Math 71: Abstract Algebra

Prishita Dharampal

Credit Statement: Talked to Sair Shaikh'26, and Math Stack Exchange.

Problem 1. *Solvable up to sixty!* Recall that A_5, which has order 60, is simple and nonabelian. The goal is to:

(ℵ) Prove that all groups of order < 60 are solvable.

This has two steps.

(α) First, use Jordan–Hölder to prove that if 60 is the first order of a finite nonabelian simple group, then all groups of order < 60 are solvable.

(β) Second, prove that every nonabelian group of order < 60 is not simple. Since the abelian simple groups are precisely those of prime order, for each composite order $n < 60$, we will try to prove that any group of order n is not simple. For example, we already know that no group of order p^α, with $\alpha > 1$, is simple and that no group of order pq, with p and q primes, is simple. Prove the following additional criteria on the order of a group for the group to not be simple:

Hints. Part (a) follows from a direct application of the congruence conditions in the Sylow theorems. For (b), assume the contrary and consider the possible number of Sylow r-subgroups; then use this to count the number of elements of order r (any two Sylow r-subgroups intersect only at the identity). Combine this with the number of elements of order p and q to find more elements than the order of the group. For (c) and (d), handle small k using the Sylow congruence conditions, and then for large k, consider the permutation representation associated to the conjugation action of G on the set of Sylow 2-subgroups. For (e) and (f), do the same using the Sylow 3-subgroups. For (g), if neither the Sylow 2- nor 7-subgroups are normal, start counting elements in these subgroups to reach a contradiction (while any two Sylow 7-subgroups only intersect at the identity, how could Sylow 2-subgroups intersect?).
Finally, use all the criteria you know to handle every composite order < 60. Have fun! How much higher can you go using these same tools?

Problem (α). First, use Jordan–Hölder to prove that if 60 is the first order of a finite nonabelian simple group, then all groups of order < 60 are solvable.

Solution.

If 60 is the first order of a finite non-abelian simple group, then groups of < 60 are either abelian, or simple (they're all finite).

1. *The group is abelian.* By Jordan–Hölder we know that a composition series for group G exists. Because G is abelian, all subgroups are normal $\implies$ all composition factors are normal $\implies$ group is solvable.

2. *The group is non-abelian and non-simple.* By Jordan–Hölder we know that a composition series for group G exists. Assume all groups of order less than n are solvable, for some $n < 59$. Then because group G of order n is not simple, we know that at least one non trivial normal subgroup N exists. Obviously, the orders of N and G/N are both less than n. Then by our induction hypothesis we know that both N and G/N are solvable, and hence G is solvable.

Problem ($\beta.a$).
If G is a finite group of order $p^k m$, with $p \nmid m$ and $m < p$ (more generally, no divisor of m other than 1 is congruent to 1 modulo p), then G has a normal Sylow p-subgroup.

Solution.

By Sylow's Theorem, we know that G ha a Sylow p-subgroup P of order p^k. We also know that the following to relations must hold:

$$n_p \mid m, \qquad n_p \equiv 1 \pmod{p}$$

where n_p is the number of Sylow p-groups in G. But the only divisor of m congruent to 1 modulo p is 1 (given). Hence $n_p = 1$, and the Sylow p-group is unique.
And by Corollary 20 if P is the unique Sylow p-group in G, then it is also normal in G. Hence G has a normal Sylow $p-$subgroup and G is not simple.

Problem (β.b).
If G is a finite group of order pqr, where p, q, r are primes with $p < q < r$, then G has a normal Sylow subgroup for at least one of p, q, or r.

Solution.

By Sylow's Theorems, we know the following,

1. G has at least one Sylow r-subgroup.
2. The number of Sylow r-subgroups n_r divides pq, and $n_r \equiv 1 \pmod{r}$.

Then, $n_r \mid pq \implies n_r = 1, p, q, pq$. But $n_r \neq p, q$ because both p and q are less than r and hence not congruent to 1 mod r. I.e. $n_r = 1, pq$.
If $n_r = 1$, then by part (a), G has a normal Sylow r-subgroup. If $n_r = pq$, then there are pq Sylow r-subgroups. Because r is prime, all pq subgroups are cyclic, and intersect only at identity. I.e. there are $pq(r-1)$ elements of order r in G, and pq elements of other orders.

