Lecture 7

Wednesday, February 4, 2015 9:59 AM

<u>Lemma</u> 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 $|x| \mid m$.

<u>Pf</u> By the Euclidean algorithm,

$$d = mr + ns$$

for some $r, s \in \mathbb{Z}$. Thus

$$x^d = x^{mr} x^{ns} = (x^m)^r (x^n)^s$$

$$= 1^r 1^s = 1. \qquad \blacksquare$$

<u>Thm</u> Let $H = \langle x \rangle$ be cyclic.

1. Every subgp / If $K \leq H$ is cyclic, $K = \langle x^d \rangle$ for $d = \min\{e \in \mathbb{Z}^+ \mid x^e \in K\}$.
2. If $|H| = \infty$, then $\forall a \neq b \in \mathbb{N}$, $\langle x^a \rangle \neq \langle x^b \rangle$, but $\langle x^a \rangle = \langle x^{-a} \rangle$. Thus $$\{K \leq H\} \longleftrightarrow \mathbb{N}$$
3. If $|H| = n < \infty$, then for each $a \in \mathbb{N}$ s.t. $a \mid n$, $\exists! K \leq H$ w/ $|K| = a$. Thus $\{K \leq H\} \longleftrightarrow \{a \in \mathbb{N} \mid a \mid n\}$.

<u>e.g.</u> $\mathbb{Z}_6 = \langle 1 \rangle$. Divisors of 6 are 1, 2, 3, 6.

$1, \langle 3 \rangle, \langle 2 \rangle, \langle 1 \rangle = \mathbb{Z}_6$ are the corr. subgps.

Wednesday, February 4, 2015 10:11 AM

<u>Moral</u> Cyclic gps are "easy."

If G is abelian, then again all subgps are (relatively) "easy." $\langle a_1, a_2, \ldots, a_k \rangle = \{ a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k} \mid \alpha_i \in \mathbb{Z} \}$

If $|a_i| = d_i < \infty$, then $|\langle a_1, \ldots, a_k \rangle| \leq d_1 \cdots d_k$.

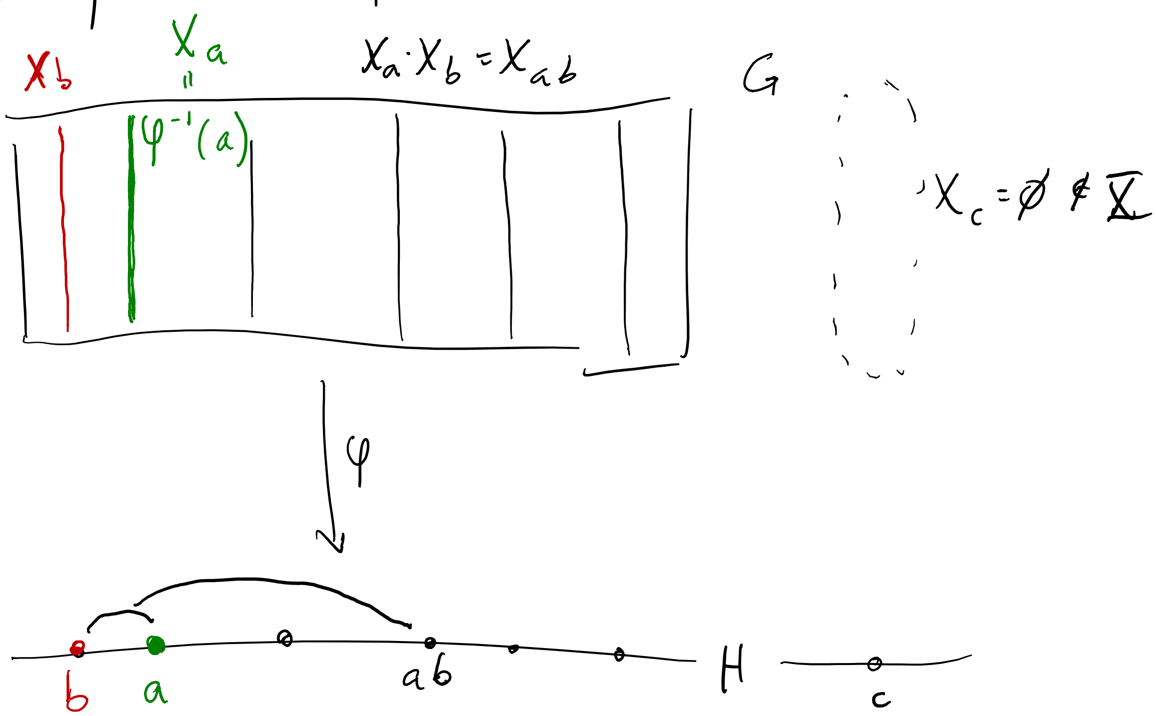
$\boxed{2}$ If G is nonabelian, $\langle a, b \rangle$ can be large and surprising!

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$$

$$|a| = |b| = 2 \text{ but } |\langle a, b \rangle| = \infty.$$

Quotients

A first pass: Suppose $\varphi : G \longrightarrow H$ a gp hom.



