Lecture 22  Proofs of Sylow theorems

Throughout, \( G \) denotes a finite group and \( p \) a prime.

**Cauchy's theorem:** If \( p \mid |G| \), there is an element of order \( p \).

Proof: see book.

**1st Sylow theorem** If \( p^n \mid |G| \), there is a subgroup \( H \leq G \) with \( |H| = p^n \).

Proof: Induction on \( n \). The case \( n=1 \) is Cauchy's theorem (let \( H = \langle g \rangle \) where \( g \) has order \( p \)).

So suppose \( p^n \mid |G| \), \( n > 1 \). By induction hypothesis, there is a subgroup \( H \leq G \) with \( |H| = p^{n-1} \). Since \( p^n \mid |G| \), we have \( p \mid |G|/|H| = |G:H| \).

Now consider the action of \( H \) on \( G/H \) by left multiplication:
\[ H \times (G/H) \rightarrow G/H \]
\[ h \cdot aH = (ha)H. \]

Because orbits are a partition,
\[ [G:H] = \# \text{ of singleton orbits} + \sum (\text{size of nonsingleton orbits}) \]

Now \( |H \cdot aH| = |H|/[\text{stab}(aH)] = p^{n-1} \) is a power of \( p \),

so the size of a non-singleton orbit is divisible by \( p \).

Since \( p \mid [G:H] \) and \( p \mid (\text{size of a nonsingleton orbit}) \), we find \( p \mid \# \text{ of singleton orbits} \).
There is always at least one singleton orbit, for
\[ H \cdot (aH) = \{ aH \} \]  
So in fact the number of singleton orbits is divisible by \( p \)

What does it mean that \( H \cdot (aH) = \{ aH \} \) ?
\[ \iff h \in H \iff a^{-1}ha \in H \forall h \in H \]  
\[ \iff H = aHa^{-1} \iff a \in N_a(H). \]

We now know that there is \( a \neq H \) such that \( H \cdot (aH) = \{ aH \} \)
So we know there is \( a \in H \) such that \( a \in N_a(H) \)
Thus \( N_a(H) \not\subseteq H \).
The number of singleton orbits is \([N_a(H):H]\), which is divisible
by \( p \).

Since \( H \) is normal in \( N_a(H) \), we can form \( N_a(H)/H \) which
is a group, and \( p \mid [N_a(H):H] \) By Cauchy's theorem,
there is a subgroup \( K \leq N_a(H)/H \) of order \( p \).
Let \( H' = \pi^{-1}(K) \) \( (\pi : N_a(H) \rightarrow N_a(H)/H) \)
Then \( H' \) has order \( p \cdot |H'| = p \cdot p^{n-1} = p^n. \]

2nd Sylow theorem \( \) Let \( H \leq G \) be a subgroup of order \( p^n \),
and let \( P \) be a \( p \)-Sylow subgroup (of order \( p^n \), \( n \geq s \)).
Then there is an \( a \in G \) such that \( aHa^{-1} \leq P \).

Proof \( \) Let \( X = \{ aPa^{-1} \mid a \in G \} \) be the set of conjugates of \( P \).
Claim \( p \) does not divide \( |X| \):
By orbit-stabilizer, \[ |X| = \frac{|G|}{|N_a(P)|} \]
\( p^n \mid |N_a(P)| \), since \( p^n \) is the largest power of \( p \) that divides \( |G| \),
\[ \frac{|G|}{|N_a(P)|} \] has no powers of \( p \) in its prime factorization.
Now let $H$ act on $X$ by conjugation.
A nonsingleton orbit has size divisible by $p$ (since it divides $|H|=p^s$).
Since $|X|$ is not divisible by $p$, there must be a singleton orbit.
That is, for some $g \in G$, $H \leq N_a(gP_{a^{-1}}) = gN_a(p)g^{-1}$.

Thus $g^{-1}Hg \leq N_a(P)$. Need to show $g^{-1}Hg \leq P$.

Let $\tilde{H} = g^{-1}Hg$.

Applying the diamond isomorphism theorem to $\tilde{H}$,
we find $\frac{|\tilde{H}P|}{|\tilde{H}|} = \frac{|P||H|}{|\tilde{H}P|}$.

The right hand side only involves powers of $p$, so $|\tilde{H}P| = p^n$ for some $n$.

Since $P \leq H \leq \tilde{HP} \leq G$, $|P||\tilde{H}P| \leq 161$,
$p^n | p^{\alpha} | 161$.

By maximality of $p$-Sylow subgroup, $n = m$ and $\tilde{H}P = P$ and $H \leq P$.

**3rd Sylow Theorem:** Let $p^n$ be the order of a $p$-Sylow subgroup $P$, and let $n_p$ be the number of $p$-Sylow subgroups.
Then $n_p \equiv 1 \pmod{p}$ and $n_p | 161/p^n$.

**Proof** Let $X$ be the set of $p$-Sylow subgroups. $G$ acts transitively on $X$ by 2nd Sylow theorem. If we consider $P$ acting on $X$ by conjugation, there is a fixed point $P \in X$:

$P \cdot P = \{gPg^{-1} | g \in \text{P}\} = \{\text{P}\}$

There are no other fixed points, for if $P \cdot Q = \{Q\}$,
then $P \leq N_a(Q)$, and by the argument in the previous proof this implies $P \leq Q$, so $P = Q$ since both have $p^n$ elements.
So there is only one singleton orbit. Every nonsingleton orbit has size \(|\phi(Q)| = |P|/\text{stab}_P(Q)|\), which is a power of \(p\), so divisible by \(p\). Thus
\[ n_p = |X| = kp + 1 \quad \text{so} \quad n_p \equiv 1 \pmod{p} \]

Since \(G\) acts transitively on \(X\),
\[ n_p = |X| = |G : P| = |G|/|N_G(P)| \quad [G : N_G(P)] \]

Now
so
\[ n_p \mid [G : P] = |G|/|P| \]