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 $p \mid |G|/p^{n-1} = |G|/|H| = [G:H]$.

Now consider the action of H on G/H by left multiplication:

$$H \times (G/H) \to G/H$$
$$h \cdot aH = (ha)H.$$

Because orbits are a partition,

$$[G:H] = \# \text{ of singleton orbits} + \sum (\text{size of nonsingleton orbits})$$

Now $|H \cdot aH| = |H| / |\mathrm{Stab}(aH)| = p^{n-1} / |\mathrm{Stab}(aH)|$ 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 $p \mid \#$ of singleton orbits.

There is always atleast one singleton orbit, for
$$H\cdot(eH)=\{heH \mid h\in H\} = \{eH\}$$
So in fact the number of singleton orbits is divisible by p

What does it mean that $H\cdot(aH)=\{aH\}$?
$\iff haH=aH$ for all $h\in H \iff a^{-1}ha\in H$ for all $h\in H$
$\iff H=aHa^{-1} \iff a\in N_G(H)$.
We now knew that there is $aH\neq H$ such that $H\cdot(aH)=\{aH\}$
So we know there is $a\notin H$ such that $a\in N_G(H)$.
Thus $N_G(H)\supsetneq H$.
The number of singleton orbits is $[N_G(H):H]$, which is divisible by p.
Since H is normal in $N_G(H)$, we can form $N_G(H)/H$ which is a group, and $p \mid |N_G(H)/H|$. By Cauchy's theorem, there is a subgroup $K\leq N_G(H)/H$ of order p.
Let $H'=\pi^{-1}(K)$ $\quad(\pi: N_G(H)\to N_G(H)/H.)$
Then H' has order $p\cdot|H|=p\cdot p^{n-1}=p^n$. $\blacksquare$

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

<u>Proof</u> Let $X=\{aPa^{-1}\mid a\in G\}$ be the set of conjugates of P.
<u>Claim</u> p does not divide $|X|$:
By orbit-stabilizer, $|X|=\dfrac{|G|}{|N_G(P)|}$ since $N_G(P)\geq P$,
$p^n \mid |N_G(P)|$, since p^n is the largest power of p that divides $|G|$, $\dfrac{|G|}{|N_G(P)|}$ 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 $g \in G$, $H \leq N_G(gPg^{-1}) = gN_G(P)g^{-1}$.

Thus $g^{-1}Hg \subseteq N_G(P)$. Need to show $g^{-1}Hg \leq P$.
Let $\tilde{H} = g^{-1}Hg$.
Applying the diamond isomorphism theorem to

$$\begin{tikzcd}[column sep=small] & \tilde{H}P \arrow[dl, dash] \arrow[dr, dash] & \\ P \arrow[dr, dash] & & \tilde{H} \arrow[dl, dash] \\ & \tilde{H}\cap P & \end{tikzcd}$$

we find

$$|\tilde{H}P| = \frac{|P||\tilde{H}|}{|\tilde{H}\cap P|}$$

The right hand side only involves powers of p, so $|\tilde{H}P| = p^m$ for some m.
Since $P \leq \tilde{H}P \leq G$, $|P| \,\big|\, |\tilde{H}P| \,\big|\, |G|$ $\quad p^n | p^m | \,|G|$.
By maximality of p-Sylow subgroup, $n=m$ and $\tilde{H}P = P$ and
$\tilde{H} \subseteq P$.

<u>3rd Sylow theorem</u>: 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 $n_p \,\big|\, |G|/p^n$.

<u>Proof</u> 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 $P \in X$:

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

There are no other fixed points, for if $P \cdot Q = \{Q\}$, then $P \subseteq N_G(Q)$, and by the argument in the previous proof this implies $P \subseteq Q$, so $P = Q$ since both have p^n elements.

So there is only one singleton orbit. Every nonsingleton orbit has size $|P\cdot Q| = |P|/|\mathrm{Stab}_P(Q)|$, 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,

$$n_p = |X| = |G\cdot P| = |G|/|N_G(P)| = [G : N_G(P)]$$

Now $[G:P] = [G:N_G(P)][N_G(P):P] = n_p[N_G(P):P]$

so $n_p \mid [G:P] = |G|/p^n$. $\blacksquare$