CHAPTER 2

FINITE GROUPS

2.1 Cauchy Theorem

Lemma 2.1.1. *Let G be a p-group and X be a finite set that G acts on. Then, $|X^G| \equiv |X| \bmod p$.*

Proof. Let $|G| = p^n$. Since orbits form an equivalence relation, we know that

$$|X| = |X^G| + \sum_{i=1}^{n} p^i n_i,$$

where n_i is the number of orbits of length p^i. Hence, $|X^G| \equiv |X| \bmod p$. □

Proposition 2.1.2. *Let G be a p-group. Then, $Z(G)$ is not trivial.*

Proof. Let G act on itself via conjugation. Then, the fixed points are given by

$$\{x \in G \mid gxg^{-1} = x \forall g \in G\} = \{x \in G \mid gx = xg \forall g \in G\} = Z(G).$$

So, the lemma above tells us that $|Z(G)| \equiv |G| \bmod p$. Since G is a p-group, we find that $|Z(G)| \equiv 0 \bmod p$. We have $e \in Z(G)$, so we find that $|Z(G)| \geq p$. Hence, $Z(G)$ is not trivial. □

Corollary 2.1.3. *Let G be a group of order p^2, for some prime p. Then, G is abelian.*

Proof. We know that $Z(G)$ is a subgroup of G. So, $|Z(G)| \in \{1, p, p^2\}$. By the proposition above, we find that $|Z(G)| \neq 1$. Now, assume that $|Z(G)| = p$. Then, let $g \in G$ with $g \notin Z(G)$. Consider the centraliser subgroup $C_G(g)$. We have $Z(G) \leq C_G(g)$, and $g \in C_G(g)$. Hence $|C_G(g)| \geq p + 1$. By Lagrange's Theorem, we must have that $C_G(g) = G$. That is, for all $x \in G$, $gx = xg$, meaning that $g \in Z(G)$. This is a contradiction. So, we must have $|Z(G)| = p^2$. Hence, G is abelian. □

Theorem 2.1.4 (Cauchy Theorem)**.** *Let G be a finite group of order dividing some prime p. Then, there exists a $g \in G$ with $|g| = p$.*

Proof. Define the set

$$X = \{(g_1, \dots, g_p) \mid g_1 \dots g_p = e\}.$$

By construction, $|X| = |G|^{p-1}$- we can freely choose $g_1, \dots, g_{p-1}$ and set $g_p = (g_1 \dots g_{p-1})^{-1}$. Since G has order dividing p, $|X| \equiv 0 \bmod p$. We can define the action from the group $\mathbb{Z}/p\mathbb{Z}$ on the set X by reorder, i.e.

$$(1 + p\mathbb{Z}) \cdot (g_1, g_2, \dots, g_p) = (g_2, \dots, g_p, g_1),$$

extended as a homomorphism. This is well-defined since

$$g_1 g_2 \dots g_p = e \iff g_2 \dots g_p = g_1^{-1} \iff g_2 \dots g_p g_1 = e.$$

Now, since $\mathbb{Z}/p\mathbb{Z}$ is a p-group, we find that $|X^G| \equiv 0 \bmod p$. We have

$$\begin{aligned} X^G &= \{(g_1, \dots, g_p) \in X \mid n \cdot (g_1, \dots, g_p) = (g_2, \dots, g_1) \ \forall n \in \mathbb{Z}/p\mathbb{Z}\} \\ &= \{(g, \dots, g) \mid g \in G, g^p = e\}. \end{aligned}$$

We know that the element $(e, \dots, e) \in X^G$. So, $|X^G| \geq 1$. Since $|X^G| \equiv 0 \bmod p$, we find that $|X^G| \geq p > 1$. In particular, there exists a $g \in G$ with $g \neq e$ such that $g^p = e$. Hence, $|g| = p$. $\square$

2.2 Sylow Theorems

Lemma 2.2.1. *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$, and let $H \leq G$ be a p-subgroup. Then, $[G : H] \equiv [N_G(H) : H] \bmod p$. In particular, if H has order p^i for $i < n$, then $N_G(H) \neq H$.*

Proof. Let $X = G/H$ be the set of left cosets of H in G. Then, H acts on X by left multiplication, i.e. $h \cdot gH = hgH$. We have

$$\begin{aligned} X^H &= \{gH \in G/H \mid hgH = gH \ \forall h \in H\} \\ &= \{gH \in G/H \mid g^{-1}hg \in H \ \forall h \in H\} \\ &= \{gH \in G/H \mid gHg^{-1} = H\} = N_G(H)/H. \end{aligned}$$

