(101)

Note that whenever s_p (= # Sylow p-Subgroups) = 1,
then Sylow's 2nd Thm. implies that the unique Sylow p-subgroup P must be normal, i.e. $P \lhd G$, since $\forall g \in G$, $|gPg^{-1}| = |P|$

$\Rightarrow gPg^{-1}$ is a Sylow p-subgroup

$\Rightarrow gPg^{-1} = P$

COROLLARY: When $|G| = pq$ with p, q primes, $p < q$ and $p \nmid q-1$, then $G \cong (\mathbb{Z}/pq\mathbb{Z})^+$

i.e. G is cyclic.

EXAMPLES: (1) $|G| = 15 = \overset{p}{\overset{\shortparallel}{3}} \cdot \overset{q}{\overset{\shortparallel}{5}}$ $(3 \nmid 5-1=4)$ $\Big\} \Rightarrow G \cong (\mathbb{Z}/15\mathbb{Z})^+$

(2) But $|G| = 21 = \overset{p}{\overset{\shortparallel}{3}} \cdot \overset{q}{\overset{\shortparallel}{7}}$ does not imply $G \cong (\mathbb{Z}/21\mathbb{Z})^+$;
$(3 \mid 7-1=6)$

(Artin analyzes the other possibility for $|G|=21$ as part of his PROP. 7.7.7)

11/2/2018

proof of COROLLARY: Note Sylow's 3rd $\Rightarrow s_q \mid p \Rightarrow s_q = 1$ or p
and $s_q \equiv 1 \bmod q \Rightarrow \boxed{s_q = 1}$
(since $p < q$)

Also Sylow's 3rd $\Rightarrow s_p \mid q \Rightarrow s_p = 1$ or q
and $s_p \equiv 1 \bmod p$
i.e. p divides $s_p - 1 \Rightarrow \boxed{s_p = 1}$
since $p \nmid q-1$

Hence there are unique Sylow p-subgroups P and Sylow q-subgroups Q, with $P \lhd G$, $Q \lhd G$

- One way to finish the proof argues $P \times Q \to PQ = G$, $(h, k) \mapsto hk$ is an isomorphism from this.
- Another way uses Sylow's 2nd to say every element of order p must lie in P, of order q must lie in Q, and since $|G| = pq > p+q-1 = |P \cup Q|$, there must be elements of order pq. ∎

(102) Let's prove the Sylow Theorems, using lots of group actions!

<u>proof of Sylow's 1st Thm:</u> Given $|G| = p^e \cdot m$, $p \nmid m$, let's consider the action of G on $S := \{\text{all } p^e\text{-element subsets } \mathcal{U} \text{ of } G\}$ via <u>left</u>-translation i.e. $g * \underbrace{\mathcal{U}}_{\{u_1, u_2, \ldots, u_{p^e}\}} := \{gu_1, gu_2, \ldots, gu_{p^e}\}$

We'll show eventually that one of the <u>stabilizers</u> $G_{\mathcal{U}_0}$ is a Sylow p-subgroup, i.e. $|G_{\mathcal{U}_0}| = p^e$.

To this end consider the orbit decomposition

$$S = \bigsqcup_{\substack{G\text{-orbits } \mathcal{O}_u \\ \text{on } S}} \mathcal{O}_u$$

and

$$|S| = \sum_{\substack{G\text{-orbits } \mathcal{O}_u \\ \text{on } S}} |\mathcal{O}_u| = \sum_{\substack{G\text{-orbits } \mathcal{O}_u \\ \text{on } S}} \frac{|G|}{|G_u|} = \sum_{\substack{G\text{-orbits } \mathcal{O}_u \\ \text{on } S}} \underbrace{\frac{p^e m}{|G_u|}}_{\substack{\equiv 0 \bmod p \\ \text{unless} \\ p^e \text{ divides } |G_u|}}$$

$$|S| = \#\left\{\begin{matrix} p^e\text{-element} \\ \text{subsets } \mathcal{U} \\ \text{of } G \end{matrix}\right\} = \binom{p^e m}{p^e}$$

where $\binom{n}{k}$ = binomial coefficient $= \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots(1)}$

