Student: Yu Cheng (Jade)

Math 611

Homework #3

October 09, 2010

Course Website Exercises

Exercise 3: Show that there is no simple group of order $112 = 2^4 \cdot 7$.

Answer: We will prove the given statement by contradiction. According to the Sylow Theorem, the number of Sylow p subgroups is congruent to 1 mod p.

$$n_2 = 1, 3, 5, 7, 9, \cdots$$

$$n_7 = 1, 8, 15, 22, \cdots.$$

According to the Sylow Theorem, if $|G| = p^k m$, the number of Sylow p subgroups divides m.

$$n_2 \mid 7 \Rightarrow n_2 = 1, or\ n_2 = 7$$

$$n_7 \mid 16 \Rightarrow n_7 = 1, or\ n_7 = 8\,.$$

Assume $n_2 = 7$ and let $H \in Sly_2(G)$. We have $|H| = 16$, $[G{:}\,H] = 7$. Let G act on the left cosets of H, there is a group homomorphism from G to S_7. It is defined as $\phi{:}\, G \to S_7$, $g \longmapsto \lambda_g$, where $\lambda_g(xH) = gxH$ for all $x \in G$. We can prove the group homomorphism as below:

$$\begin{aligned}\phi(g_1)\cdot\phi(g_2)(xH) &= \lambda_{g_1} \circ \lambda_{g_2}(xH)\\ &= \lambda_{g_1}(g_2xH)\\ &= g_1g_2xH\\ &= \lambda_{g_1g_2}(xH)\\ &= \phi(g_1g_2)(xH)\end{aligned}$$

$$\Rightarrow\ \phi(g_1)\cdot\phi(g_2) = \phi(g_1g_2)\,.$$

The previous exercise has derived the conclusion that for a simple group G with order greater than 2 and has a group homomorphism $\varphi{:}\, G \to S_k$, then image of φ satisfies $\varphi(G) \leq A_k$. Therefore, we have

$$Img(\phi) \leq A_7\,.$$

Since G is assumed to be simple, $Ker(\phi)$ is trivial, so $Img(\phi) \cong G$. Hence we have:

$$G \leq A_7 \Rightarrow |G| \mid \frac{7!}{2}$$

$$\Rightarrow 112 \mid \frac{7!}{2}.$$

This is a conflict. 112 does not divide $7!/2$. Hence $n_2 \neq 7, n_2 = 1$. Since we know that if $n_p = 1$, then P is the only Sylow p subgroup of G, and $P \lhd G$. Therefore, we've found a proper normal subgroup of G, namely, the Sylow 2 subgroup. We conclude, there is not simple group with order 112.

Exercise 4: Show that if $G/Z(G)$ is cyclic, then G is abelian. Use this to show that a group of order p^2, p is a prime, G is abelian.

Answer: All cyclic groups are abelian, so if $G/Z(G)$ is cyclic, then $G/Z(G)$ is an abelian group. And since $Z(G) \lhd G$, for all $a, b \in G$, $abZ(G)$ equals $\big(aZ(G)\big)\big(bZ(G)\big)$.

$$\big(aZ(G)\big)\big(bZ(G)\big) = \big(bZ(G)\big)\big(aZ(G)\big)$$

$$\Rightarrow abZ(G) = baZ(G)$$

$$\Rightarrow ab = ba\,.$$

Hence we've shown if $G/Z(G)$ is cyclic, then G is abelian. Now we will prove if $|G| = p^2$ where p is a prime, then G is abelian. Since $Z(G) \leq G$, we have $|Z(G)| \mid |G|$, hence, $|Z(G)|$ can be either $1, p$ or p^2.

Case #1: If $|Z(G)| = p^2 = |G|$, then $G = Z(G)$. By definition $Z(G)$ is abelian, so G is abelian.

Case #2: If $|Z(G)| = p$, then $|G/Z(G)| = p^2/p = p$. Lagrange's Theorem tells us that a group with prime order is cyclic. So $G/Z(G)$ is a cyclic group. We've also shown if $G/Z(G)$ is cyclic, then G is abelian. Hence G is abelian.

Case #3: we will show that $|Z(G)| = 1$ is not possible. Recall the class equation, where $C(y_i)$ is the centralizer for $y_i \in G$, $y_i \notin Z(G)$, and y_i is a SDR for its conjugacy class.

$$|G| = |Z(G)| + \sum_i [G: C(y_i)]\,.$$

The order of conjugacy class of G need to divide the order of G, hence every $[G: C(y_i)]$ divides $|G|$. In other words, p divides $[G: C(y_i)]$. So p divides $|G|$, and p divides $\sum_i [G: C(y_i)]$, in order for the class equation to hold, p has to divide $|Z(G)|$ as well. Therefore $|Z(G)| \neq 1$.

