Algebra I Lecture 10:

Check out §5.3 for table of some small gps.

Recognizing direct products:

<u>Find</u> gps <u>internally</u> in G. (e.g. Sylow subgps) which build it up. (One HW ex. was <u>similar</u>, quotients of $H \cap K$)

<u>Prelim</u>:

$[x,y] = x^{-1}y^{-1}xy$ = <u>commutator</u> of x, y. ← used last time.

$[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$, gp. of commutators for <u>subsets</u> $\emptyset \neq A, B \subseteq G$.

$G' = [G,G]$ comm. subgp. (notation: <u>Derived</u> series)

<u>Prop</u>: $x, y \in G$, $H \leq G$.

1). $xy = yx[x,y]$. (e.g: $xy = yx \Leftrightarrow [x,y] = 1$)

2). $H \trianglelefteq G \Leftrightarrow [H,G] \leq H$.

3). $\sigma[x,y] = [\sigma(x), \sigma(y)]$ $\forall$ <u>Aut</u>. σ (Aut means Isom. $G \to G$) (may use later)

4). G/G' ab. (we <u>saw</u> the <u>largest</u> abelian <u>quotient</u>) <u>the abelianization</u>)

<u>Pf</u>: 1). Clear...

2). $H \trianglelefteq G \Leftrightarrow g^{-1}hg \in H$ $\forall g \in G, h \in H \Leftrightarrow h^{-1}g^{-1}hg \in H$

So $H \trianglelefteq G \Leftrightarrow [h,g] \in H$ $\forall h, g \Leftrightarrow [H,G] \leq H$ (follow your nose)

3). $\sigma \in \mathrm{Aut}(G)$, $x, y \in G$.

$$\sigma([x,y]) = \sigma(x^{-1}y^{-1}xy) = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y)$$

$$= [\sigma(x), \sigma(y)].$$

4). We saw before: G/H ab $\iff gHg'H = g'HgH \ \forall g,g'$
$\iff gg'H = g'gH \iff g^{-1}g'^{-1}gg' \in H \iff [g,g'] \in H \ \forall g,g' \in G$
$\iff [G,G] = G' \subseteq H$.

This shows why G/G' is the <u>largest</u> ab. quotient.

(!) $\exists$ grps with elts of G' that are <u>not</u> commutators $[x,y]$ (but <u>products</u> of them).

<u>Ex</u>: $G = D_{2n}$

$$[r,s] = r^{-1}s^{-1}rs = r^{-1}srs = r^{-2}s^2 = r^{-2}.$$

Thus, $D_{2n}' \geq \langle r^{-2}\rangle = \langle r^2\rangle$.

$\langle r^2\rangle \trianglelefteq D_{2n}$ as elts in $\langle r\rangle$ commute w/ elts. in $\langle r^2\rangle$
and $s r^2 s^{-1} = s r^2 s = r^{-2} \in \langle r^2\rangle$.

$D_{2n}/\langle r^2\rangle$
generators: $r\langle r^2\rangle, s\langle r^2\rangle$ } (Because and [illegible])

$$r\langle r^2\rangle s\langle r^2\rangle = rs\langle r^2\rangle = sr^{-1}\langle r^2\rangle = sr\langle r^2\rangle = s\langle r^2\rangle r\langle r^2\rangle$$

$\Rightarrow D_{2n}/\langle r^2\rangle$ abelian (it must be Klein Vier as r,s have order 2)

$\Longrightarrow D_{2n}' \leq \langle r^2\rangle \Rightarrow D_{2n}' = \langle r^2\rangle$.

n ~~even~~ odd $\iff \langle r^2\rangle = \langle r\rangle$, n even $\iff [\langle r\rangle : \langle r^2\rangle] = 2$.

So D_{2n}' has index $\begin{cases} 2 & n \text{ odd} \\ 4 & n \text{ even.} \end{cases}$

<u>Theorem (Recognition).</u> $H, K \trianglelefteq G$.

