$x((x,y,z)) = x$

Study of finite groups 2013 02 27

key technique: group actions

Fact: If $H \le G$, $[G:H]=2$, then $H \trianglelefteq G$.

Proof: Left cosets of H in G are H and aH, right are H, Ha.

Well $H = H$ ✓. Now $aH = G \setminus H = Ha$ as required. ∎

generalize

Action of G on the left cosets of H: $g \cdot aH = (ga)H$

- this is transitive (one orbit)
- $G_{aH} = \{g \in G ; gaH = aH\} = \{g \in G ; ga \in aH\} = \{g \in G ; g \in aHa^{-1}\} = aHa^{-1}$
- ker of action $= \bigcap_{aH \in A} G_{aH} = \bigcap_{a \in G} aHa^{-1}$

Thus ker is intersection of all conjugates of H

Let $K = \ker \psi$, $\psi : G \to S_A$. We saw $K \trianglelefteq G$.

This proves:

Prop: If $H \le G$, $K = \bigcap_{a \in G} aHa^{-1}$, then

1) $K \trianglelefteq G$
2) $K \le H$ (why!) $\to$ well $K \subseteq eHe^{-1} = H$ and K a group
3) $G/K \cong$ subgroup of $S_{\underbrace{\{aH;\, a \in G\}}_{A}}$ $\leftarrow$ 1st iso thm with ψ

Application 1: Suppose G is finite, p smallest prime divisor of $|G|$.

If $H \le G$ with $[G:H] = p$ then $H \trianglelefteq G$ $(k = [H:K])$

Proof: By prev. prop. get $K \trianglelefteq G$, $K \le H$, $G/K \cong$ subgroup S_A.

But $|A| = p \Rightarrow |S_A| = p! \Rightarrow$ (Lagrange) $|G/K| \mid p! \Rightarrow pk \mid p! \Rightarrow k \mid (p-1)!$

Note ~~As~~ $k \mid |H|$, $k \mid |G|$,

as p smallest, prime divisors of k is $\ge p$ $\therefore k = 1$

$\Rightarrow K = H \Rightarrow H = K \trianglelefteq G$.

review this

ex: $|G| = 36$, $H \le G$, $|H| = 18$: $[G:H] = 2 \Rightarrow H \trianglelefteq G$.

Application 2: Suppose G is finite, $H \le G$, $|G| \nmid [G:H]!$.

Then $\exists K \trianglelefteq G$ st $1 < K \le H$

Proof: By prop, $\exists K \trianglelefteq G$, $K \le H$, $G/K \cong$ subgroup of S_A, $A =$ cosets of H.

Suppose $K = \{e\}$. Then $G \cong G/K \cong$ subgroup of S_A. $|S_A| = |A|! = [G:H]!$ So

$|G| \mid |S_A| \Rightarrow |G| \mid [G:H]! \Rightarrow$ ✗ $\therefore 1 < K$

2013 02 27(2)

ex. If $|G| = 36$, $H \leq G$, $|H| = 9$. Then $[G:H]! = 4\cdot3\cdot2\cdot1 = 24$.
Note $36 \nmid 24$, so $\exists K \trianglelefteq G$ st $\{e\} < K \leq H$, so $|K| \in \{3, 9\}$.

midterm on
2013 03 01

Studying Groups Through Actions 2013 03 09

$H \trianglelefteq G$, G acting on ~~itself~~ H by conjugation

Special case $G = H$

$\ker = \{g \in G ; ga = ag \ \forall a \in G\} = Z(G)$

Def orbit of $a \in A$ is $\{gag^{-1} ; g \in G\}$ the conjugacy class of a, the conjugates of

ex If G is abelian then a is the only conjugate of a

ex $G = S_n$ for $\sigma \in S_n$ has conj. class being set of elements with same cycle type

$\sigma = (1\ 2\ 3)(4\ 5) \in S_7$

$\tau \sigma \tau^{-1} = (a\ b\ c)(d\ e)$ where $\tau(i) = i^{th}$ letter

Def Stabilizer is $G_a = \{g \in G ; gag^{-1} = a\} = \{g \in G ; ga = ag\} =: C_G(a)$ the centralizer of a

Note $Z(G) = \bigcap_{a \in G} C_G(a)$

Note if $\mathcal{O}$ is conjugacy class of a then $|\mathcal{O}| = [G : C_G(a)]$

Prop Thus the number of conjugates of a is $[G : C_G(a)]$

Consider conjugacy classes:

- one element iff $[G : C_G(a)] = 1$ iff $C_G(a) = G$ iff $a \in Z(G)$
- list conjugacy classes $\mathcal{O}_1, \ldots, \mathcal{O}_k$, pick reps $a_1, \ldots, a_k$

  if G is finite then $|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{O}_i|$

  $= |Z(G)| + \sum_{i=1}^{k} [G : C_G(a_i)]$ the class equation

Theorem: If p is prime and $|G| = p^n$ $(n \geq 1)$ then $Z(G) \neq \{e\}$.

