1. $H < G$ $|G:H| = n > 1$ prove

$K \trianglelefteq G$ $|G:K| \mid n!$ or $G \lesssim S_n$

Let $\Omega = \{Hg_1, Hg_2, \ldots, Hg_n\}$ where $g_1 = e$

and Ω is the set of all the cosets of H in G

Let $\varphi: G \longrightarrow Sym(\Omega)$

$g \longmapsto \rho(g): \Omega \longrightarrow \Omega$

$Hg_i \longmapsto Hg_i g$, φ is a group homomorphism

$\ker\varphi = \bigcap_{g \in G} g^{-1}Hg$

Let $K = \ker\varphi$. if K is nontrivial, then $K \trianglelefteq G$

and since $G/K \lesssim Sym(\Omega) \Rightarrow [G:K] \mid n!$

If K is trivial then $G \lesssim Sym(\Omega) \simeq S_n$

2. $p \mid |G|$, the least prime. If $H < G$, $[G:H] = p$ then $H \trianglelefteq G$

By 1. Let $\varphi: G \longrightarrow S_p$

$[G: \ker\varphi] \mid p!$

p is the least prime shows $[G:\ker\varphi] = p$

Since $\ker\varphi = \bigcap_{g \in G} g^{-1}Hg \Rightarrow |\ker\varphi| \leq |H|$

$\Rightarrow [G:\ker\varphi] = [G:H] \Rightarrow |\ker\varphi| = |H|$

$\Rightarrow \forall g \in G$ $g^{-1}Hg = H \Rightarrow H = \ker\varphi \trianglelefteq G$

3. identify $|G| = p^2$

1°. if $\exists g \in G$ s.t. $o(g) = p^2$ then $G = \mathbb{Z}_{p^2}$

2° if $\forall g \in G$ s.t. $o(g) \neq p^2$ since $o(g) \mid |G| \Rightarrow g = e$ or $o(g) = p$

Since $Z(G) \neq 1 \Rightarrow Z(G) = \mathbb{Z}_p$

$\Rightarrow |G/\mathbb{Z}_p| = p \Rightarrow G/\mathbb{Z}_p = \mathbb{Z}_p$

$\Rightarrow G$ is abelian $\Rightarrow G = \mathbb{Z}_p \times \mathbb{Z}_p$

4. Prove every p-group G is solvable.

Lemma: Let G be a p-group. then $Z(G) \neq 1$.

Consider $G \curvearrowright G$ by conjugate.

$$|G| = \sum_{g \in G} [G : \mathrm{Stab}(g)]$$

and different g in different conjugacy classes

Since $p \mid |G|$ and $\exists e \in G$ s.t. $[G : \mathrm{Stab}(e)] = 1$.

$\Rightarrow \exists h \in G$ s.t. $p \nmid [G : \mathrm{Stab}(h)]$

but if $\mathrm{Stab}(h) \neq G \Rightarrow p \mid [G : \mathrm{Stab}(h)] \Rightarrow \mathrm{Stab}(h) = G$

$\Rightarrow h \in Z(G)$. $\Rightarrow Z(G)$ is non-trivial.

Back to this exercise.

If $|G| = p \Rightarrow G = \mathbb{Z}_p$, solvable.

Suppose for all $1 \leq n < k$. $|G| = p^n$. G is slovable.

Let $|G| = p^k$, $Z(G) \neq 1 \Rightarrow$ $|G/Z(G)| < p^k$ and

$|G/Z(G)|$ also p-group

$\Rightarrow$ by induction hypothesis $G/Z(G)$ is solvable

and $Z(G)$ is abelian so $Z(G)$ is also solvable

$\Rightarrow$ G is solvable

$\Rightarrow$ all p-group G are solvable.

5. (1) $|G| = pq$.

$n_p \equiv 1 \mod p$ and $n_p \mid q$ $\Rightarrow$ $n_p = 1$ or q

If $n_p = 1$. done.

If $n_p = q$

$n_q \equiv 1 \mod q$, $n_q \mid p$ $\Rightarrow$ $n_q = 1$ or p

If $n_q = 1$ done

If $n_q = p$

Now count elements in G.

$q(p-1) + p(q-1) + 1 = 2pq - p - q + 1 > pq$. contradiction.

$\Rightarrow$ G is not simple.

(2). $|G| = p^2 q$

$n_p \equiv 1 \mod p$ $n_p \mid q$ $\Rightarrow$ $n_p = 1$ or q

If $n_p = 1$. done

If $n_p = q$.

$n_q \equiv 1 \mod q$, $n_q = 1$ or p or p^2

If $n_q = 1$. done.

If $n_q = p^2$

There are $p^2(q-1)$ elements in some Sylow q-subgroups of G and the last p^2 elements can not form q sylow p-subgroups of G (hint. if $P \in Syl_p(G)$, $|P| = p^2$)

If $n_q = p$ then $p \equiv 1 \mod q \Rightarrow p > q$.

