Amin Zolfagharian - 610002072

---

**Problem 1.**

We prove the general cases $pq$, $p^2q$. And also for $p^\alpha$ we know that they have normal subgroup of order $m$ where $m < \alpha$.

$pq$: Let $p > q$. Let $n_p$ and $n_q$ denote the number of $p$-sylow and $q$-sylows respectively. By Sylow's theorem we know that $n_p \mid q$ and $n_p \overset{p}{\equiv} 1$. Since $n_p \mid q$ then $n_p = 1$ or $n_p = q$. If $n_p = 1$ then there is only one $p$-sylow group which means it must be normal. If $n_p = q$ then we have $q \overset{p}{\equiv} 1$ which implies $p \mid q-1$. Which can not happen since $p > q$. Thus there is only one $p$-sylow group and it is normal, thus all groups with order $pq$ are not simple.

$p^2q$: If $p > q$ then we have: $n_p \mid q$. If $n_p = 1$ then the $p$-sylow group is normal, thus $G$ is not simple. If $n_p = q$ then since we have $n_p \overset{p}{\equiv} 1$ then we have: $p \mid q-1$ which is a contradiction since $p > q$.
If $q > p$, then consider $n_q$. We know that $n_q \mid p^2$ and $n_q \overset{q}{\equiv} 1$. If $n_q = 1$ then $q$-sylow group is normal, thus the group is not simple. If $n_q = p$ then $q \mid p-1$ which is not possible since $q > p$. If $n_q = p^2$. We know that members of different $q$-sylow groups are different. Thus we have $p^2(q-1)$ distinct elements of order $q$. Now There is only $p^2$ elements left in $G$. This shows that there can only be one $p$-sylow group, which has to be normal. Thus $G$ is not simple.

$p^\alpha$: For $\alpha = 1$, there exists only one group with order $p$, $\mathbb{Z}_p$. for $\alpha > 1$ we know that for any $\beta < \alpha$ there exists a normal subgroup of order $p^\beta$. This shows that the group with order $p^\alpha$ for $\alpha > 1$ is not simple.

Now we are left with only few of orders: 24, 36, 40, 48, 54, 56, 60, 72, 80, 84, 88, 90, 96, 100.

24, 48, 96: These are all of the form $2^\alpha \cdot 3$. For all these ,consider the 2-sylow subgroup, which has index of 3. Then there exists a homomorphism $\pi : G \to S_3$. Since $|S_3| = 6$ and $|G| > 6$ then $ker(\pi) \neq 1$ which shows that $1 \neq ker(\pi) \lhd G$. Thus $G$ is not simple.

36: Let $P$ be a 3-sylow subgroup of $G$. Index of $P$ is 4. This means that there exists a homomorphism $\pi : G \to S_4$. Since $|G| = 36 > 4! = |S_4|$. Thus $|ker\pi| > 2$, and since $ker\pi \lhd G$, $G$ has a non-trivial normal subgroup, which means $G$ is not simple.

40: Consider the 5-sylow subgroup of $G$. we know that $n_5 \overset{5}{\equiv} 1$ and $n_5 \mid 8$. Thus $n_5 = 1$ which shows that this subgroup is normal, thus $G$ is not simple.

54: Index of a 3-sylow subgroup is 2. This means that there exists a homomorphism $\pi : G \to S_2$. And it is obvious that $ker\pi$ is non-trivial, therefore $G$ is not simple.

56: We know that $n_7 \overset{7}{\equiv} 1$ and $n_7 \mid 8$. Therefore $n_7 = 1$ or 8. If $n_7 = 1$ then 7-sylow group is normal. If $n_7 = 8$ then there exists $8 \times (7-1) = 48$ distince element with order 7. There are $56 - 48 = 8$ elements left in $G$. Thus there can only be one 2-sylow subgroup in $G$ which means the 2-sylow subgroup is normal in $G$, Thus $G$ is not simple.

72: We know that $n_3 \overset{3}{\equiv} 1$ and $n_3 \mid 8$. This means that $n_3 = 1$ or 4. If $n_3 = 1$ then 3-sylow subgroup is normal. If $n_3 = 4$ then let $P$ be a 3-sylow gruop. We know that the action of $G$ over $O_p$ under conjugation is transitive. And since $|O_p| = 4$, there exists a homomorphism $\pi : G \to S_4$. And since $|G| > |S_4|$, then $ker\pi \neq 1$ is a non-trivial normal subgroup of $G$, Thus $G$ is not simple.

80: Consider the 5-sylow subgroup of $G$. we know that $n_5 \overset{5}{\equiv} 1$ and $n_5 \mid 16$. Thus $n_5 = 1$ or 16. If $n_5 = 1$ then it is a normal subgroup and it is not simple. If $n_5 = 16$ then we have $16(5-1) = 64$ distinct element of order 5. Then there are only 16 elements left. which shows that there exists only one 2-sylow group of order 16, which means that 2-sylow group is normal and $G$ is not simple.

