Question 1

Show subgroups and quotient groups of nilpotent groups are nilpotent

Solution: Let G be a nilpotent group and H be a subgroup of G. Then there is a chain

$$G = G_0 > G_1 > \cdots > G_n = \{ e \}$$

such the commutator $[x, y] \in G_{i+1}$ for all $x \in G$, $y \in G_i$ by the definition of a nilpotent group. Then define $H_i = H \cap G_i$, making the chain

$$H = H_0 > H_1 > \cdots > H_n = \{ e \}$$

. Now for $x \in H, y \in H_i$, we have $x, y \in H$ since $H_i < H$ which means that $[x, y] \in H$. And since $x \in G$ and $y \in G_i$ also holds, then $[x, y] \in G_{i+1}$ by the property of nilpotent group G. Thus, $[x, y] \in H \cap G_{i+1} = H_{i+1}$. Which proves H is nilpotent.

Now, let N be a normal subgroup of G, and consider $N \lhd G_{i+1}N \lhd G_iN$ by the property of normal subgroup. Which makes $G_{i+1}N/N$ the set $\{ gN \mid g \in G_{i+1} \}$ which is a subgroup of G_iN/N Therefore, a chain $G/N = G_0N/N > G_1N/N > \cdots > G_nN/N = \{ N \}$ is constructed. Moreover, for $x \in G/N, y \in G_iN/N$, we have $x = gN$, $y = g_iN$ for some $g \in G$, $g_i \in G_i$. Therefore,

$$[x, y] = xyx^{-1}y^{-1} = (gN)(g_iN)(gN)^{-1}(g_iN)^{-1} = (gg_ig^{-1}g_i^{-1})N = [g, g_i]N$$

by definition And since for some element $g_{i+1} \in G_{i+1}$, $[g, g_i] = g_{i+1}$ as G is nilpotent. And $g_{i+1}N \in G_{i+1}N/N$, we have $[x, y] \in G_{i+1}N/N$, which certifies that the quotient group G/N is a nilpotent group.

Question 2

Prove a direct product of nilpotent groups is nilpotent

Solution: Let G and H be nilpotent groups, then there exists two chains

$$G = G_0 > G_1 > \cdots > G_n = \{ e \}$$

and

$$H = H_0 > H_1 > \cdots > H_m = \{ e \}$$

where $n \leq m$ without loss of generality. and for all $x \in G, y \in G_i$, it follows $[x, y] \in G_{i+1}$ and for $x \in H, y \in H_i$, it follows that $[x, y] \in H_{i+1}$ by the definition of nilpotent groups

Now, consider

$$K_i = \begin{cases} G_i \times H_i & \mid 0 \leq i \leq n \\ G_n \times H_i & \mid \text{otherwise} \end{cases}$$

making the chain

$$G \times H = K_0 > K_1 > \cdots > K_n > \cdots > K_m = \{ e \}$$

. Moreover, consider if $(g, h) \in G \times H$ and $(g', h') \in K_i$, then

$$[(g, h), (g', h')] = (g, h)(g', h')(g, h)^{-1}(g', h')^{-1} = (gg'g^{-1}g', hh'h^{-1}h'^{-1}) = ([g, g'], [h, h'])$$

Now for $i < n$, since $g \in G, g' \in G_i, h \in H, h' \in H_i$ by the definition of K_i, it follows $([g, g'], [h, h']) \in G_{i+1} \times H_{i+1} = K_{i+1}$ And for $i \geq n$, $g' = e$ is the only choice, hence $[g, g'] = gg'g^{-1}g'^{-1} = e \in G_n$. And $[h, h'] \in H_{i+1}$ as per above argument, therefore, $([g, g'], [h, h']) \in G_n \times H_{i+1} = K_{i+1}$.

Therefore, the statement was proved.

Question 3

Let G be a finite group of order pqr, where p, q, and r are prime numbers. Show G is not simple.

Solution: Let P, Q, R be a sylow p, q, r subgroup of G respectively, then we know $|P| = p, |Q| = q, |R| = r$. Which means P, Q, R are all cyclic. Thus, the pairwise intersection of each two sylow subgroups must be trivial. This is because the intersection of two disjoint cyclic groups must be a strict subgroup of both groups, but the order of the group must divides both, by lagrange's theorem, thus, the order of the intersection must be 1.

Now, assuming G is simple, we have that the number of sylow subgroup satisfies $n_p > 1, n_q > 1, n_r > 1$ since if $n_p = 1$, then for any $g \in G$, the conjugate $gPg^{-1} = P$ is another p-subgroup, hence itself, so $P \lhd G$. Let $p > q > r$ without loss of generality, then we have n_p is at least qr as any number $p < k < qr$ does not divide qr. As similarly, n_r is at least q, and n_q is at least p.

Since P contains $p - 1$ non-trivial elements, and each subgroup intersect trivially, there is at least $(p-1)(qr) + (q-1)p + (r-1)q + 1 = pqr - qr + pq - p + qr - q + 1 = pqr + pq - p - q + 1$ elements in G. Since $pq > p + p > p + q$, it follows $|G| > pqr$ which is a contradiction, hence G must be non-simple.