Proof: Let $a_1, \ldots a_k$ be reps for non-trivial conj. classes and consider the class equation $p^n = |Z(G)| + \sum_{i=1}^{k} [G : C_G(a_i)]$.

Note $p \mid [G : C_G(a_i)] \ \forall i \Rightarrow p \mid |Z(G)| \Rightarrow p \leq |Z(G)|$ ∎

Theorem (Cauchy's Theorem): Let G be a finite group, p a prime st $p \mid |G|$. Then G has an element of order p.

Proof: Write $|G| = pm$, use induction on m. Base-case we saw. (easy) So assume $m > 1$. If G is abelian, we saw last week.[Th] So assume G is not abelian. Write

$$pm = |Z(G)| + \sum_{i=1}^{k} [G : C_G(a_i)] \qquad (*)$$

If $\exists i$ st $p \mid |C_G(a_i)|$ then (as $C_G(a_i) < G$) apply inductive assumption.
If $\forall i$ $p \nmid |C_G(a_i)|$ then $\forall i$ $p \mid [G : C_G(a_i)]$. So by $(*)$, $p \mid |Z(G)|$. As $Z(G) < G$ as G is not abelian. By induction assumption ✓ ∎

2013 0306

Def] Let p be prime. A p-group is a group of order p^n, for $n \geq 1$.

Corollary: Let G be a finite group. Then G is a p-group iff $|G|>1$ and $\forall a \in G$ $|a|$ is a power of p.
Proof: Exercise. Easy, plus Cauchy's theorem.

Def] Let G be a finite group, p a prime st $p \mid |G|$. A p-subgroup of G is a subgroup of G that is a p-group.

Prop: Let G be a finite group, p a prime st $p \mid |G|$. Then $\exists$ p-subgroup of G.
Proof: By Cauchy's Theorem, $\exists a \in G$ st $|a| = p$. So $|\langle a \rangle| = p$, $\langle a \rangle \leq G$. ∎

ex $|G| = 24$, 2-subgroups: must have size 2, 4, or 8 ($16 \nmid 24$)

ex Let G be finite, $H \leq G$. Take $A = G/H$, and let H act on A by left multiplication
We want to find the analogue to the class equation
Let $aH \in G/H$. Then $\{aH\}$ is an orbit iff $haH = aH$ $\forall a \in H$
iff $a^{-1}haH = H$ $\forall a \in H$
iff $a^{-1}ha \in H$ "
iff $h \in aHa^{-1}$ "
iff $H \leq aHa^{-1}$
iff $H = aHa^{-1}$ as H is finite
iff $a \in N_G(H)$
iff $aH \leq N_G(H)$

Let X be the union of the 1-element orbits.
Let $\theta_1, \dots \theta_k$ be the non-trivial orbits.
So

$$|A| = |X| + \sum_i |\theta_i|$$

(*) $$[G:H] = [N_G(H):H] + \sum_i |\theta_i|$$

Note $|\theta_i| \mid |H|$ and $|\theta_i| > 1$ (✩)

Prop: Let G be a finite group, p a prime st $p \mid |G|$, H a p-subgroup of G.
Then $[G:H] \equiv [N_G(H):H]$ (mod p).
Proof: By (*), need to show $p \mid \sum_i |\theta_i|$. As $|H| = p^m$, $m>1$, by (✩) get ~~$p \mid |\theta_i|$ $\forall i$~~ $|\theta_i| = p^{m_i}$ $\forall i \Rightarrow p \mid \sum_i |\theta_i|$. ∎

2013 03 06 (2)

Theorem Let G be finite, p prime, H a p-subgroup. If $|H| = p^k$ and $p^n \mid |G|$ for $n > k$, then $\exists\, H_1 \leq G$ st $H \leq H_1$ and $|H_1| = p^{k+1}$

Proof: $\boxed{\text{Case 1}}$: $H \trianglelefteq G$: Note G/H a group and $p \mid |G/H|$. By Cauchy's theorem, $\exists\, aH \in G/H$ st $\overset{(\text{order})}{o}(aH) = p$. So $\langle aH \rangle = \{H, aH, \dots, a^{p-1}H\} \leq G/H$.

