MATH 3030 ALGEBRA I

Lecture 5

Cauchy's Theorem and p-groups

Prop★ Let G be a group of order p^n and let X be a finite G-set. Then $|X| \equiv |X_G| \pmod{p}$

Pf: Suppose that $G\cdot x_1, \dots, G\cdot x_r$ are all orbits in X with more than one element. Then

$$|X| = |X_G| + \sum_{i=1}^{r} [G : G_{x_i}]$$

But $|G| = p^n \Longrightarrow [G : G_{x_i}] \equiv 0 \pmod{p}$ for $i = 1, \dots, r$.

The result follows. #

Thm (Cauchy) Let p be a prime. If G is a finite group s.t. $p \mid |G|$,

Then $\exists\, g \in G$ with $|g| = p$.

Pf: Let $X = \{(g_1, g_2, \dots, g_p) \mid g_i \in G \text{ and } g_1 g_2 \cdots g_p = e\}$.

Since $g_1 g_2 \cdots g_p = e \iff g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$, we have $|X| = |G|^{p-1}$.

In particular, $p \mid |X|$.

Consider $\langle \sigma \rangle < S_p$ where $\sigma = (1, 2, \dots, p)$.

$\langle \sigma \rangle$ acts on X by

$$\sigma \cdot (g_1, g_2, \dots, g_p) := (g_2, g_3, \dots, g_p, g_1)$$

This is well-defined since $g_1 g_2 \cdots g_p = e \Rightarrow g_2 g_3 \cdots g_p g_1 = e$.

By Prop ★, we have

$$|X_{\langle\sigma\rangle}| \equiv |X| \equiv 0 \pmod p.$$

i.e. $p \mid |X_{\langle\sigma\rangle}|$; in particular, $|X_{\langle\sigma\rangle}| > 1$

Now, $X_{\langle\sigma\rangle} = X_\sigma = \{(g, g, \dots, g) \mid g \in G, g^p = e\}$.

So $\exists\, g \neq e$ s.t. $g^p = e$.

Since p is a prime, $|g| = p$. #

Sylow Theorems

Def Let p be a prime. A group G is called a p-group if every element in G has order a power of p. A subgroup of a group G is called a p-subgroup if the subgroup itself is a p-group.

Cor A finite group G is a p-group iff $|G|$ is a power of p.

Pf: ($\Leftarrow$) trivial.

($\Rightarrow$) If $q \neq p$ is another prime dividing $|G|$, then by Cauchy's Thm, $\exists a \in G$ s.t. $|a| = q$. So G is not a p-group. #

Def Let $H<G$. The set

$$N_G(H) := \{g\in G \mid gHg^{-1}=H\}$$

is a subgroup of G (prove this!), called the normalizer of H in G.

Rmks

- $N_G(H)=G$ iff $H \trianglelefteq G$.
- $N_G(H)$ is the largest subgroup of G in which H is normal.

Lemma If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G:H] \pmod p$$

Pf: Let $X = \{aH \mid a \in G\}$. Then $|X| = [G:H]$.

Consider the action of H on X by left multiplication.

Then

$$\begin{aligned} aH \in X_H &\iff haH = aH \quad \forall h \in H \\ &\iff (a^{-1}ha)H = H \quad \forall h \in H \\ &\iff a^{-1}ha \in H \quad \forall h \in H \\ &\iff a^{-1}Ha = H \\ &\iff a \in N_G(H) \end{aligned}$$

Hence we have $|X_H| = [N_G(H) : H]$. So the lemma follows from Prop★. #

Cor If H is a p-subgroup of a finite group G s.t. $p \mid [G:H]$ then $N_G(H) \neq H$.

Pf: By above lemma, $[N_G(H):H] \equiv [G:H] \equiv 0 \pmod{p}$.
In particular, $[N_G(H):H] > 1$. Therefore, $N_G(H) \neq H$. #

Thm (First Sylow Thm) Let G be a group of order $p^n m$ with $n \geq 1$, p a prime, and $\gcd(p,m) = 1$. Then

(1) G contains a subgroup of order p^i for each $1 \leq i \leq n$, and

(2) every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

<u>Pf</u>: (1) By Cauchy's Thm, G contains a subgroup of order p.