In summary, we've shown that a group of order p^2, where p is a prime, is an abelian group.

Exercise 5: Show that a group of order pq cannot be simple, where both p and q are primes.

Answer: If $p = q$, $|G| = p^2$, then as we've shown in the previous exercise that G is an abelian group. According to Sylow I theorem, if $p^k \mid |G|$ then $\exists H \leq G$ where $|H| = p^k$, so there exist a subgroup $K < G$ and $|K| = p$. Any subgroup of an abelian group is normal. Hence we've found a proper normal subgroup $K \lhd G$. G is not a simple.

If $p \neq q$, we will prove the given statement by contradiction. According to the Sylow Theorem, the number of Sylow p subgroups is congruent to 1 mod p.

$$n_p = 1, p + 1, 2p + 1, \cdots$$

$$n_q = 1, q + 1, 2q + 1, \cdots.$$

According to the Sylow Theorem, if $|G| = p^k m$, the number of Sylow p subgroups divides m.

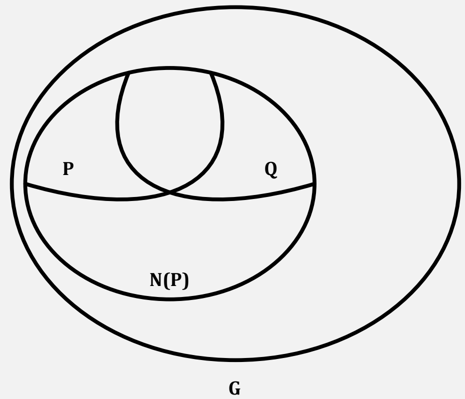
$$n_p \mid q \text{ and } n_q \mid p .$$

Without loss of generosity, we assume $p < q$. With this assumption, there is only possible value for the number of Sylow q subgroups, $n_q = 1$. Since we know that if $n_q = 1$, then Q is the only Sylow q subgroup of G, and $Q \lhd G$. Therefore, we've found a proper normal subgroup of G, namely, the Sylow q subgroup. Therefore, a group with order pq, where p, q are primes, cannot be a simple group.

Exercise 6: Let P be a Sylow p subgroup of a finite group G. Show that $N\big(N(P)\big) = N(P)$.

Answer: First we will show that $P\ char\ N(P)$. According to the properties of the characteristic subgroups, if there is only one subgroup of G with a certain cardinality, then this subgroup is a characteristic subgroup of G. This is due to the fact that group automorphisms preserve the subgroup structures. As the only subgroup with a certain cardinality, its elements would be sent back to this subgroup after applying any group automorphism on G.

We assume that there is another subgroup $Q \leq N(P)$ and $|P| = |Q| = p^k$, where $p^k \parallel |G|$. We have the following group structures in $N(P)$:



By definition, $P \lhd N(P)$, and now $Q \leq N(P)$, we could apply the *second isomorphism theorem*, and obtain the following conclusions:

$$PQ \leq G$$

$$P \lhd PQ$$

$$P \cap Q \lhd Q$$

$$PQ/P \cong Q/(P \cap Q)\ .$$

Based on these conclusions, we derive the following equations, where $p^k \parallel |G|$ and $r < k$,

$$P \lhd PQ \Rightarrow |PQ| = mP^k$$

$$P \cap Q \lhd Q \Rightarrow |P \cap Q| = p^r$$

$$PQ/P \cong Q/(P \cap Q) \Rightarrow \frac{|PQ|}{|P|} = \frac{|Q|}{|P \cap Q|}.$$

Plugging the values into the last equation, we can derive that m is a power of p.

$$\frac{mp^k}{p^k} = \frac{p^k}{p^r} \Rightarrow m = p^{k-r} > p\ .$$

This is a conflict. If m is a power of p, it means we have a subgroup, $PQ \leq G$, where $|PQ| = p^{k+\log_p m} > p^k$. But $p^k \parallel |G|$, k is the largest power of p such that p^k divides the order of G. Therefore, the assumption, there exist another group $Q \leq N(P)$ and $|Q| = |P|$, is not true. P is the only subgroup in $N(P)$ with the cardinality p^k. Therefore, we've shown $P\ char\ N(P)$.

We know that if $A\ char\ B \lhd C$ then $A \lhd C$.

$$P\ char\ N(P) \lhd N(N(P))$$

$$\Rightarrow P \lhd N(N(P))\ .$$

At the same time, we also know that $N(P)$ is the largest subgroup of G containing P as a normal subgroup. In other words, $N\big(N(P)\big)$ can't be any larger than $N(P)$. Therefore, we've shown that $N(P) = N\big(N(P)\big)$.