Lecture 21 Cauchy's theorem, Sylow theorems

Recall: If $g \in G$ (G finite) then the order of g divides $|G|$ (corollary of Lagrange's theorem).

Is the converse true? If $n \mid |G|$ is there necessarily an element of order n? No: $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. $4 \mid |G|$, but there is no element of order 4!

But we do have a "partial converse":

<u>Cauchy's Theorem</u> (5.4.6) Let G be a finite group. If p is a <u>prime</u> number dividing $|G|$, then G contains an element of order p.

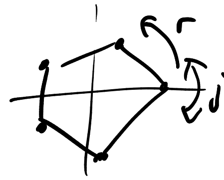
<u>Proof</u>: See the textbook for a very clever proof using group actions due to James H. McKay.

Can we do better? We can if we ask for subgroups whose order is p^n, where $p^n \mid |G|$.

<u>1st Sylow Theorem (5.4.7)</u> If p is a prime, n a natural number such that $p^n \mid |G|$, then there is a subgroup $H \leq G$ such that $|H| = p^n$.

<u>Def</u> If p^n is the <u>largest</u> power of p that divides $|G|$, then a subgroup $H \leq G$ with $|H| = p^n$ is called a p-Sylow subgroup. (The first Sylow theorem asserts the existence of a p-Sylow subgroup.)

Ex D_5 $|D_5| = 10$



$D_5 = \{e, r, r^2, r^3, r^4, j, rj, r^2j, r^3j, r^4j\}$
$r = r_{2\pi/5}$

Rotations $= \{e, r, r^2, r^3, r^4\}$ is a 5-Sylow subgroup
$\{e, j\}$ is a 2-Sylow subgroup. $\{e, rj\}$ is another 2-Sylow subgroup.

Ex $D_{20} = \{e, r, r^2, \ldots, r^{19}, j, rj, \ldots, r^{19}j\}$ $(r = r_{2\pi/20})$ $|D_{20}| = 40 = 8 \cdot 5$
So a 2-Sylow subgroup must have 8 elements.
In fact, D_{20} contains D_4 as a subgroup.

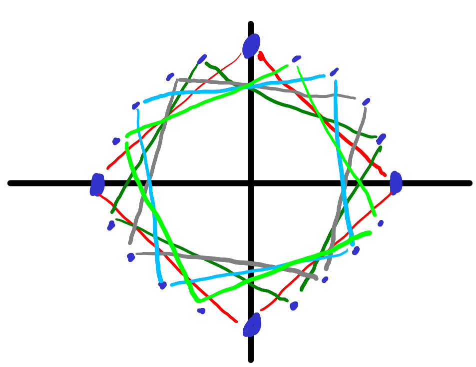
$H = \{e, r^5, r^{10}, r^{15}, j, r^5j, r^{10}j, r^{15}j\} \leq D_{20}$
is a 2-Sylow subgroup.

<u>2nd Sylow theorem</u> (5.4.9, 5.4.10) Any two p-Sylow subgroups are conjugate. If P_1 and P_2 are p-Sylow subgroups of G, there is an $a \in G$ such that $aP_1a^{-1} = P_2$.

<u>3rd Sylow theorem</u> (5.4.11) Let G be a finite group, and p a prime dividing $|G|$. Let n_p be the number of p-Sylow subgroups of G, and let P be a p-Sylow subgroup.
Then $n_p \mid |G|/|P|$ and $n_p \equiv 1 \pmod{p}$

<u>Example</u> In D_{20}, there are five 2-Sylow subgroups : $n_2 = 5$
so $n_2 = 5 \mid |D_{20}|/|P| = \frac{40}{8} = 5$
and $n_2 = 5 \equiv 1 \pmod{2}$ are both true.

Why five 2-Sylow subgroups?
5 ways to "embed" D_4 in D_{20}



An application:

<u>Proposition</u> If $|G| = pq$, where p and q are distinct primes and $p > q$, then $G \cong \mathbb{Z}_p \rtimes_\alpha \mathbb{Z}_q$ for some $\alpha : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$

<u>Proof</u>: let $P \leq G$ by a p-Sylow subgroup and $Q \leq G$ a q-Sylow subgrp. (Exist by 1st Sylow thm) Then $|P| = p$ and $|Q| = q$, so $P \cong \mathbb{Z}_p$ and $Q \cong \mathbb{Z}_q$ (classification of groups of prime order.)

Now $P \cap Q = \{e\}$ since any non identity $g \in P \cap Q$ would have order p and order q, which is absurd.

We claim P is normal in G: let n_p be the number of p-Sylow subgrps. Since all p-Sylow subgrps are conjugate (2nd Sylow), P is normal iff $n_p = 1$. But we know $n_p \mid q$ and $n_p \equiv 1 \pmod p$ (3rd Sylow) since $q < p$, we have $n_p < p$ and $n_p \equiv 1 \pmod p$, so $n_p = 1$. Thus P is normal.

Now we have $P \trianglelefteq G$, $Q \leq G$ and $P \cap Q = \{e\}$. By the recognition theorem for semidirect products, $PQ \leq G$ and $PQ \cong P \rtimes_c Q$ for $c : Q \to \mathrm{Aut}(P)$ $(c_g(h) = ghg^{-1})$

Since $|PQ| = |P||Q| = pq = |G|$, we have $PQ = G$.
Thus $G = PG \cong P \rtimes_c Q \cong \mathbb{Z}_p \rtimes_\alpha \mathbb{Z}_q$, where $\alpha : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ ∎