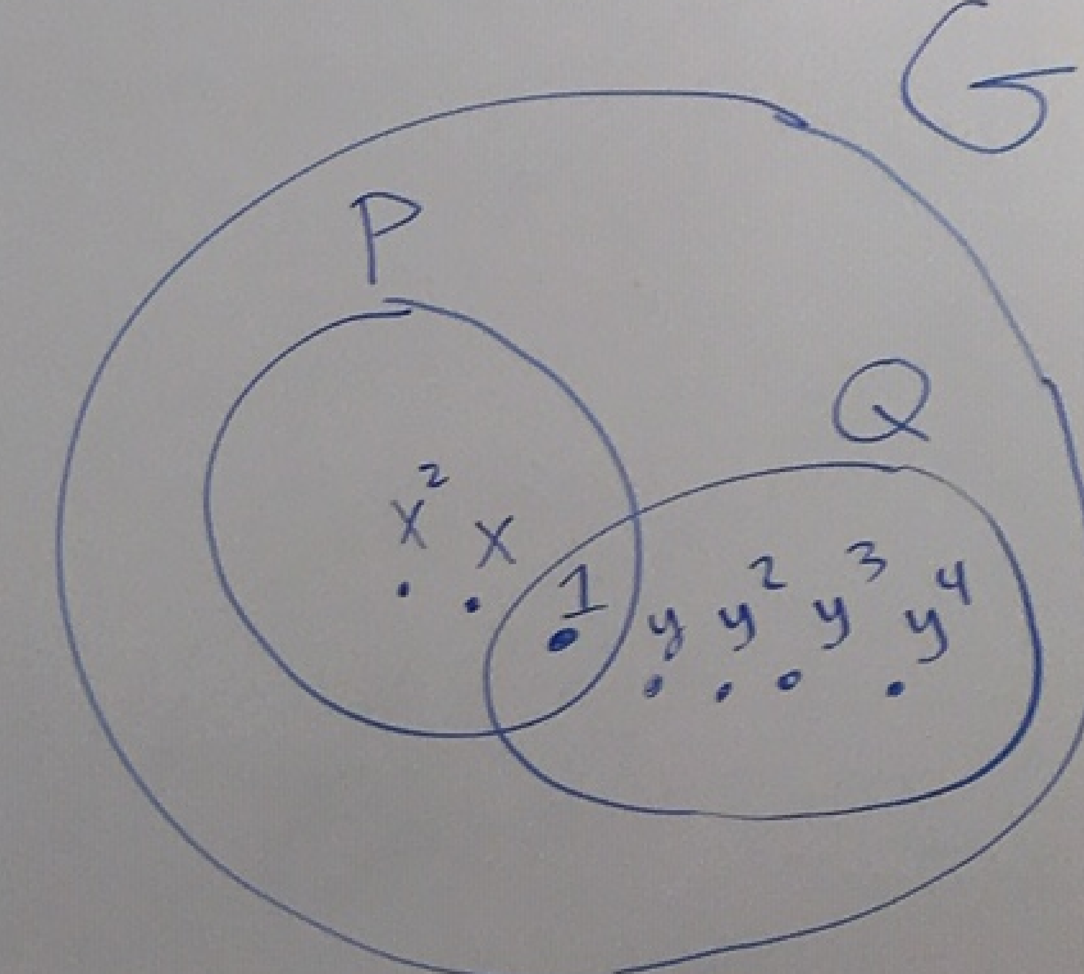
11/14
Thursday

T	R
	11/14 – Applications of Sylow } * – Simple group – Fund. Th. Finitly Generated Abelian group (FTFGAG)
11/19 – FTFGAG – commutator G'	11/21 Semi-direct product
12/2 Problems	12/4 Problems
	12/12 Final

Ex: Suppose G is a group of size 15.
Prove that G is cyclic.

proof: $|G| = 3 \cdot 5$

By Sylow's Theorem there exists a subgroup P with $|P| = 3$.
By Sylow's theorem there exists a subgroup Q with $|Q| = 5$.
Since 3 is prime, P is cyclic, so $P = \langle x \rangle$ for some $x \in G$.
Since 5 is prime, Q is cyclic, so $Q = \langle y \rangle$ for some $y \in G$.
By Sylow's theorem, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 5$.
So, $n_3 = 1, 4, 7, 10, 13, \ldots$ and $n_3 \mid 5$.
Thus, $n_3 = 1$. (There is only 1 subgroup of size 3, it's P)
So, $P \trianglelefteq G$.



