Recall

Last time — Finished proof of Sylow theorems.
Simplicity of A_n $n \geq 5$.

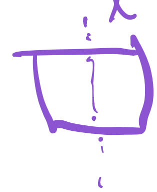
Example: Groups of order 15.

Talk about generalizing to groups of order pq.

Today: semidirect products.

a tool for building new groups out of old groups.

Example: D_8 symmetries of the square.



$$\mathbb{Z}/4\mathbb{Z} \trianglelefteq D_8$$

rotations

$\langle s \rangle$ $\quad$ $k \leftrightarrow$ rotation by $k\frac{\pi}{2}$.

$s =$ rotation by $\frac{\pi}{2}$. $\quad$ $r_\ell =$ reflection along ℓ.

$$\langle r_\ell \rangle = \mathbb{Z}/2\mathbb{Z} \leq D_8$$

$$\langle s \rangle \langle r_\ell \rangle = D_8$$

we know $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

(when H is normal $[HK : H] = [K : H \cap K]$,
$HK/H \cong K/H \cap K$.)

We can get every element of the group by multiplying elements in $\mathbb{Z}/4\mathbb{Z}$ & $\mathbb{Z}/2\mathbb{Z}$

i.e. there is a bijection of <u>sets</u>.

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to D_8$$

$$k, \quad j \mapsto r^k s^j.$$

<u>Not</u> a group isomorphism.

<u>Semidirect product</u>: change the group law on the <u>set</u> $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

so that this becomes a group isomorphism

$$(k, j) * (k', j') \leftrightarrow s^k r^j s^{k'} r^{j'}$$

$$r^j s^{k'}$$

$$= r^j s^{k'} r^{-j} r^j$$

$$= s^{(-1)^j k'} r^j$$

$$s^{k} s^{(-1)^j k'} r^{j} r^{j'}$$

conjugation of rotation by reflection

$$(k, j) * (k', j') = (k + (-1)^j k', j + j').$$

"twisted multiplication".

The example says $D_8 \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$

$\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$

$1 \mapsto$ multiplication by -1.

Definition/Theorem:

If H and K are groups and $\phi : K \to \mathrm{Aut}_{group}(H)$.

then $H \rtimes_\phi K$ is the set

$H \times K$ equipped with multiplication

$$(h_1, k_1) *_\phi (h_2, k_2) = (h_1\, \phi(k_1)(h_2), k_1 k_2).$$

This defines a group, and

$H \to H \rtimes_\phi K$
$h \mapsto (h, 0)$
identifies H with a normal subgroup of $H \rtimes_\phi K$.

$K \to H \rtimes_\phi K$
$k \mapsto (0, k)$
identifies K w/ a subgroup.

s.t. $\quad khk^{-1} = \phi(k)(h)$

$$(0,k) *_\phi (h,0) *_\phi (0,k^{-1}) = (\phi(k)(h), 0).$$

Example: $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$

D_{2n}: symmetries of regular n-gon

$\mathbb{Z}/2\mathbb{Z}$: a reflection.

Exercise: what is ϕ?

Example For any group H,

$$H \rtimes_{Id.} \mathrm{Aut}(H).$$

Recognition principle: If G is a group,

$H \leq G \qquad K \leq N_G(H)$

then HK is a subgroup of G

and if $H \cap K = \{e\}$, then the map

$$(h,k) \mapsto hk$$

is a group isomorphism

$$H \rtimes_\phi K \to HK$$

$$\left(\phi : K \hookrightarrow N_G(H) \xrightarrow{conj} \mathrm{Aut}(H)\right).$$

(Usually use this when $HK = G$ in which case $H \trianglelefteq G$).

Groups of order pq For $p > q$ prime:

Suppose G has order pq.

$n_p \equiv 1 \mod p \qquad n_p \mid q.$

$n_p = 1, p+1, 2p+1, \ldots$

$\mathbb{Z}/p\mathbb{Z}$

so $n_p = 1$. so let $H \trianglelefteq G$
$|H| = p$.

By cauchy $\exists$ a subgroup of order q. $K \cong \mathbb{Z}/q\mathbb{Z}$.

$H \cap K = \{e\}$.

$|HK| = pq$

so $HK = G$.

Recognition principle: $G \cong H \rtimes K$
$\cong \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/q\mathbb{Z}$.

$\phi : \mathbb{Z}/q\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/p\mathbb{Z})$

If $q \nmid p-1$ the only map ϕ is trivial

$\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

If $q \mid p-1$ then there is a unique cyclic subgroup of order q in $\mathbb{Z}/(p-1)\mathbb{Z}$.

There will be $q-1$ non-trivial ϕ.

$\mathbb{Z}/q\mathbb{Z} \xhookrightarrow{\phi_0} \mathbb{Z}/(p-1)\mathbb{Z}$

precompose w/ automorphism of $\mathbb{Z}/q\mathbb{Z}$ to get more.

<u>Exercise</u> check this + they also give isomorphic groups.

Important: often $\phi_1 \neq \phi_2$
but $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$

<u>Conclusion</u> If $q \nmid p-1$

then $\mathbb{Z}/pq\mathbb{Z}$ is the only group of order pq.

& otherwise there is $\mathbb{Z}/pq\mathbb{Z}$ & one nonabelian group of order pq

(up to isomorphism).