Math 120 Homework 5 Solutions

May 8, 2018

Recall a group G is *simple* if it has no normal subgroups except itself and $\{1\}$.

We will be using all three parts of Sylow's theorem (Theorem 4.5.18 from Dummit and Foote) extensively. Here's the statement:

Theorem. *(Sylow's Theorem) Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.*

1. Sylow p-subgroups of G (subgroups of order p^α) exist.
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e. Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.
3. The number n_p of Sylow p-subgroups of G satisfies

$$n_p \equiv 1 \pmod p.$$

   Further, n_p is the index $|G : N_G(P)|$ of the normalizer of any Sylow p-subgroup P, hence $n_p | m$.

Question 1

Prove that if $|G| = 312 = 2^3 \cdot 3 \cdot 13$ then G is not simple.

Let H be a Sylow 13-subgroup of G. Then, the number n_{13} of Sylow 13-subgroups of G satisfies $n_{13} \equiv 1 \pmod 13$ and $n_{13} | 2^3 \cdot 3 = 24$. But the only factor of 24 which is $1 \pmod 13$ is 1, so $n_p = 1$. Therefore there is only one 13-Sylow subgroup, which is therefore normal, so G is not simple.

Question 2

Suppose G is a simple group with $|G| = 168 = 2^3 \cdot 3 \cdot 7$. How many elements of order 7 does G contain? Justify your answer.

The number n_7 of Sylow 7-subgroups of G satisfies $n_7 \equiv 1 \pmod 7$ and $n_7 | 2^3 \cdot 3 = 24$. The only two factors of 24 which are $1 \pmod 7$ are 1 and 8, so these are the only possible values of n_7.

If $n_7 = 1$, then there is a unique Sylow 7-subgroup H which is normal, contradicting the simplicity of G. Thus, $n_7 = 8$.

Notice that a group of order 7 is cyclic, and two distinct cyclic groups of order 7 intersect in only the identity. Also, every element of order 7 generates a cyclic subgroup of order 7.

Putting these facts together, we see that there are 6 elements of order 7 in each of $n_7 = 8$ Sylow 7-subgroups, and each such element is contained in a unique such group. The total number of elements of order 7 is therefore $6 \cdot 8 = 48$.

Question 3

Prove that if $|G| = 56 = 2^3 \cdot 7$ then G is not simple.

Let H be a Sylow 7-subgroup of G. Then, the number n_7 of Sylow 7-subgroups of G satisfies $n_7 \equiv 1 \pmod 7$ and $n_7 | 2^3 = 8$. The only possibilities are $n_7 = 1, 8$.

If $n_7 = 1$ then H is unique and normal, so G is not simple.

Otherwise, if $n_7 = 8$, then by the same argument as in Question 2, there are $6 \cdot 8 = 48$ elements of order 7 in G. Now, let K be a Sylow 8-subgroup of G.

By Lagrange's theorem every element of K has order dividing 8. Thus, none of the 48 elements of order 7 lie in K. But $|K| = 8$ and $|G| = 56$, so if the 48 elements of order 7 lie outside K then they make up the entire complement $G \backslash K$. That is to say, every element $g \notin K$ has order 7. We claim that K must therefore be normal. This is just because any conjugate gKg^{-1} of K is also a group of order 8 and can't contain any of the 48 elements of order 7. Thus if H is not normal, K is.

Either way, G has a normal subgroup and can't be simple.

Question 4

Prove that if $|G| = 132 = 2^2 \cdot 3 \cdot 11$ then G is not simple.

The numbers n_2, n_3, n_{11} of Sylow subgroups of G of orders $4, 3, 11$ satisfy:

- $n_2 \equiv 1 \pmod 2$ and $n_2 | 3 \cdot 11 = 33$, so $n_2 \in \{1, 3, 11, 33\}$.
- $n_3 \equiv 1 \pmod 3$ and $n_3 | 2^2 \cdot 11 = 44$, so $n_3 \in \{1, 4\}$.
- $n_{11} \equiv 1 \pmod 11$ and $n_{11} | 2^2 \cdot 3 = 12$, so $n_{11} = \{1, 12\}$.

If any of them equals 1, then there is a unique Sylow p-subgroup for that p which is normal, so G would be simple.

Otherwise, $n_3 = 4$ and $n_{11} = 12$. But then by the same argument as in Question 2, there must be $2 \cdot 4 = 8$ elements of order 3 and $10 \cdot 12 = 120$ elements of order 11 in G (Note: this uses the fact that groups of prime order are cyclic.) In total this makes 128 of the 132 elements of G.

This leaves 4 elements of G that can possibly lie in any Sylow 2-subgroup of order 4. Thus, $n_2 = 1$ and G has a normal subgroup of order 4 anyway.

