Math 322, Lecture 8, 31 Oct 2017

Today: (1) Subgroups
(1) Coset spaces

Subgroups & generating sets

Lemma. The intersection of a (non-empty) family of subgroups is a subgroup.

Proof. Let \( \mathcal{H} \) be a set of subgroups of \( G \).

Let \( \mathcal{H} = \{ H \} \).
Then, \( e_G \in K \) for all \( K \in \mathcal{H} \) (they are subgroups), 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 \( xy^{-1} \in H \).

Definition. Given \( S \subset G \), the subgroup generated by \( S \) is the subgroup

\[
\langle S \rangle \overset{\text{def}}{=} \bigcap \{ H \subset G \mid S \subset H \}
\]

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

Remark. Note that \( S \subseteq \langle S \rangle \), so \( \langle S \rangle \) is the smallest subgroup containing \( S \).

Definition. A word in \( S \) is an expression

\[
\prod_{i=1}^{r} x_i = x_1 x_2 \ldots x_r
\]

where \( x_i \in S \), \( \varepsilon_i \in \{ \pm 1 \} \).
Aside: let $G$ be a p.p. S.C.G.

Set: let Cay $(G, S)$ be the graph with vertex set $G$, edge set $\{(g, gs) \mid s \in S\}$.

$S$ generates $G$ ($\langle S \rangle = G$) iff Cay $(G, S)$ is connected.

$diam(G) =$ maximum distance of two vertices

$$= \max_{g \in G} \min_{s \in S} 1w_G \left( g, ws \right)$$

Think of $S$ as "efficient" if $diam(G)$ wrt $S$ is small.

$CS: \text{diam} / |S_n| = \text{transp} \approx \log n$ (mergesort).

Open question: how large can $diam(S_n, S)$ get?

$\left( |S_n| = \log \#S_n \right)$

Conj. (Babai) $diam(S_n, S) \leq \left( \log \#S_n \right)^C$ (C fixed)

Best result (Helfgott-Seress) $\leq \exp \left( \log n \right)^4 \left( \log \log n \right)^C$
A word in \( \mathbb{N}, \mathbb{B} \) is something like: \( \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \varepsilon \).

By induction on \( n \), if \( w \) is a word in \( \mathbb{N} \) and \( \mathbb{N} \varepsilon \subset \mathbb{C} \), then \( w \varepsilon \).

Prop: \( \langle \mathbb{C} \rangle = \{ g \in G \mid g \text{ represented by a word in } \mathbb{C} \} \)

Pf: We just saw \( \text{RHS} \subset \text{LHS} \).

Conversely, \( \text{RHS} \) contains \( \mathbb{C} \) (as words of length 1) and is a subgp: if \( g_1, g_2 \in \text{RHS} \) are represented by words \( w_1, w_2 \), then \( g_1g_2 \) is represented by the concatenation \( w_1w_2 \), and \( g_1' \) is represented by word \( x_r' \cdot \ldots \cdot x_1' \) if \( g_1 = x_r \cdot \ldots \cdot x_1 \).

(Recall that \( (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} \)). Also, \( \text{RAS} \) is non-empty (take empty path).

Since \( \text{RHS} \) is a subgp containing \( \mathbb{C} \), it contains \( \text{LHS} \subset \langle \mathbb{C} \rangle \).

Example: Last time we defined \( \langle \varepsilon \rangle = \langle \varepsilon \rangle \).

Example: \( \mathbb{S}_3 = \langle \{ \text{transpositions} \} \rangle \)

\( \text{An} = \text{Subgp of } \mathbb{S}_n \), generated by 3-cycles:

\( \mathbb{D}_{2n} = \langle r, p \rangle \)

rotation, reflection.
Question: Say $S_G \subseteq G$, $S_H \subseteq H$ are generating sets. Does $G \times H$ generate $S_G \times S_H$?

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

\[ \mathbb{Z} \not\cong \mathbb{Z}^2 \]

---

**Coset space**

Fix a group $G$, a subgroup $H$.

Define a relation $g \equiv_{L} g' \ (H) \iff g'g \in H \iff \exists h \in H : gh = g'$.

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

**Proof:**
- If $g'g \in H$ then $(g')^{-1}g = (g'g)^{-1} \in H$ so $g' \equiv_L g \ (H)$
- If $g'g \in H$, $(g')^{-1}g'' \in H$ then $g'g'' = (g'g')(g'g')^{-1} \in H$

So $g \equiv L g' \ (H) \land g' \equiv L g'' \ (H) \Rightarrow g \equiv L g'' \ (H)$

**Remark:** When $H$ is normal, 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 $G/\equiv_L H$. 
Example \( \mathbb{Z}/n\mathbb{Z} \) \( (G = \mathbb{Z}, \; H = n\mathbb{Z}) \) the \( \iff \) \( (n) \mid (1) \)

Def: The index of \( H \) in \( G \) is the cardinality
\[ \left[ G : H \right] = \# G/H. \]

Example \( \left[ \mathbb{Z} : n\mathbb{Z} \right] = n \)

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") \( \# G = \# \left[ G : H \right] \cdot \# H. \) \( (H \) is a subgroup of \( G \))

\[ |G| = \left[ G : H \right] \cdot |H| \]

Cor: If \( G \) is finite then \( |H| \mid |G| \), and \( \left[ G : H \right] = \frac{|G|}{|H|}. \)

Cor: If \( G \) is finite, \( g \in G \) of order \( k \) then \( k \mid |G| \).

Pf: Let \( R \subset G \) be a system of coset representatives for \( G/H \) - that is, a set containing exactly one element from each coset.

Then the function \( R \rightarrow G/H \) is a bijection, \( |R| = |G/H| = \left[ G : H \right] \)

Let \( f : R \times H \rightarrow G \) be the function, \( f(rh) = rh. \)

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

then \( r^{-1}r' = h' (h')^{-1} \in H \) so \( r = r' \text{ (mod } H) \), so \( r = r' \)

then \( h = h' \) also \( (r\bar{h} = r'h') \).

\( f \) is surjective: if \( g \in G \), then \( \exists r \in R \) \( (R \text{ contains an element of each coset). Then } \exists ! r' \in H \) and \( g = r(r^{-1}g) \)

Conclude that \( |G| = |R| \cdot |H| = \left[ G : H \right] \cdot |H| \)

(finite case, $\#G = \#H \cdot \#K$)

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

In particular, $g^k = e$

Remark: Taking inverse maps $gH \mapsto Hg^{-1}$

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

Left cosets $\leftrightarrow$ Right cosets

so index same.

Remark: It's a theorem 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 group of order $p$

is cyclic, isomorphic to $C_p$.

For $p^2$, let $g \in G \cdot \langle e \rangle$. Order of $g$ divides $p^2$, not $p$

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