We proceed by induction and assume that $H < G$ is a subgroup of order p^i $(1 \leq i < n)$. Then $p \mid [G:H]$, so by above we have

$$H \lneq N_G(H) \quad \text{and} \quad 1 < |N_G(H)/H| = [N_G(H):H] \equiv [G:H] \equiv 0 \pmod{p}$$

Hence $p \mid |N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup K of order p by Cauchy's Thm again.

Now, $H < \pi^{-1}(K) < N_G(H) < G$ and $|\pi^{-1}(K)| = |K| \cdot |H| = p^{i+1}$,

where $\pi : N_G(H) \longrightarrow N_G(H)/H$ is the canonical map.

(2) By (1) and note that $H \triangleleft N_G(H) \Rightarrow H \triangleleft \pi^{-1}(K)$. #

Cor Any p-group is solvable.

Pf: Applying the 1st Sylow Thm to a p-group G gives a sequence

$$\{e\} = H_0 < H_1 < \cdots < H_{n-1} < H_n = G \quad (\text{say } |G| = p^n)$$

s.t. $H_{i-1} \triangleleft H_i$ and $H_i / H_{i-1} \cong \mathbb{Z}_p$ for $i = 1, 2, \dots, n$.

So G is solvable. #

Def A subgroup $P < G$ is called a Sylow p-subgroup if P is a maximal p-subgroup of G.

Thm (Second Sylow Thm) If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then $\exists g \in G$ s.t. $H < gPg^{-1}$.
In particular, any two Sylow p-subgroups of G are conjugate.

Pf: Let $X = \{aP \mid a \in G\}$.

Consider the action of H on X by left multiplication.

So $|X_H| \equiv |X| = [G:P] \pmod{p}$ by Prop ✯.

Now $p \nmid [G:P] \Rightarrow X_H \neq \emptyset$, and

$$\begin{aligned} aP \in X_H &\Leftrightarrow haP = aP \quad \forall h \in H \\ &\Leftrightarrow a^{-1}haP = P \quad \forall h \in H \\ &\Leftrightarrow a^{-1}Ha < P \\ &\Leftrightarrow H < aPa^{-1}. \end{aligned}$$

Hence $\exists\, a \in G$ s.t. $H < aPa^{-1}$.

When H is a Sylow p-subgroup, then $H = aPa^{-1}$. #

Thm (Third Sylow Thm) Let G be a finite group and p a prime s.t. $p \mid |G|$.
Denote by n_p the number of Sylow p-subgroups of G
Then $n_p \mid |G|$ and is of the form $kp+1$ for some $k \geq 0$.

Pf: By the 2nd Sylow Thm,

$$\# \text{ of Sylow } p\text{-subgroups} = \# \text{ of conjugates of } P \quad \text{(where } P < G \text{ is one of the Sylow } p\text{-subgps)}$$
$$= [G : N_G(P)] \mid |G|$$

The second equality is given by $|G \cdot P| = [G : G_P]$,

where G acts on $\left\{ \begin{array}{c} \text{all subgroups} \\ \text{of } G \end{array} \right\}$ by conjugation,

and noting that $G_P = N_G(P)$.

Now let $X = \left\{ \begin{array}{c} \text{Sylow } p\text{-subgroups} \\ \text{of } G \end{array} \right\}$.

Consider the action of P on X by conjugation.

Then $Q \in X_P \Leftrightarrow xQx^{-1} = Q \ \forall x \in P \Leftrightarrow P < N_G(Q)$.

Since P, Q are Sylow p-subgroups of G and hence of $N_G(Q)$, they are conjugate in $N_G(Q)$. But $Q \triangleleft N_G(Q) \Rightarrow P = Q$.