84: We know that $n_7 \overset{7}{\equiv} 1$ and $n_7 \mid 12$. This means that $n_7 = 1$ and 7-sylow subgroup is normal in $G$, thus $G$ is not simple.

88: We know that $n_{11} \overset{1}{\equiv} 11$ and $n_{11} \mid 8$. This means that $n_{11} = 1$, thus 11-sylow subgroup is normal in $G$ and $G$ is not simple.

90: We know that $n_3 \overset{3}{\equiv} 1$ and $n_3 \mid 10$. This shows that $n_3 = 1$, thus 3-sylow subgroup is norma in $G$ and $G$ is not simple.

100: We know that $n_5 \overset{5}{\equiv} 1$ and $n_5 \mid 4$. This shows that $n_5 = 1$ and therefore 5-sylow subgroup is normal in $G$ and $G$ is not simple.

The only order that we didn't show thtt is not simple is 60, and since we know that the only simple group of order 60 is $A_5$, Thus the only simple group with order less than 100 is $A_5$

**Problem 2.**

We have $4563 = 13^2 \cdot 3^3$. Now we know that $n_{13} \overset{13}{\equiv} 1$ and $n_{13} \mid 27$. This shows that $n_{13} = 1$ or $n_{13} = 27$. If $n_{13} = 1$ then we are done since the only 13-sylow subgroup is normal in $G$. Now suppose that $n_{13} = 27$. If all 13-sylow subgroups have different elements, then there are $27 \times 168 = 4563 - 27$ distinct elements of order 13 or $13^2$. And the remaining elements can only create one 3-sylow subgroup, which makes it normal. Now if 13-sylow groups have some common elements, then there exists two 13-sylow groups $P_1$ and $P_2$ such that:

$$P_1 \cap P_2 = H > 1 \overset{P_1 \neq P_2}{\Longrightarrow} |H| = 13$$

Also $H$ is normal in $P_1$ and $P_2$ since $[P_1 : H]13$, which is the least prime number possible. Therefore we have $P_1 < N_G(H)$ and $P_2 < N_G(H)$.

$$169 = |P_1| < |P_1 \cup P_2| < |N_G(H)| \mid 4563 \implies N_G(H) \geq 13^2 \cdot 3$$

This shows that $[G : N_G(H)] \leq 9$. Therefore the action of $G$ over left cosets of $N_G(H)$, gives us the homomorphism: $\varphi : G \to S_9$. But since $13 \mid |G|$ and $13 \nmid 9!$, then $ker\varphi \neq 1$, thus $ker\varphi$ is normal in $G$, and $G$ is not simple.

**Problem 3.**

Let $(\sigma, \phi) \in Aut(G) \times Aut(H)$. It is easy to see that $(\sigma, \phi)$ is also an autmorphism of $G \times H$.

$$\begin{aligned}(\sigma, \phi)[(a, b).(c, d)] &= (\sigma, \phi)[ac, bd] = (\sigma(ac), \phi(bd)) \\ &= (\sigma(a)\sigma(c), \sigma(b)\sigma(d)) = (\sigma(a), \phi(b)).(\sigma(c), \phi(d)) \\ &= (\sigma, \phi)[a, b].(\sigma, \phi)[c, d]\end{aligned}$$

This shows that $(\sigma, \phi) \in Aut(G \times H)$. Thus $Aut(G) \times Aut(H) \subset Aut(G \times H)$.
Now suppose $\delta \in Aut(G \times H)$. We know that $Ord_{G\times H}(a, b) = lcm(Ord_G(a), Ord_H(b))$. Thus $Ord_{G\times H}(a, 1) = Ord_G(a) \mid |G|$. Since $\delta$ maps elements with same order to each other then if we have $\delta(a, 1) = (b, c)$ then:

$$\begin{gathered}Ord_{G\times H}(b, c) = Ord_G(a) \mid |G| \\ Ord_{G\times H}(b, c) = lcm(Ord_G(b), Ord_H(c))\end{gathered}$$

Now if $Ord_H(c) \neq 1$ then we would have:

$$\begin{gathered}\exists p \neq 1 : \ p \mid Ord_H(c) \mid |H| \\ \implies p \mid Ord_{G\times H}(b, c) \mid |G| \\ \implies p \mid \gcd(|G|, |H|) = 1\end{gathered}$$

Which is a contradition. This shows that for any element $(a, 1)$ we have $\delta(a, 1) = (a', 1)$. And similarly we have: $\delta(1, b) = (1, b')$. Therefore if we define $\delta_1 : G \to G$ and $\delta_2 : H \to H$:

$$\begin{gathered}\forall g \in G : \delta_1(g) = g' \text{ where } \delta(g, 1) = (g', 1) \\ \forall h \in H : \delta_2(h) = h' \text{ where } \delta(1, h) = (1, h')\end{gathered}$$

Then it is trivial that $\delta_1 \in Aut(G)$, $\delta_2 \in Aut(H)$. Thus $\delta = (\delta_1, \delta_2) \in Aut(G)\times Aut(H)$. Which implies $Aut(G\times H) \subset Aut(G)\times Aut(H)$. Thus $Aut(G\times H) = Aut(G)\times Aut(H)$.