1) ~~$H,K \trianglelefteq G$~~ Then $H \cap K = 1 \Longrightarrow HK \cong H \times K$.

Pf: $H, K \trianglelefteq G \Rightarrow HK \leq G$.

The same pf. as in the Lemma on Sylow theory shows since $H \cap K = 1$, elts of H commute w/ elts of K.

Same ~~proof~~ Now idea as in Sylow theory:

$\varphi: H \times K \to HK$
$(h,k) \mapsto hk$. (just write again...)

hom: $(h,k)(h',k') \mapsto hkh'k' = hh'kk' = (hh', kk')$ —

Now the # of ways of writing each elt of HK as hk, $h \in H$, $k \in K$, is $|H \cap K|$ (exercise). (doubly of independent interest)

Or more (essentially) simply, $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = |H \times K|$

and φ onto by def $\Rightarrow HK \cong H \times K$ ∎.

Def: HK here is the internal direct prod.
$H \times K$ is called the external direct prod. } no real difference

Ex: n odd. Consider $D_{4n} = G$

$H = \langle r^2, s \rangle$ (saw before)
$K = \langle r^n \rangle$ ~~order~~ size 2.

Now let $r_1 := r^2$, so $s^2 = 1$, $r_1^n = 1$. (smallest power)
$r_1 s = r^2 s = s r^{-2} = s r_1^{-1}$ rels.

So $H \cong D_{2n}$ and has size $2n$ in particular.

Thus, $[G : H] = 2 \Rightarrow H \trianglelefteq G$.

elts of r centralizes elts of K $(r r^n r^{-1} = r^n)$

and $s r^n s = r^{-n} \in K \Rightarrow K \trianglelefteq G$. Lagrange ($|K|$ = prime) $H \cap K = 1$

$K \not\leq H$ as can't get r^n from r^2, s, as n is odd. $\Rightarrow$ Lag. $\Rightarrow D_{4n} \cong D_{2n} \times \mathbb{Z}/2\mathbb{Z}$

Read examples in book about S_n. **

Emails
Massachusetts UT. Seminar

Semi-direct products ~~Recognition~~:

$HK = G,\ H, K \trianglelefteq G,\ H \cap K = 1 \Rightarrow G \cong H \times K.$

What ~~if~~ if K is not normal, but H is, and $H \cap K = 1$ (still)

Then HK is still a gp., and elts. are products hk ~~are~~ with unique expressions still.

Recall the pf. that $HK \leq G$:

$$(h_1 k_1)(h_2 k_2) = h_1 k_1 h_2 (k_1^{-1} k_1) k_2$$
$$= h_1 \underbrace{(k_1 h_2 k_1^{-1})}_{\in H} \underbrace{k_1 k_2}_{\in K}$$
$$= h_3 k_3$$

$$\left.\begin{array}{l} h_3 = h_1 (k_1 h_2 k_1^{-1}) \\ k_3 = k_1 k_2. \end{array}\right\} (*)$$

unrelated

Idea! Start @ 2 gps. H, K and define a gp G.
using $(*)$ so that $H, K \leq G$, $H \cap K = 1$, $G = HK$, $H \trianglelefteq G$.

Q: What does conjugation mean for unrelated gps?
That is, how do we define $k_1 h_2 k_1^{-1}$?
Conjugation is an automorphism. Can use other automorphisms.

Restart here

Need: hom $\varphi : K \to \mathrm{Aut}(H)$.

No HW Next week... EXAM!!

Thm H, K gps. $\varphi : K \to \mathrm{Aut}(H)$ hom.

set $k \cdot h = \varphi(k)(h)$ (~~acts~~ (action))

Set $H \rtimes_\varphi K = \{(h,k) \mid h \in H, k \in K\}$. ① g operation

Modified Recently then for X.

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

~~twist~~ ~~"twist"~~ h_2 by k_1.
(4) "twist"

$\underline{\text{Thm}}$: 1). G is a gp.

2). $H \cong \{(h,1) \mid h \in H\}$, $K \cong \{(1,k) \mid k \in K\}$

3). $H \trianglelefteq G$, $G/H \cong K$.

