Lecture 6

Tuesday, February 3, 2015 9:58 AM

Subgroups, subgroups, subgroups!

$G \curvearrowright S$ means $G \times S \longrightarrow S$

$(g, s) \longmapsto g \cdot s$

$s \in S$, stabilizer $G_s = \{g \in G \mid g \cdot s = s\} \leq G$

$\ker(G \curvearrowright S) = \{g \in G \mid g \cdot s = s \ \forall s \in S\} \leq G.$

e.g. $G \overset{\text{conj}}{\curvearrowright} G$ via conjugation:

$g \cdot h = ghg^{-1} \in G$ for $g, h \in G$.

Property ②: $(gg') \cdot h = (gg') h (gg')^{-1}$

$= gg' h g'^{-1} g^{-1}$

$= g \cdot (g' \cdot h)$ ✓

The kernel of $G \overset{\text{conj}}{\curvearrowright} G$ is called the center of G, denote $Z(G)$.

$Z(G) = \{g \in G \mid ghg^{-1} = h \ \forall h \in G\}$

$= \{g \in G \mid gh = hg \ \forall h \in G\}$

$= \{g$ which commute w/ everything$\} \leq G.$

A fancier conjugation action:

Let $S = \mathcal{P}(G) = \{\text{subsets of } G\}$.

For $A \in S$, define $g \cdot A = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G$

This is a gp action & $G_A = \{g \in G \mid gAg^{-1} = A\}$

is called the normalizer of A, $N_G(A) \leq G$.

If $g \in N_G(A)$ then $gAg^{-1} = A$ i.e. $N_G(A) \curvearrowright A$ via conjugation: $g \in N_G(A)$, $a \in A$, $\Rightarrow gag^{-1} \in A$.

The centralizer of A in G is $C_G(A) = \ker(N_G(A) \curvearrowright A)$

$= \{g \in N_G(A) \mid gag^{-1} = a \ \forall a \in A\}$

$= \{g \in G \mid ga = ag \ \forall a \in A\} \leq N_G(A) \leq G$.

Note $Z(G) = C_G(G)$.

Subgroups generated by subsets

For $A \subseteq G$ is there a (unique) smallest subgp of G containing A?

YES.

Defn If $A \subseteq G$, define $\langle A \rangle = \bigcap_{A \subseteq H \leq G} H$ is the subgroup of G generated by A.

If we partially order $\{H \leq G \mid A \subseteq H\}$ by inclusion, then $\langle A \rangle$ is the unique minimal element!

Notation Write $\langle a_1, a_2, a_3, \ldots, a_n \rangle$ for $\langle \{a_1, \ldots, a_n\} \rangle$

also $\langle A, B \rangle$ for $\langle A \cup B \rangle$.

$\langle A \rangle$ has another description in terms of "words" in A.

$\langle$ langle $\neq <$

$\rangle$ rangle $\neq >$

Let $\bar{A} = \{ \underbrace{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}}_{\text{word in } A} \mid n \in \mathbb{N},\ a_i \in A,\ \varepsilon_i = \pm 1 \}$

Prop $\bar{A} = \langle A \rangle$. **Pf** First show $\bar{A} \leq G$. $\bar{A} \neq \emptyset$ b/c $1 \in \bar{A}$.

If $a = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$, $b = b_1^{\delta_1} \cdots b_m^{\delta_m}$, $a_i \in A$, $b_i \in A$, $\varepsilon_i, \delta_i = \pm 1$ so that $a, b \in \bar{A}$, then

$$ab^{-1} = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \cdots b_1^{-\delta_1} \in \bar{A}$$

By subgp criterion, $\bar{A} \leq G$.

Since $a = a^1$ for $a \in A$, we have $A \subseteq \bar{A}$, thus $\langle A \rangle \subseteq \bar{A}$. Now $\langle A \rangle$ is a gp containing A thus $\langle A \rangle$ contains all words in $A \Longrightarrow$ $\bar{A} \subseteq \langle A \rangle$. Thus $\bar{A} = \langle A \rangle$. □

Henceforth, we only write $\langle A \rangle$

Cyclic groups: Groups generated by a singleton set.

If $x \in G$, then $H = \langle x \rangle$ is cyclic. Note that

$$H = \{1, x, x^2, x^3, \ldots, x^{-1}, x^{-2}, x^{-3}, \ldots\}$$

$$= \{x^n \mid n \in \mathbb{Z}\}.$$

e.g. ① $\langle r \rangle \leq D_{2n}$. Then

$$\langle r \rangle = \{1, r, r^2, \ldots, r^{n-2}, r^{n-1}\}$$

Note $r^{-a} = r^{n-a}$ so we've captured inverses.

② Consider $1 \in (\mathbb{Z}, +)$.

$$\langle 1 \rangle = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \mathbb{Z} = \langle -1 \rangle.$$

Prop If $H = \langle x \rangle$, then $|H| = |x|$:

① if $|H| = n < \infty$, then $x^n = 1$ & $\{1, x, x^2, \dots, x^{n-1}\} = H$

② if $|H| = \infty$, then $x^n \neq 1$ & $x^a \neq x^b$ $\forall a \neq b \in \mathbb{Z}$.

pf Straightforward after the following observation:

if $n < \infty$ and $t = nq + r$, $0 \leq r < n$, then

$$x^t = x^{nq+r} = (x^n)^q x^r$$

$$= 1^q x^r$$

$$= x^r. \qquad \square$$

Thm Any two cyclic gps of the same order are isomorphic.

① If $n \in \mathbb{N}$, $|\langle x \rangle| = |\langle y \rangle| = n$, then $\varphi : \langle x \rangle \xrightarrow{\cong} \langle y \rangle$, $x^k \longmapsto y^k$

② if $|\langle x \rangle| = \infty$, then $\varphi : \mathbb{Z} \xrightarrow{\cong} \langle x \rangle$, $k \longmapsto x^k$

Lemma If $x \in G$, $m, n \in \mathbb{Z}$ s.t. $x^n = 1 = x^m$, then $x^d = 1$ for $d = (m, n)$. If $x^m = 1$, then $|x| \mid m$.