Algebra I - Lecture 9: Applications of Sylow Theory / Direct Products

- Ask about HW.
- 2 Exam changed dates
- ~~Counts pf.~~

Recall: Start by writing this $|G|<\infty$

Sylow Thms: $p \mid |G|$ prime, $p^k \| |G|$.

I: $Syl_p(G) \neq \emptyset$.

II: $P, Q \in Syl_p(G) \Rightarrow P, Q$ conjugate in G.

III $n_p := |Syl_p(G)|$.
$n_p \equiv 1 \mod p$. $n_p \mid (|G|/p^k)$ Very constraining!

III* $n_p = [G : N_G(P)]$, $P \in Syl_p(G)$.

All the gp. actions come together in one intricate tower.

Now, get to do fun applications.

Ex: $G = A_4$, $|G| = 12 = 2^2 \cdot 3$

$p=3$: elts of order 3: 3 cycles are all even, $\frac{4\cdot 3\cdot 2}{3} = 8$ 3-cycles, pair up σ, σ^2. $\Rightarrow n_3 = 4$.

Explicitly: $\Rightarrow Syl_3(A_4) = \{(1, (123), (132)), (1, (124), (142)),$
$(1, (134), (143)), (1, (234), (243))\}$.

check: $n_3 \equiv 1 \ (3)$ ✓
$n_3 \mid 4$ ✓

All conjugate: We saw: same cycle type $\Leftrightarrow$ conj. in S_n

Not enough in A_n, but try same idea from pf.

~~Show all~~ Take generator $(123) = \sigma$. try to conj. to other generators (in S_n)

$\tau\sigma\tau^{-1} = \sigma'$

(123)(4)	(123)(4)	(123)(4)
(124)(3)	(134)(2)	(234)(1)
ez: (34)	(234)	(1234)
odd ×	even ✓	odd ×.

instead:

(123)(4)	(123)(4)
(142)(3)	(243)(1)
τ = (243) ✓	(124) ✓

So σ can be conj. in A_4 to get a generator of any of the other gps.

Now $(\tau\sigma\tau^{-1})^2 = \tau\sigma^2\tau^{-1} \Rightarrow$ all 4 subgps are conj.

III*: $P = \langle (123) \rangle$.

$N_{A_4}(P) = P$ as $P \leq N_{A_4}(P)$ and if $\sigma \in A_4 \setminus P$,

(can check): $\sigma = (j4)\sigma'$ or $\sigma'(j4)$ w/ σ' having no 4's. ($j \neq 4$)

So $\sigma(123)\sigma^{-1}$ acts on 4 as $(j4)(123)(j4)$

sends 4 to $(123)\cdot j \neq 4 \Rightarrow$ doesn't fix $4 \Rightarrow$ goes outside P.

$\therefore [A_4 : N_{A_4}(P)] = 12/3 = 4 = n_3$ ✓

$p=2$: $Syl_2 = \{$subgps of size 4$\}$.

4 cycles are odd, so just one choice: $P = \langle (12)(34) \rangle$. (order 4.) $(13)(24)$ ✓

$\Rightarrow n_2 = 1 \equiv 1 \bmod 2$ ✓

$n_2 | 3$ ✓

Reverse: Sylow II $\Rightarrow gPg^{-1} = P \ \forall g \in G \Rightarrow P \trianglelefteq A_4$.

$\Rightarrow [A_4 : N(P)] = [A_4 : A_4] = 1 = n_2$ ✓

Lemma: $n_p = 1 \Leftrightarrow P \in Syl_p(G)$ is normal.

Pf: Sylow II says all p-Sylows conj. so

$n_p = 1 \Leftrightarrow$ all conjugates of P are P (all same size $\Rightarrow$ all Sylow.)

$\rightsquigarrow$ Often shows a gp isn't simple (like A_4).

Lemma: If $p, q \,|\, |G|$, $n_p = n_q = 1$, all elts of $P \in Syl_p(G)$ commute w/ elts of $Q \in Syl_q(G)$.

(2)

Pf: $|P|, |Q|$ rel prime $\overset{\text{Lagrange}}{\Longrightarrow} P \cap Q = \{e\}$.

Lemma $\Rightarrow P, Q \trianglelefteq G$. For $x \in P$, $y \in Q$ (compute commutator)

$\Rightarrow$ * $xyx^{-1}y^{-1} = \underbrace{(xyx^{-1})}_{\in Q} y^{-1} = x \underbrace{(yx^{-1}y^{-1})}_{\in P} \in P \cap Q = \{e\}$.

$\Rightarrow xy = yx$ ■

Direct Products: Useful in many classifications.

Recall: $G \times H = G \times H$ as a set,
$(g,h)\cdot(g',h') = (gg', hh')$ (what else?)

They contain a copy of their factors.