We conclude that $X_P = \{P\}$.

By above proposition, $|X| \equiv |X_P| = 1 \pmod{p}$. Hence $|X| = kp + 1$. #

|| Cor $n_p = 1 \Leftrightarrow$ the Sylow p-subgroup is normal.

Sylow p-subgp of G

Pf: By the 2nd Sylow Thm, $n_p = 1 \Leftrightarrow gPg^{-1} = P \ \forall g \in G \Leftrightarrow P \triangleleft G$. #

e.g.

- Consider the dihedral group D_n where n is odd.
  Then a Sylow 2-subgroup is given by $\langle \tau \rangle = \{id, \tau\}$ where $\tau \in D_n$ is a reflection. Note that $n_2 = n$ in this case.

- Consider the symmetric group S_p where p is a prime.
  Then a Sylow p-subgroup is given by $\langle \sigma \rangle$ where $\sigma \in S_p$ is a p-cycle. So $n_p = (p-2)!$, and Sylow III implies

$$(p-2)! \equiv 1 \pmod{p}$$

$$\Longrightarrow \quad (p-1)! \equiv -1 \pmod{p}$$

This is called Wilson's Theorem.

Applications of Sylow Theorems

Here are some simple applications:

Examples ① Suppose $|G| = 15$. By 1st Sylow Thm, G has a subgroup P of order 5.

By the 3rd Sylow Thm, $n_5 = 5k+1 \mid 15 \Rightarrow n_5 = 1$

So $P \triangleleft G$. Hence G is solvable and cannot be simple.

② Suppose $|G| = 20 = 2^2 \cdot 5$. By the 1st Sylow Thm, G has a subgroup P of order 5.

By the 3rd Sylow Thm, $n_5 = 5k+1 \mid 20 \Rightarrow n_5 = 1$

So $P \triangleleft G$. Hence G is solvable and cannot be simple.

To apply to more sophisticated cases, we may use some "counting" techniques:

Observation: If $H_1, H_2 < G$ are distinct subgroups of order a prime p, then $H_1 \cap H_2 = \{e\}$.

③ Suppose $|G| = 12 = 2^2 \cdot 3$. Then Sylow I & III $\Rightarrow \begin{cases} n_2 = 1 & \text{or } 3 \\ n_3 = 1 & \text{or } 4 \end{cases}$

If $n_3 = 4$ then the above lemma $\Rightarrow$ G has $4 \cdot 2 = 8$ elts of order 3

In this case, the remaining $12 - 8 = 4$ elts must form a Sylow 2-subgroup.

This implies $n_2 = 1$. Hence G is solvable and cannot be simple.

④ Suppose $|G| = 30 = 2 \cdot 3 \cdot 5$. Then Sylow I & III $\Rightarrow \begin{cases} n_3 = 1 & \text{or } 10 \\ n_5 = 1 & \text{or } 6 \end{cases}$

If $n_3 = 10$, then the above lemma $\Rightarrow$ G has $10 \cdot 2 = 20$ elts of order 3

If $n_5 = 6$, then the above lemma $\Rightarrow$ G has $6 \cdot 4 = 24$ elts of order 5

So we have either $n_3 = 1$ or $n_5 = 1$.

Hence G is solvable and cannot be simple.

Lemma Let $p \neq q$ be two prime factors of $|G|$.
If $n_p = n_q = 1$, then elements of the Sylow p-subgroup commute with elements of the Sylow q-subgroup.

Pf: Let P and Q be the Sylow p- and q-subgroup of G. Then $P, Q \trianglelefteq G$. Also $P \cap Q = \{e\}$ by the Thm of Lagrange since $p \neq q$. So for $a \in P$ and $b \in Q$,

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = \{e\}.$$

and hence $ab = ba$. #

Prop All Sylow subgroups of a finite group G are normal iff G is isomorphic to the direct product of its Sylow subgroups.

Pf : ($\Leftarrow$) Since a factor in a direct product is always a normal subgroup of the product, this direction is true.