**Problem 4.**

Suppose $\varphi \in Aut(D_8)$. Since $r$ and $s$ are generators of $D_8$ then $\varphi$ is uniquely determined with $\varphi(r)$ and $\varphi(s)$. Since $\varphi$ is an automorphism, then $Ord(r) = Ord(\varphi(r))$ and $Ord(s) = Ord(\varphi(s))$. There are only 2 elements of order 4 in $D_8$, $r$ and $r^3$. Thus $\varphi(r) = r$ or $r^3$. And there are 5 elements of order 2 in in this group, $r^2, s, sr, sr^2, sr^3$. If $\varphi(s) = r^2$ then $\varphi(D_8) = C_4 \neq D_8$, thus $\varphi$ is not an automorphism. But for any other values we have:

$$\begin{gathered}\varphi(r) = r^i, \varphi(s) = sr^j \\ \implies \varphi(r)\varphi(s) = r^i sr^j = sr^{j-i} = sr^j r^{-1} = \varphi(s)\varphi(r)^{-1}\end{gathered}$$

This shows that $\varphi(D_8) = D_8$. Therefore there are only 8 automorphisms for $D_8$. Now consider these automorphisms:

$$\delta : \begin{cases} r \to r^3 \\ s \to s \end{cases} \qquad \sigma : \begin{cases} r \to r \\ s \to sr \end{cases}$$

It is easy to see that $Ord(\delta) = 2$ and $Ord(\sigma) = 4$ in $Aut(D_8)$. Note that we have:

$$\sigma^{-1} : \begin{cases} r \to r \\ s \to sr^3 \end{cases}$$

Now it is easy to see that:

$$\sigma\delta : \begin{cases} r \to r^3 \\ s \to sr \end{cases} \qquad \delta\sigma^{-1} : \begin{cases} r \to r^3 \\ s \to s(r^3)^3 = sr \end{cases}$$

This shows that $\sigma\delta = \delta\sigma^{-1}$. Therefore $Aut(D_8) = \langle \sigma, \delta | \sigma^4 = \delta^2 = 1, \sigma\delta = \delta\sigma^{-1} \rangle = D_8$. Therefore $Aut(D_8) = D_8$.

**Problem 5.**

Suppose $H$ is a normal subgroup of $D_{2n}$. If $H \subset \langle r \rangle$, then $H = \langle r^i \rangle$ such that $i \mid n$. And it is easy to see that for any element $\delta \in D_{2n}$ we have $\delta H \delta^{-1} = H$. Thus for any $i \mid n$, $\langle r^i \rangle$ is a normal subgroup of $D_{2n}$. Now suppose $H \not\subset \langle r \rangle$. Thus there exists a $sr^i \in H$. Since $H$ is normal we have $r(sr^i)r^{-1} = sr^{i-2} \in H$. This shows that if $n$ is odd, then $H$ contains all elements of form $sr^i$. Which are half of the elements of the group. With addition of 1, $H$ contains more than half of the $D_{2n}$, Which means that $H = D_{2n}$. Since if we want to write $D_{2n}$, as a direct product, then the two subgroups are both normal in $D_{2n}$, and it is easy that direct product of these normal subgroups for odd $n$, doesn't create $D_{2n}$, then for odd $n$ it is not possible to write $D_{2n}$ as a direct product. For even $n$, if $H \subset \langle r \rangle$ it is similar to the privious part. But if $sr^i \in H$, then with conjugation $sr^{i-2} \in H$. This shows that $\langle s, r^2 \rangle \subset H$. Which has exactly half of the elements of $D_{2n}$, therefore in order for $H$ to be a proper normal subgroup, we have $H = \langle s, r^2 \rangle$. Note that this subgroup is the only normal subgroup of $D_{2n}$ such that it includes $s$. Thus if we want to write $D_{2n}$ as a direct product, one normal sbugroup is $\langle s, r^2 \rangle$. And considering the size of group, the other subgroup must be of order 2. Let $t$ be an element with order 2. Thus we would have $D_{2n} = \langle t \rangle \times \langle s, r^2 \rangle$. Therefore $D_{2n} = \langle (t, s), (t, r^2) \rangle$. Which implies $Ord((t, s)) = 2$ and $Ord((t, r^2)) = n$. We also know that $Ord((t, r^2)) = lcm(Ord(t), Ord(r^2)) = lcm(2, n/2)$. This shows that $n/2$ must be odd, in order for this direct product to create $D_{2n}$. Therefore if $n$ is of the form $2m$ where $m$ is odd, then $D_{2n}$ can be written as a direct product, otherwise it cannot.