Similarly, we know,

1. G has at least one Sylow q-subgroup.
2. The number of Sylow q-subgroups n_r divides pr, and $n_q \equiv 1 \pmod{q}$.

Then, $n_q \mid pr \implies n_q = 1, p, r, pr$. But $n_q \neq p$ because p is a prime number less than q and hence not congruent to 1 mod q.

I.e. $n_q = 1, r, pr$.
If $n_q = 1$, then by part (a), G has a normal Sylow q-subgroup. If $n_q = r$, then there are r Sylow q-subgroups. And because q is prime, all r subgroups are cyclic, and interesect only at identity. I.e. there are $r(q-1)$ elements of order q in G.

If $n_q = pr$, then there are pr Sylow q-subgroups. Because q is prime, all pr subgroups are cyclic, and intersect only at identity. I.e. there are $pr(q-1)$ elements of order q in G.

If we assume that $n_r \neq 1$ and $n_q \neq 1$, then we have 2 cases,

1. $n_r = pq, n_q = r$

$$\begin{aligned} &\implies pq \geq rq - r \\ &\quad\ pq \geq r(q-1) \end{aligned}$$

   But $r > q$ and $q - 1 > p$, so this is a contradiction and at least one of n_r or n_q needs to be 1.

2. $n_r = pq, n_q = pr$

$$\begin{aligned} \implies pq &\geq pqr - pr \\ q &\geq qr - r \\ q &\geq r(q-1) \end{aligned}$$

But $r > q$ and $q - 1 > 1$, so this is a contradiction and at least one of n_r or n_q needs to be 1.

Thus, there exists at least 1 normal Sylow p-subgroup in G, and G is not simple.

Problem ($\beta.c$).
If G is a finite group of order $2^k \cdot 3$, with $k \geq 1$, then G is not simple.

Solution.

Consider the Sylow 2-group of order 2^k, then $n_2 = 1, 3$. If $n_2 = 1$, then the Sylow subgroup is unique and by Corollary 20 also normal. If $n_2 = 3$, then by Sylow's Second Theorem all 3-Sylow subgroups are conjugate to each other. Let the set of these subgroups be $A = \{P_1, P_2, P_3\}$, then we can represent the conjugation action of G on A by $\{g \in G : gP_ig^{-1} \in S\}$. The permutation representation of this action can be defined as $\varphi : G \to S_{|A|}$. Then we have the following cases,

1. If the kernel is not trivial, then φ is not injective, and G has a normal subgroup. For φ to not be trivial, $|G| > |S_A| \implies |G| > 6 \implies k > 1$.

2. If the kernel is trivial, or $k = 1$, then by part (a) G has a normal subgroup.

Hence, G is not simple.

Problem ($\beta.d$).
If G is a finite group of order $2^k \cdot 5$, with $k \geq 1$, then G is not simple.

Solution.

Similar to the argument above, consider the Sylow 2-group of order 2^k, then $n_2 = 1, 5$. If $n_2 = 1$, then the Sylow subgroup is unique and by Corollary 20 also normal. If $n_2 = 5$, then by Sylow's Second Theorem all 5-Sylow subgroups are conjugate to each other. Let the set of these subgroups be $A = \{P_1, P_2, P_3, P_4, P_5\}$, then we can represent the conjugation action of G on A by $\{g \in G : gP_ig^{-1} \in S\}$. The permutation representation of this action can be defined as $\varphi : G \to S_{|A|}$. Then we have the following cases,

1. If the kernel is not trivial, then φ is not injective, and G has a normal subgroup. For φ to not be trivial, $|G| > |S_A| \implies |G| > 120 \implies k > 4$.
2. If the kernel is trivial, or $k = 1$, then by part (a) G has a normal subgroup.
3. If $k = 2$, then by part (a) G has a normal subgroup.
4. If $k = 3$, then the number of 5-Sylow groups $n_5 \mid 8 \implies n_5 = 1, 2, 4, 8$ but only $1 \equiv 1 \pmod 5$.
5. If $k = 4$, then $\mid G \mid = 80$, and $80 \nmid 120$, so $\nexists$ a subgroup of S_5 that G is isomorphic to. I.e φ is not injective, has a non-trivial kernel, and hence also a normal subgroup.