E.g.: $\mathbb{R}^2$ has a copy of $\mathbb{R}$; any line thru 0: 

Specifically:

Prop: $G_1, \dots, G_n$ gps, $G := G_1 \times \dots \times G_n$.

1). $\forall\, i = 1, \dots, n$.

$G_i \cong \{(1, \dots, g_i, \dots, 1) \mid g_i \in G_i\} =: \mathcal{G}_i$.
(ith spot)

Identifying G_i w/ this set,

$G/G_i \cong G_1 \times \dots \times \widehat{G_i} \times \dots \times G_n$.

2). The projection $\pi : G \twoheadrightarrow G_i$ is a surj. hom. $(g_1, \dots, g_n) \mapsto g_i$

$\ker(\pi) = \{(g_1, \dots, 1, \dots, g_n) \mid g_j \in G_j\ \forall j \neq i\}$.

3). Using the identification of (1), elts of G_i commute w/ elts of G_j, $i \neq j$.

• Later: How to identify this situation in gp construction.

Pf: 1). $\mathcal{G}_i$ is a subgp: $(1,\dots,1) \in \mathcal{G}_i$ ✓

$(1,\dots,g,\dots,1)(1,\dots,h,\dots,1)^{-1} = (1,\dots,gh^{-1},\dots,1) \in \mathcal{G}_i$ ✓

(inherits property for free as diff. components don't interact).

Show: $G_i \cong \mathcal{G}_i$.

map: $G_i \to \mathcal{G}_i$
$g_i \mapsto (1,\dots,g_i,\dots,1)$.

for similar reasons, this is a hom. its clearly bijective
$\Rightarrow$ isomorphism

Identify G_i w/ $\mathcal{G}_i \leq G$.

Consider $\varphi: G \to G_1 \times \dots \times \widehat{G_i} \times \dots \times G_n$
$(g_1,\dots,g_n) \mapsto (g_1,\dots,\widehat{g_i},\dots,g_n)$. (delete the ith component)

hom: $\varphi((g_1,\dots,g_n)(h_1,\dots,h_n))$
$= \varphi((g_1h_1,\dots,g_nh_n)) = (g_1h_1,\dots,\widehat{g_ih_i},\dots,g_nh_n)$
$= \varphi((g_1,\dots,g_n))\varphi((h_1,\dots,h_n))$ (Also comes $\cong$ for free).

Surj: $(g_1,\dots,g_{i-1},g_{i+1},\dots,g_n)$
mapped to by $(g_1,\dots,1,\dots,g_n)$, for example.

$\ker\varphi = \{(g_1,\dots,g_n) \mid g_j = 1 \ \forall j \neq i\} = \mathcal{G}_i$, identify w/ G_i.

Done by 1st Iso theorem.

2). Exercise (so similar/E-Z).

3). Say $x = (1,\dots,g_i,\dots,1) \in \mathcal{G}_i$, $y = (1,\dots,g_j,\dots,1) \in \mathcal{G}_j$, $i \neq j$

different spots.

WLOG, $i<j \Rightarrow xy = yx = (1,\dots,g_i,\dots,g_j,\dots,1)$ no interaction

We saw: Part (3) happens for Sylow p, q-subgps, $n_p = n_q = 1$.

More generally:

$\underline{Th^m}$: ~~All~~ All Sylow subgps. of G normal
$\iff$ G is isom. to direct product of all Sylow gps.

$\underline{Pf}$: ~~All Sylow subgps of G are no.~~
$\Leftarrow$: Factors of products are normal by Prop^{n}(1).
$\Rightarrow$: Conversely, Suppose $P_1, \dots, P_m \trianglelefteq G$ are all its Sylow subgps.
✓ primes $p \mid |G|$.
$\underline{\text{Lemma}} \Rightarrow$ elts. of P_i commute w/
" " P_j, $i \neq j$.

$\underline{\text{Map}}$: $\varphi: P_1 \times \dots \times P_m \to G$.
$(g_1, \dots, g_m) \mapsto g_1 \cdots g_m$ product.

$\underline{\text{Hom}}$: $\varphi(g_1, \dots, g_m)\varphi(g_1', \dots, g_m') = g_1 \cdots g_m g_1' \cdots g_m'$
$= g_1 g_1' g_2 g_2' \cdots g_m g_m'$
$= \varphi((g_1 g_1', \dots, g_m g_m'))$

$\underline{\text{Inj}}$: order of prod. of commuting elts $=$ lcm of orders
$=$ product of orders here since orders are rel. prime.
$\Rightarrow \ker(\varphi) = \{\text{elts. s.t. } |\varphi(g_1, \dots, g_m)| = 1\}$
$= \{\text{elts s.t. } \underline{\text{each}}\ g_i = 1\} = 1$.

$\underline{\text{Surj}}$: ~~This~~ φ is an injection b/w gps of equal size.

$\underline{\text{Ex}}$: All gps of order 45 are abelian.