Let $H_1 = H \cup aH \cup \cdots \cup a^{p-1}H \subseteq G$. Note $|H_1| = p|H| = p^{k-1}$. Exercise: Show $H \lneq H_1 \leq G$.

$\boxed{\text{Case 2}}$: $H \not\trianglelefteq G$: Well $H \trianglelefteq N_G(H)$. Suffices to show $p^j \mid |N_G(H)|$ for $j > k$. Let $|G| = p^n m$. By prop, $\underbrace{[G:H]}_{n-k \geq 1 \ \to\ p^{n-k}m \equiv 0 \bmod p} \equiv \underbrace{[N_G(H):H]}_{\equiv\, 0 \bmod p} \pmod p$ $\Rightarrow$

So $p \mid [N_G(H):H]$. By case 1, done. $\blacksquare$

where $p^n \| |G|$, $p^{n+1} \nmid |G|$

2013 03 08

Def] Let G be a finite group. Any subgroup of G of order p^n is a Sylow p-subgroup of G.

Theorem (Sylow's First Theorem): With G as above, $\exists$ a Sylow p-subgroup.
Proof: Follows from last class. $\blacksquare$

ex Let G be finite, $H, K \leq G$.
Let $A = G/H$. Let K act on G/H by left mult. ($k \cdot aH = (ka)H$).
$|A| = [G : H]$. What are the 1-elm orbits? How many are there?
Well $\{aH\}$ is orbit iff $kaH = aH \quad \forall k \in K$

iff $a^{-1}ka \in H$ "

iff $k \in a^{-1}Ha$ "

iff $K \subseteq a^{-1}Ha$ "

In particular, $|H| = |K|$ iff $K = aHa^{-1}$

In this situation, $\exists$ a 1-elm orbit iff H, K are conjugate

Theorem (Sylow's Second Theorem): Let G be finite, and P, Q be Sylow p-subgroups. Then P and Q are conjugate
Proof: In the above action, take $P = K$, $Q = H$. Then the action has a one-elm orbit iff P, Q are conjugate, by the above.
Analogue of class equation: let X be the union of 1 elm orbits, let $\theta_1, \ldots, \theta_k$ be the non-trivial orbits. So $|A| = |X| + \sum |\theta_i|$
Note $|A| = |G|/|Q|$, $|\theta_i| \,\big|\, |P|$.
Write $|G| = p^n m$, $n \geq 1$, $p \nmid m$ So $|P| = |Q| = p^n$.
We see $|\theta_i|$ is a proper positive power of p so the sum is a multiple of p. As LHS is not mult of p, as LHS $= m$, can't have $|X| = 0$, as required. $\blacksquare$

Observation: If $H \leq G$, the # of conjugates of H is $[G : N_G(H)]$.
Proof: Let A be all subgroups of G, let G act on A by conjugation.
So we want the size of the orbit θ of H:
$|\theta| = [G : G_H] \quad G_H = \{g \in G,\ gHg^{-1} = H\} = N_G(H)$. $\blacksquare$

2012 03 08(2)

Cor.: G finite, p prime, $p \mid |G|$. Let $n_p = \#$ of Sylow p-subgroups of G.
Then $n_p = [G : N_G(P)]$ where P is any S " " p.
Proof: By 2nd thm, $n_p = \#$ conjugates of P. By prev obser. have $n_p = [G : N_G(P)]$. ■

Cor.: As above. Then $P \trianglelefteq G$ iff $n_p = 1$.
Proof: P normal iff $N_G(P) = G$ iff $[G : N_G(P)] = [G : G]$ iff $n_p = 1$. ■

Cor.: As above. Let P, Q be Sylow p-subgroups of G. Then $P \leq N_G(Q)$ iff $P = Q$.
Proof: $\Leftarrow$ clear, $\Rightarrow$: Well $\begin{matrix} P \\ Q \end{matrix} \leq N_G(Q) \leq G$, and P, Q are Sylow p-subgroups of $N_G(Q)$. Note $Q \trianglelefteq N_G(Q)$. By prev. cor. $N_G(Q)$ has only 1 Sylow p-subgroup, so $P = Q$. ■

what is analogue

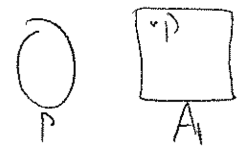
2013 03 11

Cor.: $P \cap N_G(Q) = P \cap Q$

For last Sylow thm,
let G finite, fix a Sylow p-subgroup P.
$p \mid |G|$, prime,

?

