Lecture 7: Automorphisms of groups

Last time: $G \curvearrowright G$ by conjugation. Kernel is the center:

$Z_G = \{g \in G \mid gh = hg \text{ for all } h \in G\}$

p-groups: $|G| = p^a$ $a \geq 0$, p prime [Book req's $a \geq 1$.]

Thm: $Z_G \neq \{e\}$ for any p-group with $|G| > 1$.

Thm: $|G| = p \Rightarrow G$ cyclic; $|G| = p^2 \Rightarrow G$ abelian.

[Heading towards Sylow thms about p-group subgps of arbitrary finite groups.]

Ex: $\left\{ \begin{pmatrix} 1 & a & t \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, t \in \mathbb{F}_p \right\} \leq GL_3 \mathbb{F}_p$ has order p^3 and is not abelian

---

An isomorphism $\phi: G \to G$ from a group G to itself is an automorphism. Use $\mathrm{Aut}(G)$ for the set of all such ϕ. If $\phi, \psi \in \mathrm{Aut}(G)$ so is $\phi \circ \psi$ and ϕ^{-1}! Thus $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$.

Ex: For $g \in G$, define $\mathrm{conj}_g : G \to G$, $h \mapsto ghg^{-1}$. Easy to check that this is a homom, and $\mathrm{conj}_g \circ \mathrm{conj}_{g'} = \mathrm{conj}_{(gg')}$. Thus $\mathrm{conj}_g \in \mathrm{Aut}(G)$ as inverse autom. is $\mathrm{conj}_{g^{-1}}$. Moreover, get a homom

$$\mathrm{conj} : G \longrightarrow \mathrm{Aut}(G)$$

whose image is the inner automorphisms $\mathrm{Inn}(G)$.

The kernel is Z_G since $\mathrm{conj}_g = \mathrm{id}_G \iff ghg^{-1} = h \ \forall h \iff g \in Z$.

Ex: $G = (\mathbb{Z}, +)$ Consider $\phi : \mathbb{Z} \to \mathbb{Z}$, $k \mapsto -k$.

$\phi \notin \mathrm{Inn}(G) = \{\mathrm{id}_G\}$ as G is abelian.

Ex: S_n for $n \geq 3$. Claim: $Z_{S_n} = \{e\}$

Pf: (Likely skip) For $\sigma \in Z_{S_n}$, have $(12) = \sigma (12) \sigma^{-1} = (\sigma(1)\ \sigma(2)) \Rightarrow \sigma(1) \in \{1,2\}$. Repeat with (13) $\Rightarrow \sigma(1) \in \{1,3\} \Rightarrow \sigma(1) = 1$. Continuing, see $\sigma = e$. ▨

So $\mathrm{Inn}(S_n) \cong S_n$. Fun fact: $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \geq 3$ and $n \neq 6$.

<u>Def</u>: $Out(G) := Aut(G)/_{Inn(G)}$ the outer automorphism group.

<u>Ex</u>: $Out(\mathbb{Z}) \cong C_2$

<u>Ex</u>: $Out(S_n) = \{e\}$.

<u>Ex</u>: $Out(A_n) = C_2$ for $n \geq 3$ and $n \neq 6$.

<u>Note</u>: $A_n \trianglelefteq S_n$, so get $conj: S_n \longrightarrow Aut(A_n)$ which has no kernel [basically the same reason that $Z_{S_n} = \{e\}$ except with 3-cycles]. Turns out this typically onto so $Out(A_n) \cong S_n/_{A_n} \cong C_2$.

<u>Ex</u>: $Aut(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$ where if $C_n = \langle a \mid a^n \rangle$ and $k \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $\phi_k : C_n \to C_n$, $a \mapsto a^k$ is the automorphism.

<u>Ex</u>: $Aut(\underbrace{C_p \times \cdots \times C_p}_{n}) \cong GL_n \mathbb{F}_p$.

Suppose $|G| = p^a m$ with p prime, $a \geq 1$, and $\gcd(p,m) = 1$.

A <u>Sylow</u> <u>p-subgroup</u> of G is any $P \leq G$ with $|P| = p^a$. That is, P has the <u>largest</u> <u>poss.</u> order of any p-group inside G. Set of such P is $Syl_p(G)$.

<u>Ex</u>: $C_6 = \langle a \rangle$ $\quad Syl_2(C_6) = \{\langle a^3 \rangle\}$ $\quad Syl_3(C_6) = \{\langle a^2 \rangle\}$

<u>Ex</u>: $D_6 = \langle r, s \mid r^3, s^2, (sr)^2 \rangle$

$Syl_2(D_6) = \{ \langle s \rangle, \langle rsr^{-1} = sr \rangle, \langle r^{-1} s r = sr^2 \rangle \}$

$Syl_3(D_6) = \{ \langle r \rangle \}$

<u>Thm</u>: ① $Syl_p(G) \neq \emptyset$ [Sylow p-subgps exist]

② Any two $P_1, P_2 \in Syl_p(G)$ are conjugate.

③ If $n_p = |Syl_p(G)|$, then $n_p = [G : N_G(P)]$ for any $P \in Syl_p(G)$. Moreover, $n_p \mid m$ and $n_p \equiv 1 \bmod p$.

④ Every $H \leq G$ with $|H| = p^b$ is contained in some $P \in Syl_p(G)$.

<u>Cor</u> of ①: Cauchy's Thm: If a prime $p \mid |G|$ then $\exists g \in G$ with $|g| = p$. <u>Pf</u>: Take $g \neq e$ in some $P \in Syl_p(G)$. Then $|g|$ divides $|P| = p^a$ and some g^k has order exactly p. ▨