

1. Lecture 5

We see how the Sylow theorems can be used to understand structure of groups.

LEMMA 1. *Suppose $p < q$ are primes, and G is a group of order pq . Then G has a normal subgroup of order q .*

PROOF. By Sylow's second theorem, $s_q | p$, which implies that $s_q = 1$ or $s_q = p$. By Sylow's third theorem, $s_q \equiv 1 \pmod{q}$. Since $p < q$, $q \nmid p - 1$. Therefore, $s_q = 1$. Let Q be the unique Sylow q -subgroup of G . Since $G \curvearrowright \text{Syl}_q(G) = \{Q\}$ via conjugation, it follows that Q is normal. $\square$

A subgroup N of G is called *characteristic* if for every automorphism θ of G , $\theta(N) = N$. In this case, we write $N \text{ char } G$.

Since conjugation is given by inner automorphisms, every characteristic subgroup is normal. The converse does not always hold.

EXERCISE 2. Show that $(\mathbb{Z}/p\mathbb{Z})^2$ has no characteristic subgroup of order p , and note that all of its subgroups are normal.

LEMMA 3. *For $P \in \text{Syl}_p(G)$, the following statements are equivalent.*

- (1) $P \trianglelefteq G$.
- (2) $\text{Syl}_p(G) = \{P\}$.
- (3) $P \text{ char } G$.

PROOF. (1) $\Rightarrow$ (2) Since $P \trianglelefteq G$ and $P \in \text{Syl}_p(G)$, by Sylow's second theorem, $\text{Syl}_p(G) = \{P\}$.

(2) $\Rightarrow$ (3) Recall that $\text{Aut}(G) \curvearrowright \text{Syl}_p(G)$. Hence, for every

$$\theta \in \text{Aut}(G), \quad \theta(P) = P.$$

Thus, P is a characteristic subgroup of G .

(3) $\Rightarrow$ (1) is clear. $\square$

LEMMA 4. *Suppose $P \in \text{Syl}_p(G)$, and $P \subseteq H \subseteq G$ is an intermediate subgroup. Then $P \in \text{Syl}_p(H)$.*

PROOF. Note that P is a p -subgroup of H . We also have that $p \nmid [G : P]$ and $[H : P]$ divides $[G : P]$. Hence, $p \nmid [H : P]$. Thus, P is a Sylow p -subgroup of H . $\square$

The next lemma is an extremely useful observation.

LEMMA 5. *Suppose $P_1, P_2 \in \text{Syl}_p(G)$, and $P_1, P_2 \subseteq H$ where H is a subgroup of G . Then there exists $h \in H$ such that*

$$P_2 = hP_1h^{-1}.$$

PROOF. By Lemma 4, $P_1, P_2 \in \text{Syl}_p(H)$. Hence, by Sylow's second theorem, there exists $h \in H$ such that $P_2 = hP_1h^{-1}$. $\square$

COROLLARY 6. For every $P \in \text{Syl}_p(G)$, we have $\text{Syl}_p(N_G(P)) = \{P\}$.

PROOF. We make two observations (1) P is a Sylow p -subgroup of $N_G(P)$ since P is a p -group and $p \nmid [N_G(P) : P]$, (2) P is a normal subgroup of $N_G(P)$. Hence, by Sylow's second theorem, $\text{Syl}_p(N_G(P)) = \{P\}$. This completes the proof. $\square$

One may interpret Corollary 6 as a *canonical* assignment of P to $N_G(P)$. The following corollary makes this assertion more precise.

COROLLARY 7. For $\theta \in \text{Aut}(G)$ and $P \in \text{Syl}_p(G)$, we have

$$\text{Syl}_p(\theta(N_G(P))) = \{\theta(P)\};$$

in particular, $\theta(N_G(P)) = N_G(P)$ implies that $\theta(P) = P$.

PROOF. Note that $\theta(N_G(P)) = N_G(\theta(P))$ and $\theta(P) \in \text{Syl}_p(G)$. Hence, by Corollary 6, we have

$$\text{Syl}_p(\theta(N_G(P))) = \text{Syl}_p(N_G(\theta(P))) = \{\theta(P)\}.$$

$\square$

PROPOSITION 8. Suppose P is a Sylow p -subgroup of G . Then

$$N_G(N_G(P)) = N_G(P).$$

PROOF. Clearly, $N_G(P) \subseteq N_G(N_G(P))$. Suppose $g \in N_G(N_G(P))$. Let $c_g : G \rightarrow G$ be the inner automorphism given by the conjugation by g . Hence, $c_g \in \text{Aut}(G)$ and $c_g(N_G(P)) = N_G(P)$. Thus, by Corollary 7,

$$c_g(P) = P, \quad \text{which means} \quad gPg^{-1} = P.$$

Therefore, $g \in N_G(P)$. This implies that $N_G(N_G(P)) \subseteq N_G(P)$, which completes the proof. $\square$

(This result will be used later to show every Sylow subgroup of a *nilpotent* subgroup is normal.)

PROPOSITION 9. Suppose p is prime, and G is group of order $p(p-1)$. Then G has a characteristic subgroup of order p .

PROOF. By Sylow's second theorem, $s_p | p-1$; in particular, $s_p \leq p-1$. By Sylow's third theorem, $s_p \equiv 1 \pmod{p}$. Since $s_p \leq p-1$ and $s_p \equiv 1 \pmod{p}$, we deduce that $s_p = 1$. Let P be the unique subgroup of order p . Then P is a characteristic subgroup of G . $\square$

PROPOSITION 10. Suppose p is an odd prime, and G is a group of order $p(p+1)$. Then G has a normal subgroup of order either p or $p+1$. Moreover, if G does not have a normal subgroup of order p , then p is a Mersenne prime.