Let $A = \{\text{all Sylow } p\text{-subgroups}\}$.
Let P act on A by conjugation, ie $\forall g \in P$, $g \cdot Q = gQg^{-1} \in A$,



We want the analogue of the class equation, for this action
① Pick $Q \in A$. What is stabilizer?

$$\begin{aligned} P_Q &= \{g \in P;\ g \cdot Q = Q\} \\ &= \{g \in P;\ gQg^{-1} = Q\} \\ &= \{g \in P;\ g \in N_G(Q)\} = P \cap N_G(Q). \end{aligned}$$

(Aside = $P \cap Q$)

Let $\mathcal{O}$ be the orbit containing Q, then $|\mathcal{O}| = [P : P \cap N_G(Q)]$

?

so $|\mathcal{O}| = 1$ iff $[P : P \cap N_G(Q)] = 1$
iff $P \cap N_G(Q) = P$
iff $P \leq N_G(Q)$
iff $P = Q$

So the only one element orbit under conjug. by P wrt to Sylow p-subgroup of G is P itself.

Theorem (Sylow's Third Theorem): Let G be finite, $p \mid |G|$ prime, n_p be # of Sylow p-subgroups.
Then $n_p \equiv 1 \mod p$, and $n_p \mid m$, where $|G| = p^n m$, $p \nmid m$.
Proof: Let P be a p-Sylow. Consider $(P, A, \cdot)$, as above.
Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the non-trivial orbits. (The only trivial orbit is $\{P\}$.
So $n_p = |A| = 1 + \sum_{i=1}^{k} |\mathcal{O}_i|$. (*)
Now $|\mathcal{O}_i| \mid |P| = p^n \Rightarrow |\mathcal{O}_i| = p^{d_i} \Rightarrow p \mid |\mathcal{O}_i| \rightarrow p \mid \sum_{i=1}^{k} |\mathcal{O}_i|$
Hence $(|A| =) n_p \equiv 1 \mod p$ by (*)
For second claim, $n_p = [G : N_G(P)]$ = # conjugates of P in G
= # of Sylow p-subgroups

So $n_p \mid |G| \Rightarrow n_p \mid p^n m \Rightarrow n_p \mid m$ (as $n_p \equiv 1 \mod p$)

ex $G = S_4$, $|S_4| = 24 = 2^3 \cdot 3$

P a Sylow 2-group $\Rightarrow |P| = 2^3 = 8$

Q 3 $\Rightarrow |Q| = 3$

$n_3 \equiv 1 \mod 3$, $n_3 | 8$, so $n_3 \in \{1, 4\}$

How many subgroups of S_4 of order 3?

elm of order 3 : $(a\ b\ c) \rightarrow 8$

$\Rightarrow n_3 = 4$ (?)

Why?

Pick $Q = \langle (1\ 2\ 3) \rangle$

What is $N_G(Q)? = N_{S_4}(Q)$

$[S_4 : N_{S_4}(Q)] = n_3$ (why?)

$= 4$ (by above)

$\Rightarrow |N_{S_4}(Q)| = 24/4 = 6$

What is n_2? Note all Sylow 2-subgroups have size $2^3 = 8$

By 3rd thm know $n_2 \equiv 1 \mod 2$, $n_2 | 3 \Rightarrow n_2 \in \{1, 3\}$

$D_4 \cong \{1, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (1\,2)(3\,4), (1\,3), (1\,4)(2\,3), (2\,4)\} \leq$

↳ this is a Sylow 2-subgroup of S_4

conjugate this by elms of S_4 to get the other two ($n_2 = 3$)

Applications of Sylow Theorems

Generalize

2013 03 13

Fact: Every group G of order 15 is cyclic.

Proof: By Sylow thms, let P, Q be Sylow 3,5-subgroups. So $|P|=3$, $|Q|=5$.

By A6, $Q \lhd G$, $PQ=G$, and G is abelian iff $P \lhd G$.