Question 4

Show any group of order $525 = 3 \cdot 5^2 \cdot 7$ is not simple.

Solution: Let G be a group of order 525. By the Sylow theorems, a Sylow 3-subgroup of G is of order 3, a Sylow 5-subgroup of G is of order 25 and a 7-subgroup of G is of order 7. Moreover, the number of Sylow subgroups follow $n_5 = 1, 21$, and $n_7 = 1, 15$.

Now, assume that G is simple, thus $n_7 \neq 1$ and $n_5 \neq 1$. Then, there must be $6 \times 14 = 84$ elements of order 7 since each group intersects trivially. Firstly, if each of the 21 Sylow 5-subgroups intersect trivially pairwisely, then there would be $21 \times 24 = 504$ non-trivial elements of order dividing 5. And there must be more than $504 + 84 > 524$ nontrivial elements, which is impossible.

Moreover, since G is simple, $n_3 \neq 1$, thus $n_3 \geq 7$. Which means that there is at least 14 elements of order 3.

Therefore, the intersection of any two Sylow 5-subgroup must be non-trivial. Let P and Q be two distinct (by the above assumption that $n_5 \neq 1$) Sylow 5-subgroup. Then $P \cap Q$ is a subgroup of P, thus, $|P \cap Q| = 5$ as $|P \cap Q| \neq 1, |P \cap Q| \neq 25, and\, |P \cap Q|\, |5^2$.

Let X be a set of $P \cap Q$ for any two distinct Sylow p-subgroup. If $|X| = 1$ then let $N \in X$ be that element. It follows that $gNg^{-1} = g(P \cap Q)g^{-1} = gPg^{-1} \cap gQg^{-1} \in X$. So, $gNg^{-1} = N$. Thus, N is a normal subgroup of G, which contradicts that G is simple.

Therefore, $|X| \geq 2$ must holds. In this case, there would be at least 9 nontrivial elements from each element of X, $20 \cdot 21 = 420$ nontrivial elements from the rest of 5-subgroups. 84 elements of order 7, and 14 elements of order 3. Thus, combining to $420 + 9 + 84 + 14 = 527$ nontrivial elements. Which is impossible.

Hence, a group G of order 525 cannot be a simple group.

Question 5

Let G be a finite group of order pn, where n is a natural number such $2 \leq n < p$ and p is prime. Show G is not simple.

Solution: Consider a p-subgroup P of G, it follows G must be a cyclic group of order p. Now, by the third sylow theorem, $n_p \equiv 1 \pmod p$ and $n_p | np$, so $n_p | n$, thus, $n_p = 1$.

As $n_p = 1$, there is a unique sylow p-subgroup of G. Since a sylow p-subgroup of G is of order $p \neq np$ since $n \geq 2$, it follows that $P \neq G$. Then, from the second sylow theorem, the sylow group P is a normal subgroup of G. Hence, G is not simple.

Question 6

Let P be a Sylow p-subgroup of a finite group G. Show if N is a non-trivial normal subgroup of G, then $N \cap P$ is a Sylow p-subgroup of N.

Solution: Notice that if $p \nmid |N|$ then $|N \cap P|$ is trivial by lagrange's theorem.

Now, for the remaining case, it holds that $p|\,|N|$. As $N \cap P$ cannot be trivial, then it is a p-subgroup of N by lagrange's theorem.

As, N is a normal subgroup of G, it follows that PH is a subgroup of G. By the second isomorphism theorem, $P/P \cap N \simeq PN/N$. Therefore, $|P \cap N| = \frac{|P||N|}{|PN|}$. Let $|G| = p^\alpha q$ where $\gcd(p, q) = 1$, then $|P| = p^\alpha$. And let $|N| = p^\beta r$ where $\gcd(r, p) = 1$.

Then, as $P < PN$, it follows that $p^\alpha | |PN|$, thus $|PN| = p^\alpha s$ for $\gcd(s,p) = 1$. Notice that $p^{\alpha+1} \not| |PN|$ by the maximality of a Sylow group. Therefore, $|P \cap N| = \frac{p^\alpha \cdot p^\beta r}{p^\alpha s} = p^\beta \frac{r}{s}$, for $\gcd(r/s, p) = 1$.

But since $P \cap N$ is a p-subgroup of N, then $|P \cap N| = p^m$ for some m, which restricts the only possibility to that $r/s = 1$, which makes $|P \cap N| = p^\beta$. Thus, $P \cap N$ is a Sylow p-subgroup by definition.

Question 7

Let P be a Sylow p-subgroup of a finite group G and let Q be a p-subgrop of G. Show $Q \cap N_G(P) = Q \cap P$.

Solution: The statement $Q \cap N_G(P) = Q \cap P$ is equivalent to that $x \in Q \wedge x \in N_G(P) \iff x \in Q \wedge x \in P$. The proof of later statement goes as
$(\Longrightarrow)$:

Notice that for any $g \in N_G(P)$, $gPg^{-1} = P$ by definition, thus P is a unique sylow p-subgroup of $N_G(P)$ by the second sylow theorem. Therefore, if $x \in Q$ and $x \in N_G(P)$, then x is in a p-subgroup of G and at the same time, in a group which the maximum p-subgroup is unique. Thus, x is also in the maximal p-subgroup. Therefore, $x \in P$, so it follows that $x \in Q \wedge x \in P$.

