April1

Thursday, April 1, 2021 12:19 PM

Semidirect Products as a tool for classifying finite groups.

Def$^{\underline{n}}$ (Semidirect Products)

$H, K,\quad \phi : K \longrightarrow \mathrm{Aut}(H)$

$$H \rtimes_\phi K = \{(h, k) \mid h \in H,\ k \in K\}$$

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 (k_1 * h_2),\ k_1 k_2)$$

Theorem (Recognition)

$H, K \leq G$ &

1) $H \trianglelefteq G$
2) $H \cap K = 1$

Then $HK \simeq H \rtimes_\phi K$ where

$$\begin{aligned} \phi : K &\longrightarrow \mathrm{Aut}(H) \\ k &\longmapsto \phi(k) : H \longrightarrow H \\ & \qquad\qquad\quad h \longmapsto khk^{-1} \end{aligned}$$

Outline of general strategy

1) Use Sylow's theorem to identify

$P, Q \leq G$ & $P \trianglelefteq G$

2) Counting to show $PQ = G$

3) Lagrange to show $P \cap Q = 1$

$\Longrightarrow G \simeq P \rtimes_{\phi} Q$ ←

If we can enumerate all $\phi : Q \longrightarrow \mathrm{Aut}(P)$ we enumerated all G of this form.

Groups of order pq, $p < q$

Setup $|G| = pq$. Fix $P \in \mathrm{Syl}_p G$

$Q \in \mathrm{Syl}_q G$

Know 1) $P \simeq \mathbb{Z}_p$, $Q \simeq \mathbb{Z}_q$ TH 9 4a

2) $P \cap Q = 1$ Lagrange.

3) $|PQ| = \dfrac{|P| \cdot |Q|}{|P \cap Q|} = \dfrac{pq}{1} = |G|$

$\Longrightarrow PQ = G$.

4) $Q \trianglelefteq G$.

Pf/ $n_q = \{1, \cancel{1+q}, \cancel{1+2q}, \dots\}$

n_q divides $p < q$

So $n_q = 1 \Longrightarrow Q \trianglelefteq G$.

Recognition $\Longrightarrow$ $G = PQ \simeq Q \rtimes_\phi P$

For some $\phi : P \longrightarrow \mathrm{Aut}\, Q$

Summary

$G \simeq Z_q \rtimes_\phi Z_p$ for some

$\phi : Z_p \longrightarrow \mathrm{Aut}(Z_q) \simeq Z_{q-1}$

Reduced classification to...

Question

What are the homomorphisms

$\phi : Z_p \longrightarrow Z_{q-1}$ }

Observation

ϕ is determined by where it sends a generator. Let $Z_p = \langle x \rangle$.

HW3 1c $\quad |\phi(x)|$ divides $|x| = p$ ←

Case 1

$p \nmid q-1$ $\quad$ Then $G \simeq Z_{pq}$

Then $|\phi(x)| = 1 \Longrightarrow \phi(x) = id$

$\Longrightarrow \phi =$ trivial map.

So $\boxed{Z_q \rtimes_\phi Z_p = Z_q \times Z_p \simeq Z_{pq}}$

Case 2 $p \mid q-1$

Recall

> Feb 9 lecture showed $\exists$ unique subgroup $H \leq \mathbb{Z}_{q-1}$ of order p.
>
> Say $H = \langle \gamma \rangle$.

Lagrange $\Longrightarrow$ $\phi(x) \in H$

so $\phi(x) = \gamma^i$ $\square$

In summary, we just proved

Lemma

If $p \mid q-1$ then the maps $\mathbb{Z}_p \longrightarrow \mathbb{Z}_{q-1}$ are

$$\begin{aligned} \phi_i : \mathbb{Z}_p &\longrightarrow H \leq \mathbb{Z}_{q-1} \\ x &\longmapsto \gamma^i \end{aligned}$$

$i = 0, 1, \ldots, p-1.$

Upshot There are exactly p homomorphisms $\phi_i : \mathbb{Z}_p \xrightarrow[\uparrow]{} \mathrm{Aut}(\mathbb{Z}_q)$.

Def^n

Let $G_i := \mathbb{Z}_q \rtimes_{\phi_i} \mathbb{Z}_p$. $\leftarrow$

Consequece There are (at most) p groups of order pq w/ $p<q$ & $p \mid q-1$ (up to isomorphism).

Question Are there any repeats?

$* \; G_0 = \mathbb{Z}_q \times \mathbb{Z}_p = \mathbb{Z}_{pq}$ $\qquad \phi_0(x) = \gamma^0 = id$

$* \; G_i$ nonabelian $i \neq 0$.

Consequence If $p \mid q-1$, there are at least 2 groups of order pq.

↑ show this is sharp.