By Sylow's 3rd thm, $n_3 \equiv 1 \bmod 3$, $n_3 | 5$
so $n_3 = 1$
$\Rightarrow P \lhd G \Rightarrow G$ abelian

Let $a, b \in G$ st $|a|=3$, $|b|=5$ (by Cauchy)
Let $c=ab$, $n=|c|$. Note $n \mid |G| \Rightarrow n | 15$,

$1 = c^n = (ab)^n = a^n b^n$ as abelian
so $a^n = b^{-n} \in \underbrace{P \cap Q = \{1\}}$ (as $P = \langle a \rangle$, $Q = \langle b \rangle$)
$\Rightarrow a^n = b^{-n} = 1$ ($\Rightarrow b^n = 1$)
follows from assignment
$\Rightarrow 3|n, 5|n$
$\Rightarrow 15 | n$

So $n|15$, $15|n \Rightarrow n = 15$, so $G = \langle c \rangle$. ∎

Proposition: Let G be a group of order pq where $p<q$ are prime. Then G is cyclic if $p \nmid (q-1)$

Proof: P, Q Sylow p,q-subgr.

"

By Sylow 3rd thm, $n_p \equiv 1 \bmod p$, $n_p | q$.
$\Rightarrow n_p \in \{1, q\}$, but as $p \nmid q-1$,
get $n_p = 1$ (ie $n_p \neq q$)
(~~the~~ rest fails if $n_p = q$) *

$a, b \in G$ st $|a|=p$, $|b|=q$

"

"

" ∎

ex $p=2$, $q=3$, $G = S_6$ non abelian
$G = D_8$
(example of failure *)

ex Suppose $|G|=12$, P a Sylow 2-subgroup, Q a Sylow 3-subgroup. Then $P \lhd G$ or $Q \lhd G$.
Proof: Note $n_3 \equiv 1 \bmod 3$, $n_3 | 4$, so $n_3 \in \{1,4\}$. If $n_3 = 1$ then $Q \lhd G$.
Assume then that $n_3 = 4$, ~~Note~~ say Q_1, Q_2, Q_3, Q_4. Note $n_2 \equiv 1 \bmod 2$, $n_2 | 3 \Rightarrow n_2 \in \{1,3\}$
If $n_2 = 1$ then $P \lhd G$. Assume not. So we have $|Q_i| = 3$, $|Q_1 \cap \cdots \cap Q_4| = 9 \Rightarrow 3$ left.
Thus no room for a second Sylow 3-group, let alone 4. (Things are disjoint as orders of things divide stuff) ∎

2013 03 13(2)

<u>Def</u>] A group G is called <u>simple</u> if its only normal subgroups are $\{e\}, G$.

(Aside: There was a program to classify finite simple groups)

~~Idea~~ Can use simple groups as "building blocks" to get other (finite) groups

↳ ex S_3:

$$\begin{array}{l} S_3 \\ | \\ \langle (1,2,3) \rangle = A_3 \triangleleft S_3 \\ | \\ \{e\} \end{array}$$

$S_3 / A_3 \cong \mathbb{Z}_2$ finite/simple

$A_3 \cong \mathbb{Z}_3$ (?) "

ex No group of order 72 is simple

Proof: Note $72 = 2^3 \cdot 3^2$. Assume* not simple

So $n_2 \equiv 1 \bmod 2$, $n_2 \mid 9 \Rightarrow n_2 \in \{1,3,9\} \Rightarrow n_2 \in \{3,9\}$ (else has non-triv normal subgroups)

$n_3 \equiv 1 \bmod 3$, $n_3 \mid 8 \Rightarrow n_3 \in \{1,4\} \Rightarrow n_3 = 4$

Let $Q_1, \dots, Q_4$ be the Sylow 3-subgroups. Note $|Q_i| = 9$, so the trick previous ex fails.

Note $[G : N_G(Q_1)] = n_3 = 4 \Rightarrow |N_G(Q_1)| = 18$

Look at $(G$, cosets of $N_G(Q_1), \cdot)$, $g \cdot aN = (ga)N$

Let K be the kernel. Saw ① $K \triangleleft G$

② $K \leq N$

③ $G/K \cong$ subgroup S_A, $|A| = 4$

①,② $\Rightarrow K = \{e\}$ by *, so $G \cong$ subgroup S_A

$\Rightarrow |G| \,/\, |S_A| \Rightarrow 72 \mid 24 \Rightarrow$ ⨳