4). $HK = G$, $H \cap K = 1$.

5). $\forall h \in H, k \in K$, $k \cdot h = khk^{-1}$ in G.

Pf: Mostly straightforward exercises. (We check some)

Recall

- $H, K \leq G$: (embed $\&$ identify). (we're checking (2)).

point: $1 \cdot h = h$ $\forall h \in H$. and $\boxed{k \cdot 1 = 1}$ $\forall k \in K$ *

([redacted] gp. action) Special

$\boxed{k \cdot 1 = \text{automorph } (1) = 1.}$

$\Rightarrow (h_1, 1) \cdot (h_2, 1)$

$= (h_1 1 \cdot h_2, 1 \cdot 1) = (h_1 h_2, 1)$.

$(1, k_1) \cdot (1, k_2) = (1 k_1 \cdot 1, k_1 k_2) = (1, k_1 k_2)$ ← still works on this component in this way...

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

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

$= (k \cdot h, 1) \Rightarrow \underbrace{k \cdot h}_{= \varphi(k)(h) \in H} = khk^{-1}$ in G.

to here

- $H \trianglelefteq G$: Previous Calc $\Rightarrow K \leq N_G(H)$.

Since $G = HK$ and $H \leq N_G(H)$, we have $N_G(H) = G$

$\boxed{\text{Rest} = \text{exercise.}}$ $\Rightarrow H \trianglelefteq G$ ▪

Start here

The gp. G is called the semidirect product of H, K (w.r.t. φ). Written: $H \rtimes_\varphi K$ or $H \rtimes K$ when φ is clear.

↑ reminds us:

1). $H \trianglelefteq G$.

2). not symmetric. (unlike $\times$)

3). kind of like $\times$.

Prop: TFAE:

1). $H \rtimes K \cong H \times K$.
2). $K \trianglelefteq H \rtimes K$.
3). $\varphi : K \to \mathrm{Aut}(H)$ is trivial.

Pf: (see Prop. 11 in book; omitted).
So this generalizes $H \times K$.

Thm (Recognition theorem for $\rtimes$).

$H, K \leq G$, $H \trianglelefteq G$, $\underbrace{HK = G,\ H \cap K = 1}_{\text{Def}^{\underline{n}}\ K \text{ is a complement of } H}$.

Then $G = H \rtimes_\varphi K$, $\varphi =$ conj. hom: $K \to \mathrm{Aut}(H)$.

Pf (Sketch)

Since HK, ~~$H\rtimes$~~ $H \rtimes_\varphi K$ are in bijective corr. via ~~[illegible]~~
$hk \longmapsto (h, k)$ (uniqueness due to $H \cap K = 1$). Saw.

just have to check this is a homomorphism.

This is the same calculation we did when defining semidirect prods.

Examples: H, K gps. $\varphi : K \to \mathrm{Aut}(H)$

1). H abelian, $K = \langle x \rangle \cong \mathbb{Z}/2\mathbb{Z}$ ~~the gp. of order 2~~.

$\varphi : K \to \mathrm{Aut}(H)$ | Pause here (H abelian $\Rightarrow a^{-1}b^{-1} = b^{-1}a^{-1} = (ab)^{-1} \Rightarrow (\cdot)^{-1}$ is an automorphism)

$x \cdot h = h^{-1}$ $\forall h \in H$.

$1 \cdot h = h$

Then $G = H \rtimes_\varphi K$ has H of index 2, so nml. and

$x h x^{-1} = h^{-1}$ $\forall h$.

