# PROBLEM SET #7 SOLUTIONS

**Problem 1.** Let $G$ be a finite simple group with $|G| < 100$. Prove that $G$ is either abelian or has order 60.
*Hints:*

- *Count the elements of $G$ in terms of their orders. When does this exceed $|G$?*
- *If $H$ is a large subgroup of $G$, consider the action $G$ on the set of left cosets of $H$ in $G$. What does the first isomorphism theorem say?*
- *Similarly, if $H$ is a Sylow subgroup of $G$, consider the action $G$ on the set of conjugates of $H$.*

**Solution 1.** Firstly, any group of prime order is necessarily cyclic, and hence abelian. Moreover, we have seen that any nontrivial group whose order is a prime power necessarily has a nontrivial center. Since the center is a normal subgroup, this means the group cannot be simple (unless the center is the entire group, in which case it is abelian). After removing all orders from 2 through 99 which are prime powers, we are left with 63 possibilities.

If $|G| = pq$ for $p < q$ distinct primes, then by Sylow's third theorem, we have that the number $n_q$ of Sylow $q$-subgroups is congruent to 1 mod $q$ and also divides $p$. Since every integer greater than one which is congruent to 1 mod $p$ is greater than $p$, the only possibility is that $n_q = 1$. This means that there is a unique Sylow $q$-subgroup, and it is necessarily normal since otherwise a conjugate of it would give a different Sylow $q$-subgroup. It follows that $G$ is not simple. After taking this into account, we are left with 33 possibilities.

Similarly, suppose that $|G| = pq^k$ for $p < q$ distinct primes and $k \in \mathbb{Z}_{\geq 1}$. Then the same reasoning as in the previous paragraph shows that there is a unique Sylow $q$-subgroup of $G$ which is necessarily normal. After taking this into account, we are left with 28 possibilities.

Now suppose that $|G| = p^2q$ for $p < q$ distinct primes. By Sylow's third theorem, $n_q$ divides $p^2$ and is congruent to 1 mod $q$. If $n_q = 1$ then $G$ is not simple. We cannot have $n_q = p$, since $p$ is not congruent to 1 mod $q$. The remaining possibility is that $n_q = p^2$. Then we must have that $p^2$ is congruent to 1 mod $q$, i.e. $q$ divides $p^2 - 1$, so $q$ divides either $p - 1$ or $p + 1$. Clearly we cannot have that $q$ divides $p - 1$, and we can only have that $q$ divides $p + 1$ in the case $q = 3$ and $p = 2$, i.e. $|G| = 12$.

Moreover, there is no simple group $G$ of order 12. To see this, let $H$ be a Sylow 2-subgroup, which has order 4. Let $X$ denote the set of left cosets of $H$ in $G$, so $|X| = 3$. Consider the action of $G$ on $X$ induced by left multiplication. This corresponds to a homomorphism $\Phi : G \to S_3$, and it is easy to check that the kernel is not all of $G$, since $gH \neq H$ for any $g \in G \setminus H$. Moreover, the kernel of $\Phi$ cannot be $\{e\}$, since then the first isomorphism theorem would imply that $G$ is isomorphic to a subgroup of $S_3$, but $|G| = 12$ whereas $|S_3| = 6$. Therefore $\ker(\Phi)$ must be a normal subgroup of $G$ which is neither $G$ nor $\{e\}$, so $G$ is not simple. After taking these into account, we are left with following 10 possibilities: $24, 30, 36, 40, 42, 48, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96$.

We now rule out these remaining possibilities (except for 60) by supposing that $G$ is a simple group of a given order, and deriving a contradiction. Firstly, suppose that $|G| = 40 = (2^3)(5)$. Then $n_5$ must be 1 by a simple application of Sylow's third theorem. Similarly, we rule out $|G| = 42, 66, 70, 78, 84, 88$.

