March4

Wednesday, March 3, 2021 3:48 PM

Automorphism Groups

Recall

$G \curvearrowright A$ action. For any $g \in G$, look at

$$\sigma_g : A \longrightarrow A$$
$$a \longmapsto g \cdot a$$

σ_g bijective: $(\sigma_g)^{-1} = \sigma_{g^{-1}}$

$\rightsquigarrow \sigma_g \in S_A$

Do for all $g \in G$, get a homomorphism

$$G \longrightarrow S_A$$

called the permutation representation of $G \curvearrowright A$

Goal Study permutation rep for

$G \curvearrowright G$ by conjugation

$g * a = gag^{-1}$

Fix $g \in G$, look at

$$\sigma_g : G \longrightarrow G$$
$$\sigma_g(a) = gag^{-1}$$

Bijective function.

Lemma σ_g as above is an isomorphism

proof

Know σ_g bijective. Suffices to show its a homomorphism. Fix $a, b \in G$

$$\begin{aligned}\sigma_g(a)\sigma_g(b) &= (ga\cancel{g^{-1})(g}bg^{-1}) \\ &= g(ab)g^{-1} \\ &= \sigma_g(ab) \qquad \varnothing\end{aligned}$$

Remark This is special to conjugation action. If $G \circlearrowright G$ by left mult, $g \neq 1$ $g \in G$

$\sigma_g(1) = g \neq 1$ so σ_g not hom.

Summarize

If $G \circlearrowright G$ by conj. Get perm rep

$$\phi : G \longrightarrow S_G$$

BUT im ϕ consists of isomorphisms!!

(not just bijections)

Defn

Let G be a group. The automorphism group of G is

$$\mathrm{Aut}(G) := \{ \phi : G \to G \mid \phi \text{ is an isomorphism} \}$$

This is a grap under composition.

Note

Being an isomorphism is stronger than being a permutation.

$$\begin{array}{ccc} \mathrm{Aut}(G) & & S_G \\ \| & & \| \\ \{\phi : G \to G \mid \text{iso}\} & \subseteq & \{\phi : G \to G \mid \text{bijective}\} \end{array}$$

Prop G a grp. Then

$$\mathrm{Aut}(G) \le S_G$$

Pf/ $\phi, \psi \in \mathrm{Aut}\, G$

$\phi^{-1} \in \mathrm{Aut}(G)$ HW 3 Id

$\psi \circ \phi \in \mathrm{Aut}(G)$ HW 3 Iδ $\varnothing$

G acts on G by conjugation
Get a permutation rep.

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[dr, "\phi"'] & S_G \arrow[d, phantom, sloped, "\geq"] \\
 & \mathrm{Aut}(G)
\end{tikzcd}$$

"ϕ factors through $\mathrm{Aut}(G)$"

Goal Study this map ϕ further....

What is $\ker\phi$? $\leftarrow Z(G)$

$$\begin{aligned}
\ker\phi &= \{g \in G \mid \overset{\substack{\sigma_g \\ \shortparallel}}{\phi(g)} = id\} \\
&= \{g \in G \mid \sigma_g(a) = a \quad \forall a \in G\} \\
&= \{g \in G \mid gag^{-1} = a \quad \forall a \in G\} \\
&= Z(G)
\end{aligned}$$

By the first isomorphism theorem

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d] & \mathrm{Aut}(G) \\
G/Z(G) \arrow[ur, "\uparrow \text{injective}"'] &
\end{tikzcd}$$

i.e. $\boxed{G/Z(G) \simeq I \leq \mathrm{Aut}(G).}$

Consequences:

Corollary 1 $g, a \in G$

$$|gag^{-1}| = |a|$$

Pf/ $|gag^{-1}| = |\sigma_g(a)| \underset{\uparrow \text{HW 3 1e}}{=} |a|$ $\varnothing$

Corollary 2

Let $K \leq G$. $g \in G$.

Then ① $gKg^{-1} \leq G$.

② $K \xrightarrow{\sim} gKg^{-1}$

Proof

$gKg^{-1} = \sigma_g(K) \leq G$ (HW 5 #1)

$\rightsquigarrow K \xrightarrow{\sigma_g} gKg^{-1}$ iso $\varnothing$

Exercise $\phi : G \to H$ any isomorphism.

$K \leq G$

$\rightsquigarrow \phi(K) \leq H$ & $K \xrightarrow[\simeq]{\phi} \phi(K)$

Def^{n}

$G \circlearrowright G$ by conjugation

$$\phi : G \longrightarrow \mathrm{Aut}(G) \quad \text{perm. rep.}$$

Then the inner automorphisms of G

$$\mathrm{Inn}(G) := \mathrm{im}\,\phi \le \mathrm{Aut}(G).$$

Fact $G/Z(G) \simeq \mathrm{Inn}(G) \longleftarrow$

Examples

1) G abelian $\iff \mathrm{Inn}(G) = 1$ $\quad (gag^{-1} = a \ \ \forall g,a)$

2) D_8. $\qquad Z(D_8) = \langle r^2 \rangle$

HW 6 5c

So $\underset{\substack{\rotatebox{90}{$\in$} \\ \sigma_r}}{\mathrm{Inn}(D_8)} \simeq D_8/\langle r^2 \rangle \cong V_4$