But $n_p = q$ and $q \equiv 1 \mod p \Rightarrow$ contradiction!

(3) $|G| = pqr$

WLOG. assume $p > q > r$.

$n_p \equiv 1 \mod p$. $n_p \mid qr$ shows $n_p = 1$ or $n_p = qr$

if $n_p = 1$. done.

if $n_p = qr$

$n_q \equiv 1 \mod q$. $n_q \mid pr$ shows $n_q = 1$ or p or pr

if $n_q = 1$. done. , suppose at least $n_q = p$

$n_r \equiv 1 \mod r$. $n_r \mid pq$. $n_r = 1$ or q or p or pq

if $n_r = 1$. done. suppose at least $n_r = q$

Count the elements.

$qr(p-1)+p(q-1)+q(r-1)$

$= pqr - \cancel{qr} + pq - p + \cancel{qr} - 1$

$= pqr + p(q-1) - 1 > pqr$ contradiction!

6. if $|G| = 56$ the G not simple.

$|G| = 56 = 2^3 \cdot 7$

$n_7 \equiv 1 \bmod 7$, $n_7 \mid 8 \Rightarrow n_7 = 1$ or 8

Suppose $n_7 = 8$

$n_2 \equiv 1 \bmod 2$, $n_2 \mid 7 \Rightarrow n_2 = 1$ or 7

Suppose $n_2 = 7$

Since there are $8(7-1) = 48$ element in some Sylow 7-subgrps

only 8 elements left. can't form 7 sylow-2 subgrp.

$\Rightarrow$ contradiction.

7. $|G| = p^3$ non-abelian. prove $G' = Z(G)$

Since $|Z(G)| \neq 1$, $|Z(G)| = p$ or p^2 or p^3

if $|Z(G)| = p^3$ then G is abelian

if $|Z(G)| = p^2$ then $G/Z(G)$ is cyclic $\Rightarrow$ G is abelian.

$\Rightarrow$ $|Z(G)| = p$, and $|G/Z(G)| = p^2$, $G/Z(G)$ is abelian.

it shows $G' \leq Z(G)$ but $G' \neq 1$ (if $G'=1$, G is abelian)

$\Rightarrow$ $G' = Z(G)$

8. $N \lhd G$, $|N| = p$. $N \leq Z(G)$

Let $G \curvearrowright N$ by conjugace.

consider class equation.

$$|N| = \sum [G : stab(n)], \quad n \in N$$

for all $[G : Stab(n)]$ either $[G : stab(n)] = 1$ or

$p \mid [G : stab(n)]$

Since $e \in N$, $[G : stab(e)] = [G : G] = 1$

it shows $\forall n \in N$, $[G : stab(n)] = 1 \Rightarrow \forall n \in N, \forall g \in G$

$$g^{-1} n g = n \Rightarrow N \leq Z(G)$$

9. $G = N N_G(P)$.

Consider $G \curvearrowright Syl_p(N) = \{P = P_1, \ldots, P_s\}$ by conjugace.

this action is transitive.

$\forall g \in G$. suppose. $g^{-1} P g = P_i$

also $\exists$ $n \in N$ s.t $n^{-1} P n = P_i$.

$\Rightarrow$ $g^{-1} P g = n^{-1} P n \Rightarrow (g n^{-1})^{-1} P \, g n^{-1} = P$

$\Rightarrow \quad gn^{-1} \in N_G(P)$

$\Rightarrow \quad G = N_G(P)\,N = N\,N_G(P)$

10. $|G| < \infty$. $P_2 \in Syl_2(G)$. P_2 is cyclic

prove $\exists\, H < G$ s.t. $[G:H] = 2$.

Consider Cayley theorem. suppose $|G| = n$

By right regular permutation representation

embedding G into S_n $\quad G \hookrightarrow S_n$

Let $P_2 = \langle a \rangle$ then $a \longmapsto \underbrace{(\qquad\qquad)}_{2^k\text{-cycle}}$

2^k-cycle, a odd permu.

$\Rightarrow$ all preimage of even permu. forms a subgroup of G

which index is two.

I will introduce "p-nilpotent group" to you in exercise

class, and you will find this exercise is trivial.

11. $\vec{G}$: $\vec{g} : x \longmapsto x g^{-1}$

$\check{G}$: $\check{g} : x \longmapsto g x$

$\hat{G}$: $\hat{g} : x \longrightarrow g x g^{-1}$

12. $\mathrm{Aut}(\mathbb{Z}_p^d) \simeq GL_d(\mathbb{Z}_p)$

13. $\mathrm{Aut}(D_{2n})$.

$\mathrm{Aut}(D_{2n}) \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$

$\mathbb{Z}_n^*$ means $\mathrm{Aut}(\mathbb{Z}_n)$.