ is $\equiv(n)$)

Defs The <u>index</u> of H in G is the cardinality

$$[G:H] = \# G/H.$$

Examples $[\mathbb{Z}:n\mathbb{Z}]=n$

Index measures how far H is from G.

If G is commutative $gH=\{gh : h\in H\} = \{hg : h\in H\} = Hg$.

Thm ("Lagrange's thm") $\#G = [G:H]\cdot \#H$. (H is a subgp of G)

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

Cor If G is finite then $\#H \mid \#G$, and $[G:H] = \dfrac{\#G}{\#H}$.

Cor If G is finite, $g\in G$ of order k then $k \mid \#G$.

Pf: Let $R\subset G$ be a <u>system of coset representatives</u> for G/H: that is a set containing exactly one element from each coset.

Then the function $R\to G/H$, $r\mapsto rH$ is a bijection, $|R|=|G/H|=[G:H]$

Let $f: R\times H\to G$ be the function $f(r,h)=rh$.

f is injective: if $f(r,h)=r'h'$ we have $rh=r'h'$

then $r^{-1}r' = h\cdot(h')^{-1}\in H$ so $r\equiv_L r'\,(H)$, so $r=r'$

then $h=h'$ also ($rh=r'h'$).

f is surjective: if $g\in G$, then $\exists r\in R$: $r\equiv_L g\,(H)$

(R contains an element of each coset). Then $r^{-1}g\in H$, and $g=r(r^{-1}g) = f(r,r^{-1}g)$

Conclude that $|G| = |R\times H| = |R|\times|H| = [G:H]\cdot|H|$.

HW: If $K < H < G$, then $[G:K] = [G:H] \cdot [H:K]$

(finite case: $\frac{\#G}{\#K} = \frac{\#G}{\#H} \cdot \frac{\#H}{\#K}$)

Restate Cor: G finite, $g \in G$, order k, then $k = \#\langle g \rangle \mid \#G$.

In particular, $g^{\#G} = e$

Remark: taking inverses maps $gH \leftrightarrow Hg^{-1}$

that is a bijection $G/H \leftrightarrow H\backslash G$.

left cosets right cosets

so index is the same.

Remark: It's a thm of Philip Hall that if G is finite, G/H and $H\backslash G$ have a common system of representatives

Example: Let p be prime. Then any gp of order p is cyclic, isom to C_p

Pf: Let $g \in G \setminus \{e\}$. Order of g divides p, not 1

so order of g is p, $\langle g \rangle = G$.