- $\sigma_r(s) = rsr^{-1} = sr^2$
- $\sigma_r(r) = rrr^{-1} = r$

On arbitrary elts $\quad \sigma_r(r^i) = r^i$

$$\sigma_r(sr^i) = \sigma_r(s)\,\sigma_r(r^i) = sr^2r^i = sr^{i+2}$$

observe $\quad |\sigma_r| = 2$

Exercise $\quad G \circlearrowright G$ by conjugation

$\sigma_x = \sigma_y \iff xy^{-1} \in Z(G)$

③ Exercise $Z(S_n) = \{1\}$ $n \geq 3$.

$\implies S_n \simeq \mathrm{Inn}(S_n) \leq \mathrm{Aut}(S_n)$

Funny fact. This is $=$ unless $n=6$.

④ $K = \langle (1\ 2) \rangle \leq S_3$ $g = (1\ 3)$

$(1\ 3) \cdot 1 \, (1\ 3)^{-1} = 1$

$(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3)$

$gKg^{-1} = \langle (2\ 3) \rangle \leq S_3$.

Both $\langle (1\ 2) \rangle$ & $\langle (1\ 3) \rangle \simeq \mathbb{Z}_2$.

Exercise/Slight Generalization

Let $H \trianglelefteq G$. $G \curvearrowright H$ by conjugation

$g * h = ghg^{-1} \in H$. Then

①
$$\begin{tikzcd}
G \arrow[r] \arrow[dr, "\phi"'] & S_H \arrow[d, phantom, "\rotatebox{90}{$\leq$}"] \\
& \mathrm{Aut}(H)
\end{tikzcd}$$

② $\ker \phi = C_G(H)$

③ $G/C_G(H) \simeq J \leq \mathrm{Aut}(H)$

indep of G.

④ Extend this further

$$H \trianglelefteq N_G(H) \leq G$$

def. $x \in N_G(H) \Longrightarrow xHx^{-1} = H.$

Apply 1 - 3 above w/ $G = N_G(H)$ &

$$\begin{tikzcd}
N_G(H) \arrow[r] \arrow[d] & \mathrm{Aut}(H) \\
N_G(H)/C_G(H) \arrow[ur, hook] &
\end{tikzcd}$$

Application/Example of ④

Suppose $H \leq G$ & $|H| = 2$. Then $N_G(H) = C_G(H)$

Pf/ $\phi : H \xrightarrow{\sim} H = \{1, x\}$

$1 \longmapsto 1$

$x \longmapsto x$

so $\phi = id.$

$\mathrm{Aut}(H) = 1$

$$\begin{tikzcd}
N_G(H) \arrow[r] \arrow[d] & \mathrm{Aut}(H) \arrow[d, equal] \\
N_G(H)/C_G(H) \arrow[ur, hook, "inj"'] & 1
\end{tikzcd}$$

(perm rep of conjugation action)

$$\Longrightarrow N_G(H)/C_G(H) = 1 \Longrightarrow N_G(H) = C_G(H)$$

Exercise

Consequence $|H| = 2$, $H \trianglelefteq G \iff H \leq Z(G)$

Saw $\mathrm{Aut}(\mathbb{Z}_2) = 1$. Let's do some more.

Prop $\mathrm{Aut}(\mathbb{Z}_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Pf/ First observation $\mathbb{Z}_n = \langle x \rangle$. Then a map $\phi : \mathbb{Z}_n \longrightarrow H$ is determined by where it sends x.

Given $z = \mathbb{Z}_n$, $z = x^d$ so $\phi(z) = \phi(x^d)$
$= \phi(x)^d$.

Second Observation

$\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ sends x to x^a.
for $a = 0, 1, \ldots, n-1$

Then $\phi(z) = \phi(x^d) = \phi(x)^d = x^{ad} = (x^d)^a = z^a$.

All homoms $\mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ are

$$\phi_a(z) = z^a \quad \forall z \in \mathbb{Z}_n.$$

↑ call it this.

Third observation

ϕ_a isom $\Longleftrightarrow$ x^a generates $\mathbb{Z}_n$

$\Longleftrightarrow$ $\gcd(a,n)=1$.

Define

$$\begin{aligned} \Phi : (\mathbb{Z}/n\mathbb{Z})^{\times} &\longrightarrow \mathrm{Aut}(\mathbb{Z}_n) \\ a &\longmapsto \phi_a . \end{aligned}$$

① Well defined

$a \equiv b \mod n \implies x^a = x^b$ (bc $|x|=n$ & HW 2 #8c)

② Homomorphism

$\Phi(a)\Phi(b) = \phi_a \phi_b$

$\Phi(ab) = \phi_{ab}$

$$\phi_a \cdot \phi_b(z) = \phi_a(z^b) = (z^b)^a = z^{ab} = \phi_{ab}(z)$$

✓

③ Surj

$\phi_a = \Phi(a)$

④ Injective

$\phi_a(x) = x^a = x \implies a \equiv 1 \mod n$

($|x|=n$ & HW2 #6c)

Return to classification story

Done $|G| = p, p^2$. $|G| \le 7$.