Now suppose that $|G| = 24 = (2^3)(3)$. In fact, the argument above for $|G| = 12$ easily generalizes to prove the following:

**Lemma 1.** If $G$ is a finite group and $H$ is a subgroup of index $m$, then there exists a homomorphism $\Phi : G \to S_m$ whose kernel is not all of $G$. In particular, if $|G|$ does not divide $m!$, then the kernel cannot be $\{e\}$, and hence $G$ is not simple.

If $|G| = 24$, we can apply this lemma to a Sylow 2-subgroup, which has index 3. We then get a contradiction, since 24 does not divide $3! = 6$. A very similar argument takes care of $|G| = 36, 48, 80, 96$.

Now suppose that $|G| = 30 = (2)(3)(5)$. Then we must have $n_3 = 10$ and $n_5 = 6$. This gives $10 * 2 = 20$ elements of order 3 and $6 * 4 = 24$ elements of order 5, which is impossible.

Now suppose that $|G| = 56 = (2^3)(7)$. In principle we could have $n_2 = 7$ and $n_7 = 8$. Note that each Sylow 2-subgroup has order 8, and hence 4 elements of order 8. Therefore we would have $7 * 4 = 28$ elements of order 8, and $8 * 6 = 48$ elements of order 7, which is impossible since $28 + 48 > 56$.

Now suppose that $|G| = 72 = (2^3)(3^2)$. If $n_3 \neq 1$, then we must have $n_3 = 4$. Let $X$ denote the set of Sylow 3-subgroups of $G$, so $|X| = 4$. Let $G$ act on $X$ by conjugation. This corresponds to a homomorphism $\Phi : G \to S_4$. Since $G$ acts transitively on $X$ thanks to Sylow's second theorem, the kernel cannot be all of $G$. It also cannot be $\{e\}$, since then $|G| = 72$ would have to divide $|S_4| = 24$, similar to the above lemma. Since the kernel of $\Phi$ is a normal subgroup of $G$, this gives a contradiction.

Finally, suppose that $|G| = 90 = (2)(3^2)(5)$. In principle we could have $n_3 = 10$ and $n_5 = 6$. This accounts $10 * 6 = 60$ elements of order 9, and $6 * 4 = 24$ elements of order 5. Taking into account the identity element, there are then at most 5 elements of order 2, so $n_2 \leq 5$. Now let $X$ denote the set of Sylow 2-subgroups. Since $|G| = 90$ cannot divide $n_2!$, we get a contradiction as in the previous paragraph.

**Addendum:** Actually the above argument for $|G| = 90$ is incomplete, since in principle the Sylow 3-subgroups could be isomorphic to $\mathbb{Z}/(3\mathbb{Z}) \times \mathbb{Z}/(3\mathbb{Z})$, in which case there are no elements of order 9. As an alternative, we can use the following:

**Lemma 2.** Let $G$ be a finite group with $|G| = 2m$ for $m \in \mathbb{Z}_{\geq 1}$ odd. Then $G$ has an index two normal subgroup.

*Proof.* By Cayley's theorem, there is an injective homomorphism $\iota : G \hookrightarrow S_G$. Let $\varepsilon : S_G \to C_2$ denote the sign homomorphism (its kernel is the alternating subgroup). Let $\Phi = \varepsilon \circ \iota : G \to C_2$ denote the homomorphism given by composing these two homomorphisms. By Cauchy's theorem, there is an element $x \in G$ of order 2. Then $\iota(x)$ is the permutation of $G$ sending $g \in G$ to $xg$ (c.f. the proof of Cauchy's theorem). Since $x^2 = e$, this permutation has order two. Moreover, this permutation does not fix any elements in $G$, i.e. $xg \neq g$ for any $g \in G$. It follows that the cycle decomposition of $\iota(x)$

must consist of $m$ disjoint transpositions, and therefore $\Phi(x) = -1^m = -1$. This shows that $\Phi$ is surjective, and hence its kernel is an index two normal subgroup of $G$. $\square$