Hence, G is not simple.

Problem ($\beta.e$).
If G is a finite group of order $2^2 \cdot 3^k$, with $k \geq 1$, then G is not simple. For $k = 1$, use part (c).

Solution.

There are 2 cases, if $k = 1$, then G is a finite group of order 12, and can be represented as $|G| = 2^k \cdot 3$, where $k = 1$. Hence G is not simple by part (c). If $k \geq 2$, then we know by Sylow's First Theorem that there exists at least one Sylow 3-subgroup of order 3^k in G. The number of Sylow 3-subgroups n_3 divides 4, i.e. $n_3 = 1, 2, 4$. But n_3 is also congruent to 1 mod 3, so n_3 must be 1. By Corollory 20, we know that if the Sylow p-subgroup is unique it is also normal. Hence, G is not simple.

Problem $(\beta.f)$.
If G is a finite group of order $3^k \cdot 5$, with $k \geq 1$, then G is not simple.

Solution.

We know by Sylow's First Theorem that there exists at least one Sylow 3-subgroup of order 3^k in G. The number of Sylow 3-subgroups n_3 divides 5, i.e. $n_3 = 1, 5$. But n_3 is also congruent to 1 mod 3, so n_3 must be 1. By Corollory 20, we know that if the Sylow p-subgroup is unique it is also normal. Hence, G is not simple.

Problem ($\beta.g$).
No group of order 56 is simple.

Solution.

The prime factorization of 56 is $2^3 \cdot 7$. We know by Sylow's First Theorem that there exists at least one Sylow 7-subgroup of order 7 in G. The number of Sylow 7-subgroups n_7 divides 8, i.e. $n_7 = 1, 2, 4, 8$. But n_7 is also congruent to 1 mod 7, so n_7 can only be either 1 or 8. If $n_7 = 1$ then by Corollory 20, we know that if a Sylow p-group is unique it is also normal, then we are done. But if $n_7 = 8$, then we know that the conjugates intersect only at identity (cyclic groups), i.e. the number of elements of order 7 (all elements in a cyclic group of prime order have order equal to the prime) is $8(7-1) = 42$. So there exist 8 elements of order not equal to 7.

Again by Sylow's First Theorem we also know that there exists at least one Sylow 2-subgroup of order 8 in G. The order of none of these elements is 7, because $7 \nmid 8$. Then we can say that there only exists 1 Sylow 2-subgroup. And by Corollory 20, we know that if the Sylow p-subgroup is unique it is also normal. Hence, G is not simple.

Problem ($\beta.h$).
Optional. What is the largest number $N > 60$ you can find such that no group of composite order n, with $61 \leq n \leq N$, is simple?

Solution.

Using just the facts we have proved so far, we can show that groups with order upto 71 are not simple. But if we prove that all groups of order 72 are not simple, then we can go upto 83.

Proof for $|G| = 72$.
$|G| = 72 = 2^3 \cdot 3^2$. But for this group consider the Sylow 3-subgroup, this subgroup has order 9, and the number of Sylow 3-subgroups $n_3 \mid 8 \implies n_3 = 1, 2, 4, 8$, but n_3 is also congruent to 1 mod 3 $\implies n_3 = 1, 4$. If $n_3 = 1$, then a normal subgroup exists and G is not simple. If $n_3 = 4$ then we can define a homomorphism from $\varphi : G \to S_4$, but $|S_4| < |G|$, i.e φ is not injective, i.e the kernel is not trivial, i.e. a normal subgroup exists. Hence, the group of order 72 is not simple.