Today $|G| = pq$ (some cases).

Theorem (Cauchy's Theorem for groups of order pq p, q prime).

Let $|G| = pq$ $p \neq q$ prime. Then $\exists$ $x \in G$ w/ $|x| = q$. (thus p by symmetry).

Proof

Lagrange $|Z(G)| = 1, p, q, pq$.

Lemma (*)
If $|Z(G)| = p, q, pq \implies G$ abelian.

Pf/ If $|Z(G)| = pq \implies G$ abelian.

If $|Z(G)| = p$

$$\implies |G/Z(G)| = pq/p = q.$$

$$\implies G/Z(G) \simeq \mathbb{Z}_q$$ TH 1 4a

$\Longrightarrow$ G abelian HW 6 2b $\emptyset$

If G abelian, we have Cachy's theorem for abelian groups $\Longrightarrow$ done.

Only remaining case $Z(G) = 1$

Assume that no elt of order q.

$\Rightarrow$ $\forall$ $x \in G$, $x \neq 1$

① $|x| = p$

② $x \notin Z(G)$.

③ $$\underset{\substack{\uparrow \\ p}}{\langle x \rangle} \leq \underset{\substack{\uparrow \\ ⓟ\ \text{on}\ pq}}{\underline{C_G(x)}} \underset{\substack{\uparrow \\ \text{by ②}}}{\cancel{\leq}} \underset{\substack{\uparrow \\ pq}}{G}$$

$$\langle x \rangle = C_G(x)$$

④ $$|G : C_G(x)| = pq/p = q$$

Class equation

$$\underset{\substack{\uparrow \\ pq}}{|G|} = \underset{\substack{\uparrow \\ 1}}{|Z(G)|} + \sum \underset{\substack{\uparrow \\ kq}}{\overbrace{|G : C_G(x_i)|}^{q}}$$

Says $kq + 1 = pq$ yikes! $\lightning$

Thus $\exists$ x w/ $|x| = q$

Classification

Theorem

$|G| = pq$. $p < q$. $p \nmid (q-1)$.

Then ① G abelian & ② $G \simeq \mathbb{Z}_{pq}$.

Examples

$|G| = 33 = 3 \cdot 11$ $3 \nmid 10 \rightsquigarrow G \simeq \mathbb{Z}_{33}$

$|G| = 51 = 3 \cdot 17$ $3 \nmid 16 \longrightarrow G \simeq \mathbb{Z}_{51}$

$|G| = 6 = 2 \cdot 3$ $2 \mid (3-1)$

HW 3 $G \simeq \mathbb{Z}_6$ or S_3.

Pf/ Prove ①. ② Follows same argument HW6 3d.

As before

$$|Z(G)| = 1, \underbrace{p, q, pq}_{\text{we win by Lemma } *.}$$

Reduce to case where $Z(G) = 1$

By Cauchy, $\exists$ $x \in G$ w/ $|x| = q$.

Let $H = \langle x \rangle$.

$$|G:H| = \frac{pq}{q} = p \leftarrow \text{smallest prime dividing } |G|.$$

$\Longrightarrow H \trianglelefteq G$. $H \simeq \mathbb{Z}_q$ abelian

$$\underset{q}{H} \underset{\text{Hw 4 3f}}{\le} \underset{\textcircled{q} \text{ or } pq}{C_G(H)} \le \underset{pq}{G}$$

But $C_G(H) \neq G$

bc $H \not\subseteq Z(G)$.

$\rightsquigarrow H = C_G(H)$.

$H \trianglelefteq G \rightsquigarrow G \curvearrowright H$ by conjugation

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & \mathrm{Aut}(H) \simeq (\mathbb{Z}/q\mathbb{Z})^{\times} \\
G/C_G(H) \arrow[ur] & \\
G/H \arrow[u, phantom, "\parallel"] & \\
\mathbb{Z}_p \arrow[u, phantom, "\rotatebox{90}{$\simeq$}"] &
\end{tikzcd}$$

Lagrange

$|\mathbb{Z}_p| \mid |(\mathbb{Z}/q\mathbb{Z})^{\times}|$

$p \mid (q-1)$

But $p \nmid (q-1)$. ↯

Thus $Z(G) \neq 1$. & G abelian

Upshot

Having this big normal subgroup + some numerical conditions gave us tools to use Lagrange to classify groups.

Next time Expand on this.

Exercise

$$V \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p\mathbb{Z}).$$

Then a function

$$\phi : V \longrightarrow V \text{ is a homom}$$

$\Longleftrightarrow$ it is $\mathbb{F}_p$-linear.

(1) $\phi(u+w) = \phi(u) + \phi(w)$

(2) $\phi(\lambda v) = \lambda \phi(v)$

Therefore $\mathrm{Aut}(V) \simeq GL_n(\mathbb{F}_p)$.