Prop If $i, j \neq 0$, $G_i \simeq G_j$

Proof

$$\begin{tikzcd} \mathbb{Z}_p \arrow[r, shift left, "\phi_i"] \arrow[r, shift right, "\phi_j"'] & \mathrm{Aut}(\mathbb{Z}_q) \end{tikzcd}$$

$$\begin{tikzcd} x \arrow[r, mapsto, shift left] \arrow[r, mapsto, shift right] & \begin{matrix}\gamma^i \\ \gamma^j\end{matrix} \end{tikzcd}$$

order p

$$\langle \gamma^j \rangle = \langle \gamma^i \rangle = \langle \gamma \rangle = H \leq \mathrm{Aut}(\mathbb{Z}_q)$$

In particular, $\exists\, k$ s.t. $\underline{\gamma^j = (\gamma^i)^k}$

Define $\psi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$

$x \longmapsto x^k$

That fits into:

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[d, "\psi"'] \arrow[dr, "\phi_j"] & \\
\mathbb{Z}_p \arrow[r, "\phi_i"] & \mathrm{Act}(\mathbb{Z}_q)
\end{tikzcd}$$

This commutes.

$$\begin{aligned}
&\phi_i(\psi(x)) \\
&= \phi_i(x^k) \\
&= (x^i)^k \\
&= x^j \\
&= \phi_j(x) \quad \checkmark
\end{aligned}$$

Define the following map.

$$\begin{tikzcd}
G_j \arrow[r, "\Phi = (id, \psi)"] \arrow[d, equal] & G_i \arrow[d, equal] \\
\mathbb{Z}_q \rtimes_{\phi_j} \mathbb{Z}_p \arrow[r] & \mathbb{Z}_q \rtimes_{\phi_i} \mathbb{Z}_p \\
(z, x^a) \arrow[r, mapsto] & (z, x^{ka})
\end{tikzcd}$$

This is an iso. Bijective: ✓.

Check it's a homomorphism.

$$\Phi\big((z, x^a)\cdot(w, x^b)\big) = \Phi\big(z\, \phi_j(x^a)(w),\ x^{a+b}\big)$$

$$= \Phi\big(z \cdot y^{ja}(w),\ x^{a+b}\big)$$

$$= \left(z \cdot \gamma^{ja}(w),\ x^{ka+kb}\right) \leftarrow$$

$$\Phi(z, x^a) \cdot \Phi(w, x^b) = (z, x^{ka})(w, x^{kb})$$

$$= \left(z\, \phi_i(x^{ka})(w),\ x^{ka+kb}\right)$$

$$= \left(z \cdot \gamma^{ika}(w),\ x^{ka+kb}\right)$$

$$= \left(z\, \gamma^{ja}(w),\ x^{ka+kb}\right). \leftarrow$$

Theorem (Classification of groups of order pq)

Let G be a group of order pq for primes p & q.

i) If $p = q$ then $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

ii) If $p < q$ & $p \nmid q-1 \implies G \simeq \mathbb{Z}_{pq}$

iii) If $p < q$ & $p \mid q-1 \implies G \simeq \mathbb{Z}_{pq}$

or $G \simeq \mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$ for

$$\phi : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$$

$$x \longmapsto \gamma$$

where $|\gamma| = p$.

In particular, $\mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$ is the unique nonabelian group of order pq.

Examples

Groups of order 6: $\mathbb{Z}_6$, S_3

Groups of order 10: $\mathbb{Z}_{10}$, D_{10}

Groups of order $2q$: $\mathbb{Z}_{2q}$, D_{2q}.
q odd prime.

Natural Question

There is a (surjective) function

$$\left\{ \begin{matrix} \text{Homomorphisms} \\ \phi : K \longrightarrow \operatorname{Aut} H \end{matrix} \right\} \xrightarrow[\text{construction}]{\text{semidirect}} \left\{ \begin{matrix} \text{Groups of form} \\ H \rtimes_\phi K \end{matrix} \right\} \Big/ \text{up to iso.}$$

Not bijective in general.

Example $p \mid q-1$

$$\left\{ \begin{matrix} \text{Maps} \\ \mathbb{Z}_p \longrightarrow \operatorname{Aut}(\mathbb{Z}_q) \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{Groups} \\ \mathbb{Z}_q \rtimes \mathbb{Z}_p \end{matrix} \right\} \Big/ \text{up to iso.}$$

↑ p of these

↑ 2 of these.

Question

Suppose $\phi, \psi : K \longrightarrow \operatorname{Aut} H$

when is $H \rtimes_\phi K \simeq H \rtimes_\psi K$??

Let's give a partial answer modelling off of the proof we just saw.