$n_3 = $ # of sylow 3-subgroups

$n_5 = $ # of sylow 5-subgroups

$n_3 = 1$ iff $gPg^{-1} = P$ $\forall g \in G$

By Sylow's theorem, $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 3$.

So, $n_5 = 1, 6, 11, 16, \ldots$ and $n_5 \mid 3$.

Thus, $n_5 = 1$. (There is only one subgroup of size 5, it's Q)

Therefore, $Q \trianglelefteq G$.

<u>Claim 1 : $xy = yx$</u>

Since $P \leq G$ and $Q \leq G$ we get $P \cap Q \leq G$.

Since $P \cap Q \leq P$ and $P \cap Q \leq Q$ by Lagrange,

$|P \cap Q|$ divides $|P| = 3$ and $|Q| = 5$.

Thus, $|P \cap Q| = 1$.

So, $P \cap Q = \{1\}$.

Since $P \trianglelefteq G$ and $x^{-1} \in P$ we get $yx^{-1}y^{-1} \in P$.

Since $x \in P$ and $yx^{-1}y^{-1} \in P$ we get $\boxed{xyx^{-1}y^{-1} \in P}$

Since $Q \trianglelefteq G$ and $y \in Q$ we get $xyx^{-1} \in Q$.

Since $xyx^{-1} \in Q$ and $y^{-1} \in Q$ we get $\boxed{xyx^{-1}y^{-1} \in Q}$.

So, $xyx^{-1}y^{-1} \in P \cap Q$. Thus, $xyx^{-1}y^{-1} = 1$. So, $xy = yx$. $\boxed{\text{Claim 1}}$

$^{-1} \in P$

$y^{-1} \in P$

$\in Q$

$Q.$

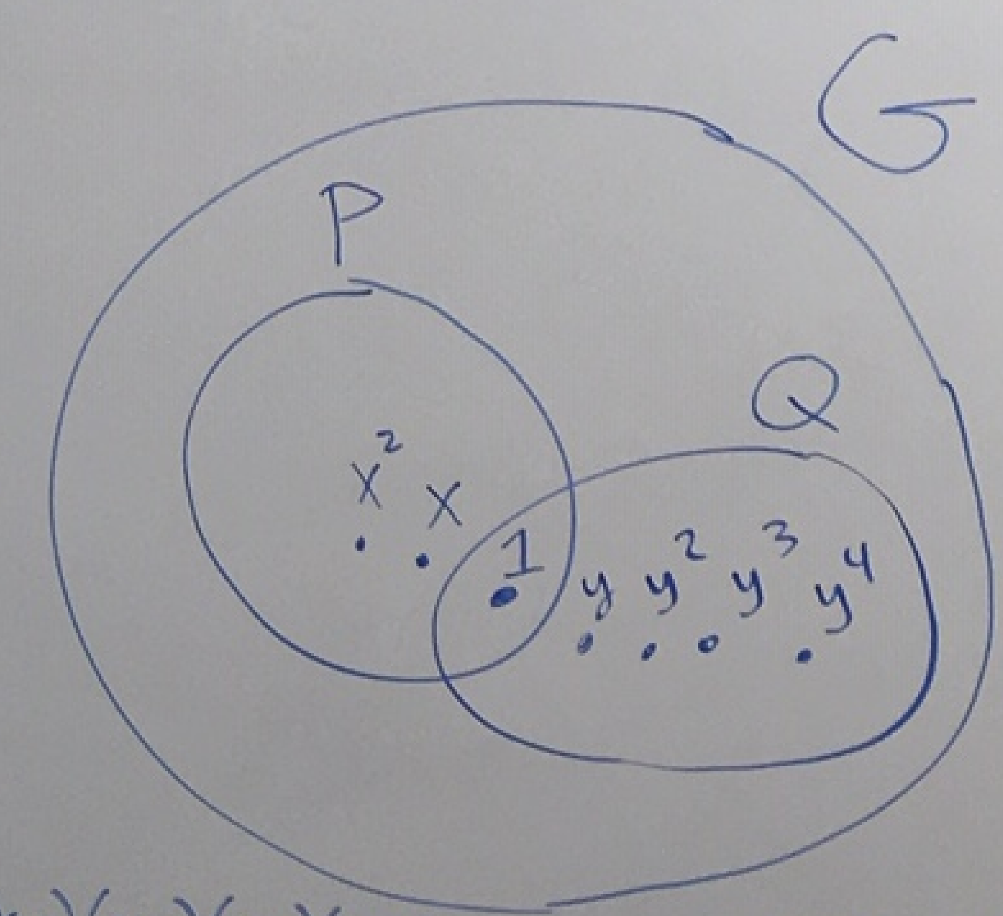
$\in Q$

$Q.$

$yx.$ Claim 1

Claim 2: $|xy| = 15$

Since $|G| = 15$, we know $|xy|$ divides 15.
So, $|xy| = 1, 3, 5,$ or 15.



