Math 493 Lecture 16

Professor Andrew Snowden

Transcribed by Thomas Cohn

10/30/19

Sylow Theorems

Let G be a finite group. Let p be a prime, and write $|G| = p^e m$, where $p \nmid m$.

Defn: A p-**Sylow subgroup** of G is a subgroup of order p^e.

Thm: (First Sylow Theorem) A Sylow subgroup exists, $\forall G$, $\forall p$.

Cor: (Cauchy's Theorem) If $p \mid |G|$, then G has an element of order p.
Proof: Let H be a p-Sylow subgroup of H. $\operatorname{ord} H = p^e > 1$, so let $h \in H$ with $h \neq 1$. Then $\operatorname{ord}(h) \mid |H| = p^e$, and $\operatorname{ord}(h) \neq 1$, so $\operatorname{ord}(h) = p^k$ for some $k > 0$. Thus, $\operatorname{ord}(h^{p^{k-1}}) = p$. $\square$

Observe: Any conjugate of a Sylow subgroup is a Sylow subgroup.

Thm: (Second Sylow Theorem) Let G be a group, H a p-Sylow subgroup, and let K be any subgroup of G. Then $\exists H'$ a conjugate of H such that $H' \cap K$ is a p-Sylow subgroup of K.

Cor: Any two p-Sylow subgroups in G are conjugate.
Proof: Let H, K be p-Sylow subgroups. By the second theorem, there is a conjugate H' of H s.t. $K \cap H'$ is a p-Sylow subgroup of K. Thus, $K \cap H' = K$, so $K \subseteq H'$. Thus, $K = H'$ (because they're the same order). $\square$

Cor: Any subgroup of G that's a p-group is contained in some p-Sylow subgroup.
Proof: Let H be a p-Sylow subgroup. Let K be a p-subgroup. Then there exists a conjugate H' of H s.t. $K \cap H' = K$, so $K \subseteq H'$ is a p-Sylow subgroup. $\square$

Thm: (Third Sylow Theorem) Recall: $|G| = p^e m$. Let s be the number of p-Sylow subgroups. Then $s \mid m$ and $s \equiv 1 \pmod{p}$.

Remark: Let H be a p-Sylow subgroup of G. Then H is a normal subgroup if and only if $s = 1$. Can often prove $s = 1$ using the third Sylow theorem.
Now, we move on to prove the theorems...

First Sylow Theorem Proof

Let $|G| = p^e m$. let $\mathcal{U}$ be the set of all subsets of G of size p^e.
G acts on $\mathcal{U}$: given $g \in G$, $U \in \mathcal{U}$, $g \cdot U = gU = \{gh \mid h \in U\}$.

Prop: $\#\mathcal{U} = \binom{n}{p^e} = \frac{n(n-1)(n-2)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots 1}$. This is a general fact: the number of k-element subsets of a set of size n is $\binom{n}{k}$.

Prop: $p \nmid \#\mathcal{U}$.

Proof: $\#\mathcal{U} = \frac{n(n-1)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots 1}$. If $0 \leq k < p^e$, then the power of p dividing $n-k$ is the same as $p^e - k$, so the p's in the numerator and denominator cancel in each pair.
$\#\mathcal{U} = \#O_1 + \cdots + \#O_r$, where the O_i's are the orbits of G. Since $p \nmid \#\mathcal{U}$, we must have $p \nmid \#O_i$ for some i. Say O_i is the orbit of $U \in \mathcal{U}$. Let $H = \mathrm{stab}(u)$. $\forall h \in H, x \in U$, we have $hx \in U$, so U contains the coset Hx. Thus, U is a union of cosets, so $\#H \mid \#U = p^e$. Thus, $\#H = p^k$ for some $0 \leq k \leq e$. By the counting theorem, $\#O_i \cdot \#\,\mathrm{stab}(u) = \#G = p^e m$. $\#\,\mathrm{stab}(u) = \#H = p^k$, so $\#O_i = p^{e-k} \cdot m$. Since $p \nmid \#O_u$, $e = k$, so H is a p-Sylow. $\square$

Second Sylow Theorem Proof

Let G be a group, $H \subseteq G$ a p-Sylow, and $K \subseteq G$ some other subgroup. We want to show there's a conjugate of H, H', s.t. $H' \cap K$ is a p-Sylow of K.

Consider the action of G on G/H. Recall that the stabilizers for this action are conjugates of H.
$\#G/H = m$, so $p \nmid \#G/H$. Thus, there exists an orbit of K on G/H of cardinality not divisible by p. Say its the orbit of gH. The stabilizer of gH in G is $H' = gHg^{-1}$, so the stabilizer in K is $H' \cap K$.