$\underline{\text{Pf}}$: Suppose $|G| = 45$.
$9 \| 45$, $5 \| 45$.

Sylow III $\Rightarrow$ $n_3 \mid 5$, $n_3 \equiv 1 \bmod 3 \Rightarrow n_3 = 1$
$n_5 \mid 9$, $n_5 \equiv 1 \bmod 5 \Rightarrow n_5 = 1$
$\Rightarrow \exists\, P, Q \trianglelefteq G$, $|P| = 9$, $|Q| = 5$.

Gps of order 9, 5 are abelian (5 is prime, $9 = p^2$, recall: $Z(G) \neq 1$ class eq^{n}. $G/Z(G)$ cyclic $\Rightarrow G$ abelian). useful sometimes to recall math steps.

Now $PQ \trianglelefteq G$ as $P \trianglelefteq G$. (or $Q \trianglelefteq G$)

Lagrange $\Rightarrow |PQ| \equiv 0 \mod 5, 9$.

$\Rightarrow |PQ| \equiv 0 \mod 45$

$\Rightarrow PQ = G$.

Now G is abelian as P, Q commute in themselves (abelian) and w each other by the Lemma).

N.B. Same works for $p^2 q = |G|$, $p < q$, $q \not\equiv 1 \mod p$.

Ex: Gps of size $1573 = 11^2 \cdot 13$ are abelian. (2 of them; C_{1573}, $\mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$)

~~Here~~

Thm: p, q primes, $p < q$, $q \not\equiv 1 \mod p$, $|G| = pq$.

$\Rightarrow G$ is cyclic, $G \cong \mathbb{Z}/pq\mathbb{Z}$. [Used on HW.]

Pf: Assume the notation above.

Cauchy's theorem $\Rightarrow \exists$ elt. a of order p $\rightsquigarrow P = \langle a \rangle$
elt b of order q. $Q = \langle b \rangle$ Sylow subgps.

Sylow III $\Rightarrow n_p | q$, $n_p \equiv 1 \mod p \Rightarrow n_p = 1$ or q.

but it's not q as $q \not\equiv 1 \mod p$ by assumption.

$\Rightarrow n_p = 1 \Rightarrow P \trianglelefteq G$.

Sylow III again $\Rightarrow n_q | p$, $n_q \equiv 1 \mod q$.

$\Rightarrow n_q = 1$ or p.

But $1 < p < q$, $n_q \equiv 1 \mod q \Rightarrow n_q = 1 \Rightarrow Q \trianglelefteq G$.

Lemma $\Rightarrow$ elts of P commute w elts of Q. (orders)

$\Rightarrow a, b$ commute $\Rightarrow |a \cdot b| = \operatorname{lcm}(p, q) = p \cdot q$

$\Rightarrow \langle ab \rangle = G$.

Ex: If $|G| = 30$, G has normal 3, 5 Sylow subgps.

Pf: ~~If~~ Cauchy $\Rightarrow \exists g \in G$, $|g| = 2$.

left regular action:

$G \circlearrowright G$ left. mult.

Perm. rep^n: $\pi : G \hookrightarrow S_{30}$

H.W problem (4.2.11) $\Rightarrow \pi(g)$ = product of 15 trans.

$\Rightarrow \pi(g)$ is odd.

$\Rightarrow G \xrightarrow{\pi} S_{30} \xrightarrow{\text{sgn}} \{\pm 1\}$. composes to $G \twoheadrightarrow \{\pm 1\}$.

$K = \ker(\text{sgn} \circ \pi) \trianglelefteq G$, $|K| = 15 = 3 \cdot 5$.

$3 \nmid (5-1) \underset{\text{(last)}}{\Rightarrow} K$ is cyclic. Its 3-Sylow, 5-Sylow are normal in K since K is abelian.

Normal in G by next lemma.

Lemma: $N \trianglelefteq G$, $P \in \text{Syl}_p(N)$, $P \trianglelefteq N \Rightarrow P \trianglelefteq G$

Pf: $P \trianglelefteq N \Rightarrow N$ is the only p-syl. gp. of N.

$\Rightarrow \forall g \in G$, $gPg^{-1} \subseteq gNg^{-1} \underset{(N \trianglelefteq G)}{=} N \Rightarrow gPg^{-1}$ sylow P in N.

$\Rightarrow \underset{\text{(only sylow p- in N)}}{gPg^{-1} = P} \Rightarrow P \trianglelefteq G$.

Extra time: see sheet.

Fun:

Wilson's th^m:

$(p-1)! \equiv -1 \mod p$

Pf 1: $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot p-1$ all pair w inverses. only ± 1 don't pair w themselves $\rightarrow 1 \cdot (-1) = -1 \mod p$

Pf 2) S_p: sylow = p-cycles

$(p-2)!$ many gps. $n_p = (p-2)! \equiv 1 \mod p$.