Question 5

Prove that if $|G| = 231 = 3 \cdot 7 \cdot 11$ then $|Z(G)| \geq 11$ (in particular, G is not simple).

The number n_{11} of Sylow 11-subgroups of G satisfies $n_{11} \equiv 1 \pmod 11$ and $n_{11} | 3^2 \cdot 7 = 63$. The only possibility is $n_{11} = 1$, so G has a unique normal Sylow 11-subgroup H. We claim that $H \subseteq Z(G)$.

Suppose otherwise. Then, for some $g \in G$ and $h \in H$, $hg \neq gh$. Right-multiplying by g^{-1}, we get $h \neq ghg^{-1}$. But $ghg^{-1} \in H$ because $h \in H$ and H is normal, and since H is cyclic, $ghg^{-1} = h^m$ for some $m \in \{2, \ldots, 10\}$.

Applying the conjugation by g operation repeatedly, and noting that

$$\begin{aligned} gh^n g^{-1} &= (ghg^{-1})^n \\ &= (h^m)^n \\ &= h^{mn}, \end{aligned}$$

it follows that $g^k h g^{-k} = h^{m^k}$ for any natural number k. In particular, taking $k = |g|$ the order of g in G, we have

$$\begin{aligned} h &= 1 \cdot h \cdot 1 \\ &= g^{|g|} h g^{-|g|} \\ &= h^{m^{|g|}}, \end{aligned}$$

and since h has order 11, $m^{|g|} \equiv 1 \pmod 11$. In other words, $|g|$ is divisible by the order of m as an element of $(\mathbb{Z}/11\mathbb{Z})^\times$. But this is a group of order 10, and m is not the identity, so by Lagrange's theorem (or

Fermat's Little Theorem), the order of m in this group is 2, 5, or 10. By Lagrange's theorem again, none of these can divide the order of any element g of G, since $|G| = 3 \cdot 7 \cdot 11$, so we have a contradiction. Thus $H \subseteq Z(G)$ and $|Z(G)| \geq |H| = 11$, as desired.

Question 6

Prove that if $|G| = 33 = 3 \cdot 11$ then G is abelian.

The numbers n_3 and n_7 of Sylow 3- and 7-subgroups satisfy $n_3 \equiv 1 \pmod 3$, $n_3|11$, $n_{11} \equiv 1 \pmod 1)1$, $n_{11}|3$, and so $n_3 = n_{11} = 1$ and there are unique normal Sylow 3- and 11-subgroups of G. Call them H_3 and H_{11}, respectively. We claim that both lie in $Z(G)$.

Suppose H_3 is not in the center. Then, there is some $g \in G$ and $h \in H_3$ for which $ghg^{-1} \neq h$. But $ghg^{-1} \in H_3$ since H_3 is normal, and H_3 has only one other non-identity element, h^2. Thus, $ghg^{-1} = h^2$. Iterating conjugation by g once more, $g^2hg^{-2} = h$.

Continuing in this fashion, $g^{|g|}hg^{-|g|} = h$ if $|g|$ is even and h^2 if $|g|$ is odd. Also, $g^{|g|} = 1$ by definition, so $|g|$ is even. But G is a group of odd order so no element can have even order. Hence, $H_3 \subseteq Z(G)$.

Similarly, suppose H_{11} is not in the center. There is some $g \in G$ and $h \in H_{11}$ for which $ghg^{-1} = h^m$ for some $m \in \{2, \ldots, 10\}$. By the same argument as in Question 5, the order of g must be divisible by either 2 or 5. But neither is possible, since the order of g must divide $|G| = 33$. Thus $H_{11} \subseteq Z(G)$ as well.

Now, $Z(G)$ contains subgroups H_3 and H_{11} of orders 3 and 11 respectively. By Lagrange's theorem, $|Z(G)|$ must be divisible by $3 \cdot 11 = 33$, so $Z(G)$ is the whole group G, and G is abelian.

Question 7

If $|G| = 39 = 3 \cdot 13$, does G have to be abelian? Prove or give a counterexample.

No, let $G = \langle a, b | a^{13} = 1, b^3 = 1, bab^{-1} = a^3 \rangle$. The hard part is to check that G has exactly 39 elements, each of which can be represented uniquely as $a^i b^j$ for some $0 \leq i \leq 12$ and $0 \leq j \leq 2$. Alternately, we can just define the elements of our group to be the 39 symbols $a^i b^j$ for $0 \leq i \leq 12$ and $0 \leq j \leq 2$, and define the group multiplication by

$$(a^x b^y) \cdot (a^z b^w) = a^{x + 3^y z \bmod 13} b^{y+w \bmod 2}$$

[TC: this amounts to the semidirect product $\mathbb{Z}_{13} \rtimes \mathbb{Z}_3$ that we later saw in class.] This is a nonabelian group because $ab = b^3 a = b^2(ba)$ and $b^2 \neq 1$.