Let $X_a = \varphi^{-1}(a) = \{ g \in G \mid \varphi(g) = a \}$

Define $\underline{X} = \underline{X}(\varphi) = \{ X_a \mid a \in H, \ X_a \neq \emptyset \}$

Does this have a group structure? Try

$X_a, X_b \in \underline{X}$, define $X_a \cdot X_b = X_{ab}$.

Well-defined op: Must check $X_{ab} \neq \emptyset$. $g \in X_a$, $g' \in X_b$

and $\varphi(g) = a$, $\varphi(g') = b \Rightarrow \varphi(gg') = ab \Rightarrow gg' \in X_{ab} \neq \emptyset$.

Wednesday, February 4, 2015 10:25 AM

Assoc: $X_a \cdot (X_b \cdot X_c) = X_a \cdot X_{bc} = X_{a(bc)}$

$= X_{(ab)c} = X_{ab} \cdot X_c$

$= (X_a \cdot X_b) \cdot X_c$ ✓

Id: $X_1 \cdot X_a = X_{1a} = X_a = X_{a1} = X_a \cdot X_1$

$\Rightarrow X_1$ is an id if $X_1 \in \overline{X}$.

$1 \in X_1$ b/c $\varphi(1) = 1$. so $X_1 \in \overline{X}$.

Inv: $X_a \in \overline{X}$, is $X_{a^{-1}} \in \overline{X}$? If $\varphi(g) = a$ then

$\varphi(g^{-1}) = (\varphi(g))^{-1} = a^{-1}$

so $g^{-1} \in X_{a^{-1}}$.

$X_a \cdot X_{a^{-1}} = X_{aa^{-1}} = X_1 = X_{a^{-1}a} = X_{a^{-1}} X_a$.

<u>Thm</u> $\overline{X}(\varphi) \cong \mathrm{im}(\varphi)$

$X_a \longleftrightarrow \varphi(a)$

<u>Pf</u> Bijection by construction.

$$\begin{array}{ccc} X_{ab} & \longmapsto & \varphi(ab) \\ \| & & \| \\ X_a \cdot X_b & \longmapsto & \varphi(a) \cdot \varphi(b). \end{array}$$

$\square$

Avatar of the "First isomorphism theorem"!

e.g. $\mathbb{R} \xrightarrow{\varphi} S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

$\theta \longmapsto e^{2\pi i \theta}$

$$X_{e^{2\pi i\theta}} = \{ x \in \mathbb{R} \mid e^{2\pi i x} = e^{2\pi i \theta} \}$$

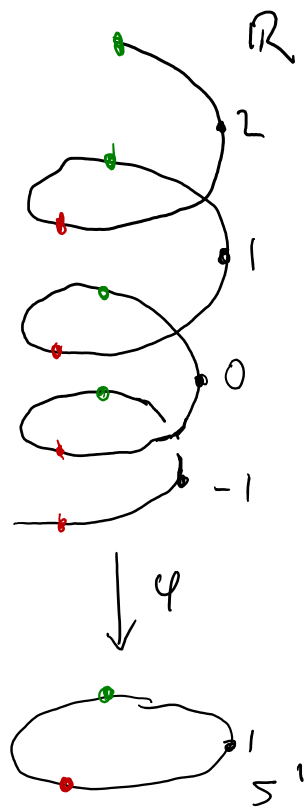
$$= \{ x \in \mathbb{R} \mid x - \theta = n \in \mathbb{Z} \}$$

$$= \{ \theta + n \mid n \in \mathbb{Z} \} = \theta + \mathbb{Z}$$

e.g.

$X_1 = \mathbb{Z} \subseteq \mathbb{R}$

Note $X_1 = \ker(\varphi)$



Defn Let $\varphi : G \to H$ be a gp hom and let $K = \ker(\varphi)$. The quotient group G/K (read "G mod K") is just $\overline{\underline{X}}(\varphi)$.

Note G/K take $K \leq G$ and collapses it into the identity elt $X_1 \in G/K$.

Wednesday, February 4, 2015 10:43 AM

Prop Let $\varphi: G \to H$ be a hom of gps w/ kernel K. Let $X \in G/K$. Then for any $u \in X$, we have

$$X = \{uk \mid k \in K\} = \{ku \mid k \in K\}.$$

⚠ This is not the same as $uk = ku$ $\forall k \in K$.

Pf Since $X \in G/K = \underline{X}(\varphi)$, $\exists a \in H$ s.t. $X = \varphi^{-1}(a) \neq \emptyset$.

For $u \in X$, $\varphi(u) = a$. Define $uK = \{uk \mid k \in K\}$.

Claim $uK \subseteq X$: $\varphi(uk) = \varphi(u)\varphi(k) = a \cdot 1 = a$. ✓

Claim $X \subseteq uK$: For $g \in X$. Want $k \in K$ s.t. $uk = g$.

Must take $k = u^{-1}g$. Then $\varphi(k) = \varphi(u^{-1})\varphi(g)$

$$= a^{-1} \cdot a = 1$$

$\Rightarrow k \in K$. ✓

Thus $X = uK$. $X = Ku$ by similar arguments. $\square$