$\uparrow$ conj. is $\cdot$ in $H \rtimes K$ [rel'ns on r, s]

If H is $\mathbb{Z}/n\mathbb{Z}$, $G \cong D_{2n}$. If $H = \mathbb{Z}$, G is D_∞ the infinite dihedral gp

2). G gp. of order pq, $p < q$. $H = \mathbb{Z}/q\mathbb{Z}$, $K = \mathbb{Z}/p\mathbb{Z}$. (Sylow; H has index p = smallest prime $\Rightarrow$ normal)

$p \nmid q-1 \Rightarrow G$ cyclic

As $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \boxed{(\mathbb{Z}/q\mathbb{Z})^\times} \cong (\mathbb{Z}/(q-1)\mathbb{Z})$, so every hom $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ is trivial. (image = 1). (in a hom $|\varphi(x)| \mid |x|$)

$\boxed{a \mapsto (x \mapsto xa)}$ $(6)\ 6 = 2 \times 7$

primitive elt. mod n in gp of units

If $p \mid (q-1)$, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$

Cauchy $\Rightarrow$ $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ has a subgp. of order p.

(unique as $\mathrm{Aut}(\mathbb{Z}_q)$ cyclic) (my p. generated, $\mathbb{Z}_{q}$ to this)

So there is a non-trivial hom $\varphi : K \to \mathrm{Aut}(H)$.

Let $G = H \rtimes K$. Then $|G| = pq$, K is not normal in G as $\varphi \neq 1$. (by our earlier Prop.)

$\Rightarrow$ G is non-abelian

(Note: if $p=2$, then $G \cong D_{2q}$.) saw before.

Uniqueness: JNS. semi-dir. do anything.

(Do next time: Classification theorem)

Corresponds to composing w/ aut. of $\mathrm{Aut}(H)$

$\varphi, \varphi' : \mathbb{Z}_p \to \mathbb{Z}/(q-1)\mathbb{Z}$

$\varphi : x \mapsto a$

$\varphi' : x \mapsto b$ Say $b = a^n$

then

$\exists!$ subgp of order p. (cyclic gp)

$n_p \equiv 1 \mod p$

$n_p \mid q$

$K \to \mathrm{Aut}\, H$.

$\varphi = \psi \circ \varphi'$

$\varphi(x^3) = \varphi(x^2)\varphi(x) = \varphi(x^2)\varphi(x)$

$\psi \circ \varphi' : K \to K \to \mathrm{Aut}\, H$.

ψ: map $x \mapsto x^n \neq id$

$\psi^n = u$

We have explained this now

~~Given a non-~~

If $\varphi = id$,

then $G \cong H \times K \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/(pq\mathbb{Z})$

If $\varphi, \varphi' \neq id$,

$\mathrm{Aut}(H) \cong (\mathbb{Z}/(q-1)\mathbb{Z})$

$\psi = \varphi(\varphi')^{-1} \in \mathrm{Aut}(H)$.

so $\boxed{\varphi = \psi \circ \varphi'}$

$\mathrm{Aut}(K)$ BE $\mathrm{Aut}(H)$.

HW: $H \rtimes_\varphi K \cong H \rtimes_{\varphi \circ \beta} K$

By HW, they give the same gp.

next lect. theory: resolve such gps

Burnside: $|G| = p^a q^b \Rightarrow G$ is solvable

Feit-Thompson: $|G|$ odd $\Rightarrow G$ solvable

So gps of orders:

$p \to 1$ cyclic

$p^2 \to 1$ cyclic, 1 abelian $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$, all abelian

$pq \to 1$ cyclic, 1 non-abelian $\mathbb{Z}/p \rtimes \mathbb{Z}_q \cong D_{2p}$ if $p=2, q \neq p$. if $p \mid q-1$

- no non-cyclic if $p \nmid q-1$

$p^2q \to$ 1 cyclic, 2 abelian: $\mathbb{Z}_{p^2} \times \mathbb{Z}_q \cong \mathbb{Z}_{p^2q}$ or $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$. $p \nmid q-1$.

$p \mid (q-1)$: P Sylow P normal.

Case: $P \cong \mathbb{Z}_{p^2} \to$ aut cyclic of order $p(p-1)$ $\mathbb{Z}/p\mathbb{Z}$ $\to$ conj. classes in $\mathbb{Z}/p\mathbb{Z}$ $\to$ aut. classes

(7)