Math 122 Wednesday, November 2

If G acts on a set S then it acts on the power set $P(S) = \{\text{all subsets } T \subset S\}$
$\#S = n \Rightarrow \#P(S) = 2^n$ even for infinite sets $S < P(S) < P(P(S))$ etc
$g(T) = T' \subset S$

ex G acts on $G = S$ by conjugation $s \mapsto gsg^{-1} = g(s)$
so also acts on subgroups $H \subset G$. Can check $gHg^{-1} = H'$ another subgroup.
O_H = subgroups H' conjugate to H.

$G > G_H = \{g \in G : gHg^{-1} = H\} =: N_G(H)$ the normalizer of H in G.
Clear that $H \triangleleft N_G(H)$. $H \triangleleft G \Leftrightarrow N_G(H) = G$
The normalizer is the largest subgroup of G in which H is normal.

Note: $\#(G/N_G(H)) = \#$ of conjugate subgroups H' of H in G (divides the index of H in G)
As always $G/G_H \cong O_H$ as a set.

$H \subset G$ a finite group. $\#H$ divides $\#G = \#H \cdot \#(G/H)$. If d divides $\#G$ is there a subgroup $H \subset G$ of order d? No. $G = A_4$ $\#G = 12$ but no subgroup of order 6.
But answer is yes if $d = p^a$ (Sylow)

Thm (Sylow) Assume the order of G has the form $\#G = p^n m$, m prime to p.
1. There is a subgroup H of order p^n ← these are called Sylow-p subgroups.
(In fact there is an H of order p^a for any $a \leq n$. Proof on homework.)
2. If $K < G$ is a p-subgroup then K is conjugate to a subgroup of H ($gKg^{-1} \subset H$).
If K is a Sylow-p subgroup then K is conjugate to H. (Any two Sylow-p subgroups of G are conjugate).
3. The number N of Sylow-p subgroups satisfies $N \equiv 1 \pmod{p}$ and N divides $m = \#G/\#H$

ex $G = GL_n(\mathbb{Z}/p\mathbb{Z})$ has order $(p^n - 1) \cdots (p^n - p^{n-1})$ by considering how many choices there are for each column. So $\#G = p^{\frac{n(n-1)}{2}}(p^n - 1) \cdots (p - 1)$. Subgroup $H = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$ has this order. For $G = S_n$ this is much harder.

Pf of 1) Let G act by left multiplication on the set S of subsets T of G of order p^n.
Then $\#S = \binom{\#G}{p^n} = \dfrac{p^n m (p^n m - 1) \cdots (p^n m - k) \cdots (p^n m - p^n + 1)}{p^n (p^n - 1) \cdots (p^n - k) \cdots 1}$ Note p^a divides $p^n m - k$ iff p^a divides $p^n - k$ so $\#S$ is prime to p.
I will prove that there is at least one $T \in S$ where $\#G_T = p^n$. Then take $H = G_T$.
Apply our counting formula: $\#S = \sum_{\text{orbits}} \#O_T = \sum_{\text{orbits}} \#G/\#G_T$. As the LHS is prime to p, there is at least one T such that $\#G/\#G_T$ is also prime to $p \Rightarrow p^n$ divides $\#G_T$.
But we know $\#G_T \leq p^n$ for all $T \in S$ because for $t \in T$ there are only p^n options for $gt \in T$.
Hence $\#G_T = p^n$ so $H = G_T$ is a Sylow-p subgroup.

Pf of 2) Let H be a Sylow-p subgroup by left multiplication on $S = G/H$ of order m. Note this action is transitive. $\text{Stabalizer}_{gH} = gHg^{-1} \supset K \Rightarrow H \supset g^{-1}Kg$. Now let K be a subgroup of order p^a and restrict the action of G on S (of order prime to p) to K. The orbits of K on G/H are the double cosets KgH and the action is no longer necessarily transitive. By the counting formula $\#S = \sum_{\text{orbits of } K} \#K/\#K_{gH}$. Each $\#K/\#K_{gH}$ must divide $\#K = p^a$ but LHS is prime to p so at least one $\#K/\#K_{gH} = 1 \Rightarrow K_{gH} = K \Rightarrow K$ fixes some coset $gH \Rightarrow K \subset gHg^{-1} = \text{Stab}_{gH}$ under action of $G \Rightarrow g^{-1}Kg \subset H$ as desired.

Principle If a p-group G acts on a set of order prime to p it has a fixed point s (i.e. $G_s = G$). We'll use this again.

Pf of 3) By 2 every Sylow-p subgroup $H' = gHg^{-1}$ is conjugate to G. Thus G acts transitively by conjugation on set of Sylow-p subgroups. $\#S = N = \#$ conjugates of H $= \#G/\#N_G(H)$ divides m as $\underbrace{H \trianglelefteq N_G(H)}_{m} \subset G$. Now restrict this action to H. Then it has a fixed point H but there are no other fixed points. Indeed suppose H' were a fixed point. Then $hH'h^{-1} = H'$ for all $h \in H$. Thus $H \subset N(H') \subset G$ is Sylow-p subgroup of $N(H')$. But H' is also a Sylow-p subgroup of $N(H')$ but the only conjugate of H' in $N(H')$ is H' (as $H' \trianglelefteq N(H')$) contradicting $2' \Rightarrow H' = H$. Hence by counting formula $\#S = \underbrace{1}_{\text{fixed point}} + \sum_{\text{Sylow-}p\text{'s} \neq H} \#H/\#H_{H'}$ and each of these other terms is a power of p. So $\#S = N \equiv 1 \pmod{p}$.

Cor If $\#G = 15 = 3 \cdot 5$ then G is cyclic.

Pf: There is a Sylow-3 subgroup H of order 3. How many? Number must divide 5 and be congruent to 1 mod 3 $\Rightarrow \exists$ only one and $H \trianglelefteq G$. Similarly $\exists$ a Sylow-5 subgroup K of order 5. Number of these must divide 3 and equal 1 mod 5 $\Rightarrow \exists$ only one and $K \trianglelefteq G$. In particular, there is one element in G of order 1, exactly two elements of order 3 and exactly 4 elements of order 5 (otherwise there would be more Sylow-p subgroups). So the other elements must have order $15 \Rightarrow G$ is cyclic.