(A number theory LEMMA: $\binom{p^e m}{p^e} \not\equiv 0 \bmod p$ for $e \geq 1$, i.e. $p \nmid \binom{p^e m}{p^e}$)

<u>Proof:</u>

$$\binom{p^e m}{p^e} = \frac{(p^e m)(p^e m-1)(p^e m-2)\cdots(p^e m-j)\cdots(p^e m-(p^e-1))}{(p^e)(p^e-1)(p^e-2)\cdots(p^e-j)\cdots(p^e-(p^e-1))}$$

has p dividing the numerator and denominator the <u>exact</u> <u>same number of times</u> since the highest power p^ℓ dividing $p^e m - j$ is the same for $p^e - j$ via this calculation: write $j = p^\ell m'$ with $m' \not\equiv 0 \bmod p$ (so $\ell < e$ since $1 \leq j \leq p^e$)

and then $p^e m - j = p^e m - p^\ell m' = p^\ell(\underbrace{p^{e-\ell} m}_{\equiv 0 \bmod p} - \underbrace{m'}_{\not\equiv 0 \bmod p})$

$$p^e - j = p^e - p^\ell m' = p^\ell(\underbrace{p^{e-\ell}}_{\equiv 0 \bmod p} - \underbrace{m'}_{\not\equiv 0 \bmod p}) \quad \blacksquare$$

e.g. $\binom{2^2 \cdot 15}{2^2} = \binom{60}{4}$

$= \frac{\overset{15}{60} \cdot 59 \cdot \overset{29}{58} \cdot 57}{4 \cdot 3 \cdot 2 \cdot 1}$

= odd!

(103)

CONCLUSION: At least one G-orbit $\mathcal{O}_{U_0}$ must have p^e dividing $|G_{U_0}|$.

On the other hand, one always has $|G_{U_0}|$ dividing $|U_0| = p^e$ because G_{U_0} acts on $U_0 = \{u_1, u_2, \ldots, u_{p^e}\}$ via left-translation

and so G_{U_0} decomposes U_0 into G_{U_0}-orbits which are cosets $G_{U_0} \cdot u_i$ having the same size $|G_{U_0} \cdot u_i| = |G_{U_0}|$.

Hence p^e divides $|G_{U_0}|$ which divides $|U_0| = p^e$, so $|G_{U_0}| = p^e$

i.e. G_{U_0} is a Sylow p-subgroup. ∎

11/5/2018 >

proof of Sylow's 2nd Thm: Given any p-subgroup $H < G$, if we can show $H < gPg^{-1}$ for some particular Sylow p-subgroup $P < G$ then this will show both parts (take $H = P'$ any other Sylow-p-subgroup to conclude $P' = gPg^{-1}$).

Consider H acting on $S := \{\text{left cosets } gP : g \in G\} = G/P$ via left-translation, i.e. $h * gP := hgP$

As usual,
$$|G/P| = |S| = \sum_{\substack{H\text{-orbits}\\ \text{in } S}} |\mathcal{O}_s| = \sum_{\substack{H\text{-orbits } \mathcal{O}_s\\ \text{in } S}} \underbrace{\frac{|H|}{|H_s|}}$$

$\equiv 0 \bmod p$ unless $H_s = H$ (since H is a p-group)

$$|G/P| = \frac{p^e m}{p^e} = m \not\equiv 0 \bmod p$$

Hence $\exists$ some $s \in S = G/P$ with $H_s = H$,

i.e. $\exists$ some coset gP with $hgP = gP \quad \forall h \in H$

$g^{-1}hgP = P$

$g^{-1}hg \in P$

$h \in gPg^{-1}$, i.e. $H < gPg^{-1}$ ∎