Lemma 0

Let $\phi, \psi : K \longrightarrow \operatorname{Aut} H$. Suppose $\exists\ \gamma \in \operatorname{Aut} K$, s.t.

$$\begin{tikzcd} K \arrow[rd, "\phi"] \arrow[d, "\gamma"'] & \\ K \arrow[r, "\psi"] & \operatorname{Aut} H \end{tikzcd}$$

$\psi \circ \gamma = \phi$

Then
$$\begin{tikzcd} H \rtimes_\phi K \arrow[r, "{(id, \gamma)}"] & H \rtimes_\psi K \\ (h, k) \arrow[r, mapsto] & (h, \gamma(k)) \end{tikzcd}$$

is an isomorphism.

Pf/HW. Model off of G_i situation.

Groups of order 12

Know of 5 groups of order 12.

$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$

A_4, D_{12}, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$

↑ inversion extension.

Theorem

These are all of them. $|G| = 12 = 2^2 \cdot 3$

Pf/ $P \in Syl_2(G)$, $Q \in Syl_3(G)$

HW8 #3B showed $Q \ntrianglelefteq G \implies \boxed{G \simeq A_4}$

We can therefore assume $Q \trianglelefteq G$.

- $P \cap Q = 1$ LG
- $PQ = G$ counting.

$\implies G \simeq Q \rtimes P$

TH1
4

Know $|P| = 4 \rightsquigarrow P \simeq \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$

$|Q| = 3 \longrightarrow Q \simeq \mathbb{Z}_3$

Case 1 $P \simeq \mathbb{Z}_4$

$$G \simeq \mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_4$$

Classify maps

$$\phi : \underset{\langle x \rangle}{\overset{\shortparallel}{\mathbb{Z}_4}} \longrightarrow \underset{\{id,\ \iota\}}{\overset{\shortparallel}{Aut(\mathbb{Z}_3)}}$$

inversion

$$x \xmapsto{\phi_1} id \rightsquigarrow G \simeq \mathbb{Z}_3 \rtimes_{\phi_1} \mathbb{Z}_4$$

$$\simeq \mathbb{Z}_3 \times \mathbb{Z}_4 = \boxed{\mathbb{Z}_{12}}$$

$\rightarrow x \xmapsto{\phi_2} i$

Then $\mathbb{Z}_3 \rtimes_{\phi_2} \mathbb{Z}_4 = \boxed{\mathbb{Z}_3 \rtimes \mathbb{Z}_4}$

$\uparrow$ inversion extension

Case 2 $P \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a \rangle \times \langle b \rangle$

$$G \simeq \mathbb{Z}_3 \rtimes_{\phi} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

Maps

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_3) = \{1, \iota\}$$

$$(a, b) \longmapsto \{id, \iota\}$$

2a Both go to identity.

$$\rightarrow G \simeq \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \boxed{\mathbb{Z}_6 \times \mathbb{Z}_2}$$

2b 3 maps left

ϕ_1	ϕ_2	ϕ_3
$a \mapsto \iota$	$a \mapsto \iota$	$a \mapsto id$
$b \mapsto \iota$	$b \mapsto id$	$b \mapsto \iota$

$\phi_1 \leftrightarrow \phi_2$: $\gamma(a) = ab$, $\gamma(b) = b$

$\phi_2 \leftrightarrow \phi_3$: $\gamma(a) = b$, $\gamma(b) = a$

$\forall\ i, j$

$$\begin{tikzcd}
Z_2\times Z_2 \arrow[dr, "\phi_i"] \arrow[dd, "\gamma"] & \\
& \mathrm{Aut}\, Z_3 \\
Z_2\times Z_2 \arrow[ur, "\phi_j"'] &
\end{tikzcd}
\quad \Rightarrow \quad
\begin{tikzcd}
Z_3 \rtimes_{\phi_i} (Z_2\times Z_2) \arrow[d, phantom, "\cong"] \\
Z_3 \rtimes_{\phi_j} (Z_2\times Z_2)
\end{tikzcd}$$

Lemma 0

Only one group order 12 left, must be $\boxed{D_{12} \simeq Z_3 \rtimes_{\phi_i} (Z_2\times Z_2)}$

Groups of order 30

Setup w/ some lemmata. All exercises

Lemma 1

Let H, K be groups of coprime order. Then

$$\mathrm{Aut}(H\times K) \simeq \mathrm{Aut}(H)\times \mathrm{Aut}(K).$$

Lemma 2 H, K, L 3 groups.

Let $\phi: K \longrightarrow \mathrm{Aut}(H)$

$K \circlearrowright L$ trivially.