($\Longrightarrow$) Write $|G| = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$. Since all Sylow subgroups are normal, $n_{p_i} = 1 \ \forall i$. Let P_i be the Sylow p_i-subgp in G.

Consider the map

$$\begin{aligned} \varphi : P_1 \times \cdots \times P_\ell &\longrightarrow G \\ (a_1, \ldots, a_\ell) &\longmapsto a_1 \cdots a_\ell \end{aligned}$$

Lemma $\Rightarrow$ φ is a homomorphism.

Note that $|a_i|$ is a power of p_i, so $|a_1|, \ldots, |a_\ell|$ are rel. prime.

$\Rightarrow |a_1 \cdots a_\ell| = |a_1| \cdots |a_\ell|$.

Therefore φ is injective, and hence bijective since it's a map between two groups of equal size. #

Rmk : This also shows that $G = P_1 P_2 \cdots P_\ell$.

Thm Let p and q be primes such that $q > p$, and let G be a group of order pq. Then

(1) G is solvable and hence not simple.

(2) If $q \not\equiv 1 \pmod{p}$, then $G \cong \mathbb{Z}_{pq}$

Pf: By the 3rd Sylow Thm, $n_q \mid |G| = pq$ and $n_q \equiv 1 \pmod{q}$. This forces $n_q = 1$ since $p < q$. So the Sylow q-subgroup Q is normal in $G \Rightarrow \{e\} < Q \lhd G$ is a solvable series for G.

Now suppose that $q \not\equiv 1 (\mathrm{mod}\ p)$. Then the 3rd Sylow Thm also implies that $n_p = 1$.
Let P and Q be the Sylow p- and q-subgroup of G.
Then P and Q are cyclic of order p and q respectively.
The previous proposition $\Rightarrow G \cong P \times Q \cong \mathbb{Z}_{pq}$. #

<u>Rmk</u> If $q \equiv 1 \pmod p$ then it can be shown that there are exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a nonabelian group K generated by two elements c and d

s.t. $|c| = q$, $|d| = p$, $dc = c^s d$

where $s \not\equiv 1 \pmod q$ and $s^q \equiv 1 \pmod q$

In particular, if q is an odd prime, then every group of order $2q$ is isomorphic either to $\mathbb{Z}_{2q}$ or the dihedral group D_q.

<u>Rmk</u> Similar arguments can show that groups of order $p^2 q$ and $p^2 q^2$ are solvable. More generally, we have Burnside's $p^a q^b$ Theorem: any finite group of order $p^a q^b$ is solvable, but its proof is beyond our scope.

⑤ Suppose $|G| = 255 = 3 \cdot 5 \cdot 17$. Sylow III $\Rightarrow n_{17} = 1 \Rightarrow \exists!$ Sylow 17-subgp $H \trianglelefteq G$.

By above, $|G/H| = 15 \Rightarrow G/H$ is cyclic. So $[G,G] < H \Rightarrow |[G,G]| = 1$ or 17.

By Sylow III again $\Rightarrow \begin{cases} n_3 = 1 \text{ or } 85 \\ n_5 = 1 \text{ or } 51 \end{cases}$

If $n_3 = 85$ and $n_5 = 51$, then G has $85 \cdot 2 + 51 \cdot 4 = 374$ elts, which is impossible.

So either $n_3 = 1 \Rightarrow |[G,G]| = 1$ or 3,

or $n_5 = 1 \Rightarrow |[G,G]| = 1$ or 5

We conclude that $[G,G]$ is trivial.

This implies that G is abelian and hence cyclic.

$\lvert G\rvert$	isom. classes
1	$\langle e\rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2\times\mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, D_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_4$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, D_4, Q

$\lvert G\rvert$	isom. classes
9	$\mathbb{Z}_9$, $\mathbb{Z}_3\times\mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_2\times\mathbb{Z}_6$, A_4, D_6, T
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7
15	$\mathbb{Z}_{15}$