$|xy| \neq 1$:

Suppose $(xy)^1 = 1$.
Then $x = y^{-1} \in Q$.
So, $x \in P \cap Q = \{1\}$.
But then $x = 1$, which is nonsense!!
(since x has order 3)

$|xy| \neq 3$:

We have

$$(xy)^3 = (xy)(xy)(xy) \underset{\text{Claim 1}}{=} x^3 y^3 = 1 \cdot y^3 = y^3 \neq 1$$

y has order 5

$|xy| \neq 5$:

We have

$$(xy)^5 = (xy)(xy)(xy)(xy)(xy) \underset{\text{Claim 1}}{=} x^5 y^5 = x^5 \cdot 1 = x^2 \neq 1$$

x has order 3

Therefore, $|xy| = 15$ and $G = \langle xy \rangle$. $\blacksquare$

Ex: Let G be a group of size $255 = 3 \cdot 5 \cdot 17$ is abelian.

proof: By Sylow's theorem, there exists a subgroup P of G of size 17.
And $n_{17} \equiv 1 \pmod{17}$ and $n_{17} \mid 3 \cdot 5$.

So, $n_{17} = 1, 18, \ldots$ and $n_{17} \mid 15$.
Thus, $n_{17} = 1$ and so $P \trianglelefteq G$.

Previous Theorem: Since $P \trianglelefteq G$ we have that $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$.

Since $|P| = 17$ and 17 is prime $P \cong \mathbb{Z}_{17}$.
So, $\mathrm{Aut}(P) \cong \mathrm{Aut}(\mathbb{Z}_{17})$
$\cong \mathbb{Z}_{17}^{\times}$
Thus, $|\mathrm{Aut}(P)| = |\mathbb{Z}_{17}^{\times}| = 16$

If p is prime $\mathbb{Z}_p^{\times} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ and has size $p-1$

So, $|G/…$
But also,
Thus, $|G/C_G…$
So, $G = C_G…$
That is, $gp=…$
In particular, …
So, $|P| = 1…$
but also

So, $\left|G/C_G(P)\right|$ divides $|\mathrm{Aut}(P)| = 16$.

But also, $\left|G/C_G(P)\right| = \dfrac{|G|}{|C_G(P)|}$ divides $|G| = 255$.

Thus, $\left|G/C_G(P)\right| = 1$.

So, $G = C_G(P) = \{g \in G \mid gp = pg \text{ for all } p \in P\}$

That is, $gp = pg$ for all $p \in P$ and $g \in G$.

In particular, $P \leq Z(G)$.

So, $|P| = 17$ divides $|Z(G)|$

but also $|Z(G)|$ divides $|G| = 255 = 3 \cdot 5 \cdot 17$

So, $|Z(G)| = 17,\ 3 \cdot 17,\ 5 \cdot 17$, or $3 \cdot 5 \cdot 17$.

If $|Z(G)| = 17$, then $\left|G/Z(G)\right| = \frac{255}{17} = 15$.

So, $G/Z(G)$ is cyclic by the previous example.

By a HW problem, since $G/Z(G)$ is cyclic, G is abelian.

So, $G = Z(G)$. Contradiction. (This implies $|G| = |Z(G)| = 17$.)

If $|Z(G)| = 3 \cdot 17$, then $\left|G/Z(G)\right| = \frac{255}{3 \cdot 17} = 5$.

So, since 5 is prime, $G/Z(G)$ is cyclic and again we get $G = Z(G)$. Contradiction. (This implies $|G| = 3 \cdot 17$)

If $|Z(G)| = 5 \cdot 17$, then $\left|G/Z(G)\right| = \frac{255}{5 \cdot 17} = 3$.

So, since 3 is prime, $G/Z(G)$ is cyclic and we get $G = Z(G)$. Contradiction. (This implies $|G| = 5 \cdot 17$)

So, $|Z(G)| = 3 \cdot 5 \cdot 17 = 255$ and $G = Z(G)$.

So G is abelian. $\square$