Define an action $K \circlearrowright (L\times H)$ $*$

$$k\cdot(\ell, h) = (\ell, kh).$$

Then this is an action by automorphisms

$$(L\times H)\rtimes_* K \xrightarrow{\ \sim\ } L\times(H\rtimes_\phi K)$$

$$((\ell, h), k) \longmapsto (\ell, (h, k))$$

is an isomorphism.

Lemma 3 (Last Time).

$$\begin{tikzcd} \mathbb{Z}_2 \arrow[r] & \mathrm{Aut}(\mathbb{Z}_n) \\ x \arrow[r, mapsto] & \iota \end{tikzcd}$$

Then $\mathbb{Z}_n \rtimes \mathbb{Z}_2 \simeq D_{2n}$.

Let $|G| = 30$. Know.

① (March 11) $\exists\ H \trianglelefteq G$ w/ $H \simeq \mathbb{Z}_{15}$

② (Cauchy) $\exists\ K \leq G$ $|K| = 2$.

③ (Lagrange) $H \cap K = 1$

④ (counting). $HK = G$

Therefore $G \simeq \mathbb{Z}_{15} \rtimes_{\phi} \mathbb{Z}_2$

Classify all maps

$$\phi : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_{15}).$$

Observe

$$\mathrm{Aut}(\mathbb{Z}_{15}) \simeq \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_5)$$

$$\overset{L1}{\simeq} \mathrm{Aut}(\mathbb{Z}_3) \times \mathrm{Aut}(\mathbb{Z}_5)$$

$$\simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}).$$

Maps

$$\phi : Z_2 \longrightarrow (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$$

$$x \longmapsto (a, b)$$

↑ double to 0.

4 of them

1) $\phi_1(x) = (0, 0)$

2) $\phi_2(x) = (1, 0)$

3) $\phi_3(x) = (0, 2)$

4) $\phi_4(x) = (1, 2)$.

What are the actions on $(y, z) \in Z_3 \times Z_5$

ϕ_1 Trivial action.

$$\boxed{Z_{15} \rtimes_{\phi_1} Z_2 \simeq Z_{15} \times Z_2 \simeq Z_{30}}$$

ϕ_2 $(1, 0) = (\iota, id)$

↑ element of order 2 in Aut Z_3

$$x \cdot (y, z) = (y^{-1}, z)$$

ϕ_3 $(0, 2) = (id, \iota)$

↑ order 2 in aut Z_5

$$x \cdot (y, z) = (y, z^{-1})$$

ϕ_4 $(1, 2) = (\iota, \iota)$ $\quad x \cdot (y, z) = (y^{-1}, z^{-1})$

⇝ Action of x on Z_{15}

is inversion.

i.e. $\phi_4 : \mathbb{Z}_2 \longrightarrow Act(\mathbb{Z}_{15})$

$x \longmapsto c$

$$\Longrightarrow \boxed{\mathbb{Z}_{15} \underset{\substack{\uparrow \\ \text{inversion}}}{\rtimes_{\phi_4}} \mathbb{Z}_2 \underset{\substack{\uparrow \\ L3}}{\simeq} D_{30}}$$

Comput for $\phi_2 : x \longmapsto (c, id)$ trivial

$$(\mathbb{Z}_3 \times \mathbb{Z}_5) \rtimes_{\phi_2} \mathbb{Z}_2 = (\mathbb{Z}_5 \times \mathbb{Z}_3) \rtimes_{\phi_2} \mathbb{Z}_2$$

$$\overset{L2}{\simeq} \mathbb{Z}_5 \times \underline{(\mathbb{Z}_3 \rtimes_i \mathbb{Z}_2)}$$

$$\overset{L3}{\simeq} \boxed{\mathbb{Z}_5 \times D_6}$$

Compute for $\phi_3 : x \longmapsto (id, c)$.

$$(\mathbb{Z}_3 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_2 \overset{L2}{\cong} \mathbb{Z}_3 \times (\mathbb{Z}_5 \rtimes_i \mathbb{Z}_2)$$

$$\overset{L3}{\simeq} \boxed{\mathbb{Z}_3 \times D_{10}.}$$

These are all distinct.

HW n odd $Z(D_{2n}) = 1 \leftleftarrows$

* $|Z(\mathbb{Z}_{30})| = 30 \longleftarrow$

* $|Z(D_{30})| = 1$

HW 7 or 8

* $|Z(Z_5 \times D_6)| = |Z(Z_5) \times Z(D_6)|$

$$= |Z(Z_5)| \cdot |Z(D_6)|$$

$$= 5$$

* $|Z(Z_3 \times D_{10})| = |Z(Z_3)| \times |Z(D_{10})|$

$$= 3$$

All groups are nonisomorphic!

Theorem The groups of order 30 are precisely (up to iso)

- Z_{30}
- D_{30}
- $Z_5 \times D_6$
- $Z_3 \times D_{10}$