§7.7 The Sylow Theorems

SEE-luv but we've been saying see-low for too long...

Throughout: $|G| = n$.

Idea: Study an arbitrary finite group ($|G| = n$) by studying subgroups that are of order p^r, where r is the largest power of p that divides n.

$$n = p^r m \qquad p \nmid m.$$

If $H \leq G$ has $|H| = p^r$, then H is a Sylow p-subgroup of G

In other words: A Sylow p-subgroup is a p-group whose index is not divisible by p. ("maximal p-subgroup")

~~1^{st} Sylow theorem~~ Sylow I

If $p \mid |G|$, then G contains a Sylow p-subgroup

Pf.

Let S = set of all subsets of G of order p^r.

Idea: Study $G \curvearrowright S$ induced by left multiplication.

Decompose S into orbits:

$$N := |S| = \sum_{\substack{\text{orbits} \\ \mathcal{O}}} |\mathcal{O}|$$

Claim: $N \not\equiv 0 \pmod p$

$$N := |S| = \binom{n}{p^r} = \frac{n!}{(n-p^r)!\,(p^r)!} = \frac{n(n-1)\cdots(n-p^r+1)}{p^r(p^r-1)\cdots 2\cdot 1}$$

By studying the terms mod p, one can show that $p \nmid N$.

$\Rightarrow$ At least one orbit $\mathcal{O}_{[U]}$ has order that is not divisible by p. We focus now on this subset $[U] \in S$.

Now consider the stabilizer $G_{[U]}$. Write counting formula now w/ ②

Claim: $|G_{[U]}| \mid |U|$ Participation slip: Complete this proof.

Let $H = G_{[U]}$. Consider the restricted action $H \curvearrowright \mathcal{U}$.

(H is the stabilizer of $\mathcal{U} \Rightarrow$ permutes the elements of $\mathcal{U}$.)

For $u \in \mathcal{U}$, the orbit of u is Hu, a right coset of H.

$\Rightarrow \mathcal{U}$ is partitioned by right cosets of H. (pause)

These are all the same size.

$\Rightarrow |H| = |G_{[U]}| \mid |U| = p^r \Rightarrow |G_{[U]}| \equiv 0 \bmod p.$

Now use counting formula:

$$\underbrace{p^r}_{\equiv 0 \bmod p}\ \underbrace{m}_{\not\equiv 0 \bmod p} = |G| = \underbrace{|G_{[u]}|}_{\overset{?}{\equiv} 0 \bmod p} \cdot \underbrace{|O_{[u]}|}_{\not\equiv 0 \bmod p}$$

$\Rightarrow |O_{[u]}| = m$

$\Rightarrow |G_{[u]}| = p^r$. We found it!

<u>Cor. to Sylow I.</u> A finite group whose order is divisible by a prime p contains an element of order p.

Let's just think through why... $|H| = p^r \rightsquigarrow$ find elt. //

e.g. If $|G| = 6$, the elements can't all have order 1 or 2.

There are 2 more Sylow theorems, and their proofs are similar in length + technique: considering group actions. These use the conjugation action though.

(Good practice to see how well you understand conj action on group to work through the proofs.)

2nd ~~Sylow Theorem~~ Sylow II Let G be finite group w/ $p \mid n = |G|$.

(a) all Sylow p-subgroups are conjugate subgroups.

ie the conjugation action of G on the set $\{$Sylow p-subgroups of $G\}$ is transitive.

(b) Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

(Note if $|H| = p^r \Rightarrow |gHg^{-1}| = p^r$ as well.)

Cor. G has exactly one Sylow p-subgroup $H \Leftrightarrow$ that H is normal in G. (why?)

3rd ~~Sylow theorem~~ Sylow III (with same setup as throughout:)

$|G| = n = p^r m$, $p \nmid m$. Let $s = \#$ Sylow p-subgroups

Then $s \mid m$, and $s \equiv 1 \pmod{p}$.

Q Why would this be useful?

Example / Prop. Every group of order 15 is cyclic.

($\Rightarrow$ there's only one isom class!)

Pf.

Let $|G| = 15 = 3 \times 5$.

Let $s_3 = \#$ Sylow 3-subgroups.

$\text{III} \Rightarrow \quad s_3 \mid 5, \; s_3 \equiv 1 \pmod 3 \qquad \Rightarrow s_3 = 1.$

$\Rightarrow$ the unique Sylow 3 subgroup H is normal.

Let $s_5 = \#$ Sylow 5 subgroups

$\text{III} \Rightarrow \quad s_5 \mid 3, \; s_5 \equiv 1 \pmod 5$

$\Rightarrow \exists! \; K \leq G, \; |K| = 5, \; K \trianglelefteq G.$

Since $|H| = 3$ & $|K| = 5$, $H \cap K = \{1\}$.

(& HK must have order 15 $\Rightarrow$ $HK = G$).

Prop 2.11.4 $\Rightarrow G \cong H \times K \cong C_3 \times C_5 \cong C_{15}$. $\blacksquare$