$H' \cap K \subseteq H'$, so $H' \cap K$ is a p-group. By the counting formula (for the action of K on G/H),

$$\#O_{gH} \cdot \underbrace{\#\,\mathrm{stab}(gH)}_{H' \cap K} = \#K \quad \Rightarrow \quad \#O_{gH} = \frac{\#K}{\#H' \cap K} \quad \Rightarrow \quad p \nmid \frac{\#K}{\#H' \cap K} \quad \Rightarrow \quad H' \cap K \text{ is a } p\text{-Sylow}$$

$\square$

Third Sylow Theorem Proof

Assume $|G| = p^e m$. Let s be the number of p-Sylow subgroups of G. We need to show (1) $s \mid m$ and (2) $s \equiv 1 \pmod{p}$.

(1) Let $\mathcal{H} = \{H_1, \ldots, H_s\}$ be the set of all p-Sylows. G acts on $\mathcal{H}$ by conjugation. This action is transitive by a corollary of the second theorem. Let $H = H_1$. What is $\mathrm{stab}(H)$? It's $\left\{g \mid gHg^{-1} = H\right\} = N$, called the **normalizer** of H. It's clear that $H \subset N$. By the counting formula,

$$\#\underbrace{O_H}_{\mathcal{H}} \cdot \#\underbrace{\mathrm{stab}_H}_{N} = \#G$$

So $s = \frac{\#G}{\#N}$, and $\#G = p^e m$, and $p^e = \#H \mid \#N$, so we conclude $s \mid m$. $\square$

(2) Think about H acting on $\mathcal{H}$ by conjugation. H fixes $H = H_1$. We claim this is the only fixed point. Proof: Suppose H fixes H_i. This implies $H \cdot H_i$ is a subgroup, because for $ab \in HH_i$, $a'b' \in HH_i$, $(ab)(a'b') = \underbrace{(aa')}_{\in H}\underbrace{(a')^{-1}ba'b'}_{\in H_i}$.

Exercise: HH_i is a p-group. Since $H \cdot H_i$ contains H, we must have $H = H \cdot H_i$.
So $H = H_i$, thus $i = 1$.
Now, use the class equation for $H \circlearrowleft \mathcal{H}$.

- O_{H_1} has size 1.
- Every other orbit has size divisible by 1.

Thus, $s = 1 \pmod{p}$. $\square$

Groups of Order 15, 21, 12

Prop: Every group of order 15 is cyclic.

Proof: Let H be a 3-Sylow, K be a 5-Sylow. $H \cong \mathbb{Z}/3\mathbb{Z}$, $K \cong \mathbb{Z}/5\mathbb{Z}$.
Let s be the number of 3-Sylow subgroups. By the third Sylow theorem, $s \mid 5$, so $s = 1$ or $s = 5$, and $s \equiv 1 \pmod 3$. We must have $s = 1$. Thus, H is the unique 3-Sylow, so H is normal.
Let s' be the number of 5-Sylow subgroups. $s' \mid 3$, so $s' = 1$ or $s' = 3$. $s' \equiv 1 \pmod 5$, so $s' = 1$. Thus K is normal.

We claim that $G = HK$. Proof: we know HK is a subgroup, because H is normal, and that it contains H and K. Thus, $3, 5 \mid \#HK$, and $\#HK \mid \#G = 15$. So $\#HK = 15$. Clearly, $H \cap K = \{1\}$, because $\#H \cap K \mid \gcd(\#H, \#K) = 1$. So $G \equiv H \times K \cong \mathbb{Z}/15\mathbb{Z}$. $\square$

Prop: There are 2 groups of order 21 up to isomorphism.

Proof: Let G be a group of order $21 = 3 \cdot 7$. Let s be the number of 7-Sylows. By the third theorem, $s \mid 3$, so $s = 1$ or 3. Because $s \equiv 1 \pmod 7$, $s = 1$. Let H be the unique 7-Sylow (note that it's normal). Let K be a 3-Sylow. Just as in the previous proof, we know $G = H \cdot K$ and $H \cap K = \{1\}$. So $G \cong H \rtimes K$.
The structure of the semi-direct product is determined by the action of K on H.

$$\mathbb{Z}/3\mathbb{Z} \cong K \to \mathrm{Aut}(H) = \mathbb{F}_7^\times \cong \mathbb{Z}/6\mathbb{Z} \overset{\text{CRT}}{\cong} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Thus, we have two groups of order 21 (up to isomorphism):

- $\mathbb{Z}/21\mathbb{Z}$
- $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ where $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ is nontrivial.

$\square$

Prop: There are 5 groups of order 12 up to isomorphism. These groups are

- $\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- A_4 (the alternating group)
- D_6 (the dihedral group)
- One more

Proof: Let H be a 2-Sylow, so $H = \mathbb{Z}/4\mathbb{Z}$ or $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Let K be a 3-Sylow, so $K \cong \mathbb{Z}/3\mathbb{Z}$.
The key claim we will make is that at least one of H or K is normal.
Proof: Let s be the number of 3-Sylows. $s \mid 4$, and $s \equiv 1 \pmod 3$, so $s = 1$ or $s = 4$. If $s = 1$, then K is normal. *I'm missing the remainder of the proof from my notes.*
Thus, we have $G = HK$, with $H \cap K = \{1\}$. So $G \cong H \rtimes K$ or $G \cong K \rtimes H$. $\square$