$(\Longleftarrow)$:

Since $P \lhd N_G(P)$, it follows that $P \subseteq N_G(P)$, thus, if $x \in Q \wedge x \in P$ then $x \in Q \wedge x \in N_G(P)$.

Question 8

Let G be a non-cyclic group of order 21. Find the number of Sylow 3-subgroups of G.

Solution: If G is a non-cyclic group of order 21. Then, the number of 3-subgroup of G is $n_3 \equiv 1 \pmod 3$ with $n_3|21$ restricting the choice to $n_3 = 1$ or $n_3 = 7$ by the third sylow theorem. Note also the order of a 3 subgroup is 3, since $21 = 3 \times 7$ Moreover, 7-subgroup of G is unique since $n_7 = 1$ is the only number satisfies the third theorem. Now, if G is non-cyclic, then the order of each element in G is either 1, 3, or 7. And there is only one element with only 1, the identity, and 6 elements with order 7, which are the elements in the unique 7-subgroup of G. Thus, the remaining 14 elements must have order 3, which means $n_3 = 7$ as each subgroup of order 3 consists of two unique non-trivial elements of order 3 and an identity.

Therefore, the number of Sylow 3-subgroup of G is 7.

Question 9

Prove the number of Sylow p-subgroups of $GL_2(\mathbb{Z}/p\mathbb{Z})$ is equal to $p + 1$.

Solution: From the third Sylow theorem, the number of Sylow p-subgroup, n_p must satisfies $n_p \equiv 1 \pmod p$. Let G denotes $GL_2(\mathbb{Z}/p\mathbb{Z})$, then it follows for $g \in G$, $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, such $\det(g) = ad - bc \neq 0$. For $ad = bc$, it follows that $a = bcd^{-1}$, thus a depends uniquely on b, c, d if $d \neq 0$ as d^{-1} is unique. And for $d = 0$, $ad = bc$ if and only if $b = 0$ or $c = 0$.

Thus, if $d = 0$ we have $p \cdot (p-1) \cdot (p-1)$ choices for a, b, c and $d \neq 0$, we have $p \cdot (p-1) \cdot p$ choices for the remaining a, b, c. This means the order $|G| = p \cdot (p+1) \cdot (p-1)^2$

Therefore, a p subgroup of G is a cyclic group of order p. Now, notice $g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ generates a subgroup of order p. The corresponding group is $P = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid 0 \leq a < p \right\}$. Now, all the other sylow subgroup must be in the from gPg^{-1} for some $g \in G$.

Claim 1

for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, the inverse g^{-1} is $\frac{1}{\det(g)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Proof: Consider $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \det(g) & 0 \\ 0 & \det(g) \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ☐

Now consider a conjugation action of G on P. Then, the size of all p-subgroup is $n_p = \left|\left\{ gPg^{-1} \mid g \in G \right\}\right| = |GP| = [G : G_P]$ by the orbit stabilizer theorem. Now, since the stabilizer $|G_P| = \left|\left\{ g \mid gPg^{-1} = g \right\}\right| = |N_G(P)|$

For $g \in G$, and $\langle \bar{p} \rangle = P$

$$g\bar{p}g^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} ad-bc-ac & a^2 \\ -c^2 & ad-bc+ac \end{bmatrix}$$

is in P only if $c^2 = 0$, which is when $c = 0$. And when $c = 0$, $g\bar{p}g^{-1} = \begin{bmatrix} 1 & \frac{a^2}{ad-bc} \\ 0 & 1 \end{bmatrix} \in P$ Thus, it follows that $N_G(P) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \mid \forall a, b, c \right\}$

So, $|N_G(P)| = p(p-1)(p-1)$ as b can be any value, but a and d must not be 0 in order for the matrix to be an element of $G = GL_2(\mathbb{Z}/p\mathbb{Z})$. Therefore, $n_p = |G| \,/\, |N_G(P)| = p + 1$

Question 10

Let a finite group G act transitively on a finite set X. Show

$$|\{ (g, x) \in G \times X \mid g \cdot x = x \}| = |G|$$

Solution: Since G acts transitively on X, then there is one orbit of the action, which means $Gx = X$. Now, by the orbit stabilizer theorem, $|Gx| = \frac{|G|}{|G_x|}$, thus $|G| = |G_x|\,|X|$. By the definition, $G_x = \{ g \in G \mid g \cdot x = x \}$. Now, consider

$$G_x \times X = \{ (g, x) \mid g \in G_x, x \in X \} = \{ (g, x) \mid g \cdot x = x, x \in X \} = \{ (g, x) \in G \times X \mid g \cdot x = x \}$$

Thus, $|\{ (g, x) \in G \times X \mid g \cdot x = x \}| = |G_x \times X| = |G_x| \cdot |X| = |G|$