PROOF. Without loss of generality, we may assume that G does not have a normal subgroup of order p . This implies that $s_p \neq 1$. By Sylow's second theorem, $s_p | p + 1$. By Sylow's third theorem, $s_p \equiv 1 \pmod{p}$. Note that

$$s_p | p + 1, p | s_p - 1, s_p \neq 1 \quad \text{implies} \quad s_p = p + 1.$$

For every $P \in \text{Syl}_p(G)$, $s_p = [G : N_G(P)]$, and so $[G : N_G(P)] = p + 1$. Thus, $|N_G(P)| = p$, which implies that $N_G(P) = P$. Since P is cyclic, $P \subseteq C_G(P)$. Hence

$$P \subseteq C_G(P) \subseteq N_G(P) = P.$$

Thus, $C_G(P) = P = N_G(P)$.

(Interlude. Burnside's normal p -complement theorem: if $N_G(P) = C_G(P)$ for every $P \in \text{Syl}_p(G)$, then G has a normal subgroup N of order $[G : P]$ where P is a Sylow p -subgroup. Note that, by this theorem, Proposition 10 follows immediately. Since we will not prove this result in class, you may not use it unless explicitly told otherwise.)

The next statement is useful in other problems as well. So, we formulate it as a separate statement:

LEMMA 11. Suppose p is a prime factor of the order of a group G . Then

$$\bigcup_{P \in \text{Syl}_p(G)} P = \{x \in G \mid \text{ord}(x) \text{ is a power of } p\}.$$

PROOF. ($\subseteq$) For every $P \in \text{Syl}_p(G)$ and $x \in P$, the order of x divides $|P|$. Hence, the order of x is a power of p .

($\supseteq$) If the order of x is a power of p , then $\langle x \rangle$ is a p -subgroup of G . Hence, by Sylow's second theorem, there exists a Sylow p -subgroup P such that $\langle x \rangle \subseteq P$. Thus, $x \in \bigcup_{P \in \text{Syl}_p(G)} P$. $\square$

LEMMA 12. Suppose $v_p(|G|) = 1$, where v_p is the p -valuation. Then

$$\bigcup_{P \in \text{Syl}_p(G)} P \setminus \{1\} = \{g \in G \mid \text{ord}(g) = p\}.$$

Moreover, $f_p(G) = s_p(G)(p - 1)$.

PROOF. By $v_p(|G|) = 1$, we deduce that if the order of an element x of G is a power of p , then $\text{ord}(x)$ is either 1 or p . Hence, by Lemma 11, it follows that

$$\bigcup_{P \in \text{Syl}_p(G)} P \setminus \{1\} = \{x \in G \mid \text{ord}(x) = p\}.$$

Since the order of every element $x \in P \setminus \{1\}$ is p , we have $\langle x \rangle = P$. Thus, if P_1 and P_2 are distinct Sylow p -subgroups of G , then $P_1 \cap P_2 = \{1\}$. Therefore,

$\{P \setminus \{1\} \mid P \in \text{Syl}_p(G)\}$ consists of pairwise disjoint subsets of G . Hence,

$$\left| \bigcup_{P \in \text{Syl}_p(G)} P \setminus \{1\} \right| = s_p(G)(p-1).$$

This completes the proof. $\square$

Let $N := G \setminus \{g \in G \mid \text{ord}(g) = p\}$. Then by Lemma 12,

$$|N| = p(p+1) - (p-1)(p+1) = p+1 \quad \text{and} \quad \forall g \in G, gNg^{-1} = N.$$

We say that N is a normal subset. It remains to show that N is a subgroup.

Claim 1. If there exists a subgroup H of order $p+1$, then $H = N$; in particular, H is a normal subgroup of G .

PROOF OF CLAIM 1. For every $x \in H$, the order of x divides $p+1$, and so it is in N . Therefore, $H \subseteq N$. Since $|H| = |N|$, we deduce that $H = N$. This completes the proof. $\square$

Claim 2. For all $x \in P \setminus \{1\}$, $C_G(x) = P$.

PROOF OF CLAIM 2. Since $P = \langle x \rangle$, we have $C_G(x) = C_G(P) = P$. $\square$

Claim 3. For all $x \in N \setminus \{1\}$, $C_G(x) \subseteq N$.

PROOF OF CLAIM 3. Suppose to the contrary that there exists $y \in C_G(x) \setminus N$. Then, $y \in P \setminus \{1\}$. So, by Claim 2, $C_G(y) = P$, which implies that $x \in P$. This contradicts the assumption that $x \in N$. $\square$

Claim 4. For all $x \in N \setminus \{1\}$, $|cl(x)| = p$ and $|C_G(x)| = p+1$; and so by Claim 1, $C_G(x) = N$ is a normal subgroup.

PROOF. Since N is a normal set, $cl(x) \subseteq N \setminus \{1\}$. Hence, $|cl(x)| \leq p$.

By Claim 3, $|C_G(x)| \leq |N| = p+1$. Since

$$|G| = |C_G(x)||cl(x)| \leq p(p+1) = |G|,$$

it follows that both equalities should hold. $\square$

We leave the rest of the proof as an exercise. $\square$