Hence,

$$[G : H] = |X| \equiv |X^H| = [N_G(H) : H] \bmod p.$$

□

Theorem 2.2.2 (Sylow I). *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$. Then, for all $1 \leq i \leq n$, G has a subgroup of order p^i. Moreover, for all $1 \leq i < n$ and a subgroup H_i of order p^i, there exists a subgroup K_i of order p^{i+1} such that $H_i \lhd K_i$.*

Proof. We show this by induction. By Cauchy's Theorem, we know that there exists a subgroup of order p, so the statement holds for $i = 1$. Now, assume the statement holds for some $1 \leq i < n$. Hence, there exists a subgroup $H_i \leq G$ of order p^i. By the result above, we know that $N_G(H_i) \neq H_i$. Therefore, the quotient $N_G(H_i)/H_i$ is not trivial. Moreover, $[G : H_i] \equiv 0 \bmod p$ since $i \neq n$. Hence, $[N_G(H_i) : H_i] \equiv 0 \bmod p$. By Cauchy's Theorem, there exists a $gH_i \in N_G(H_i)/H_i$ such that $|gH_i| = p$. We know that $\langle gH \rangle = H_{i+1}/H_i$ by correspondence theorem, for some subgroup $H_i \leq H_{i+1} \leq N_G(H_i)$. Since $|H_{i+1}/H_i| = p$, we find that $|H_{i+1}| = p^{i+1}$. So, there exists a subgroup H_{i+1} of order p^{i+1}. Moreover, since $H_{i+1} \leq N_G(H_i)$, we must have $H_i \lhd H_{i+1}$. So, the result follows from induction. □

Definition 2.2.3. Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$, and let $H \leq G$. We say that H is a *Sylow-p subgroup* if $|H| = p^n$.

Theorem 2.2.4 (Sylow II). *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$. Then, all the Sylow-p subgroups are conjugate.*

Proof. Let H and K be Sylow-p subgroups. We show that H and K are conjugate. Let $X = G/H$ be the set of left cosets of H in G. Then, K acts on X by left multiplication, i.e. $k \cdot gH = kgH$. We know that $|X^K| \equiv X \bmod p$. Since $|X^K| = m$, we find that $|X^K| \not\equiv 0 \bmod p$. Hence, there exists a $gH \in X^K$. This implies that for all $k \in K$, $k \cdot gH = gH$. Therefore, $g^{-1}kg \in H$ for all $k \in K$. Since H and K have the same cardinality, we must have that $g^{-1}Kg = H$. So, H and K are conjugate. □

Theorem 2.2.5 (Sylow III). *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$. Then, the number of Sylow-p subgroups, n_p, satisfies the following:*

- *$n_p \equiv 1 \bmod p$; and*

- $n_p \mid m$.

Proof. Let $X = \mathrm{Syl}_p(G)$ be the set of all the Sylow-p subgroups in G, and fix $H \in X$. Then, H acts on X by conjugation- this is well-defined by Sylow II. We know that $H \in X^H$, so the set of fixed points X^H is not empty. In that case, let $K \in X^H$. We claim that $K = H$. Since $K \in X^H$, we find that for all $h \in H$, $hKh^{-1} = K$. Hence, $H \leq N_G(K)$. Since $N_G(K) \leq G$, we find that H and K are both Sylow-p subgroups in $N_G(K)$ as well. By Sylow II, we can find a $g \in N_G(K)$ such that $H = gKg^{-1}$. Moreover, since $g \in N_G(K)$, we also have $gKg^{-1} = K$. Hence, $H = K$. This implies that $X^H = \{H\}$. Therefore,

$$n_p = |X| \equiv |X^H| = 1 \bmod p.$$

Now, let G act on X by conjugation. By Sylow II, we know that this action has precisely one orbit, of size n_p. So, the Orbit-Stabliser theorem tells us that $n_p \mid p^n m$. Moreover, since $n_p \nmid p$, we find that $n_p \mid m$. □

Corollary 2.2.6. *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$. Then, $n_p = [G : N_G(H)]$, where H is a Sylow-p subgroup.*

Proof. Let G act on X by conjugation. We have $|\,\mathrm{Orb}_G(H)| = n_p$. Moreover,

$$\mathrm{Stab}_G(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H).$$

Hence, the Orbit-Stabliser theorem tells us that $n_p = [G : N_G(H)]$. □

Lemma 2.2.7. *Let G be a group of order $p^n m$, for a prime p with $(p, m) = 1$. Then, $n_p = 1$ if and only if there exists a Sylow-p subgroup that is normal in G.*

Proof. First, assume that $n_p = 1$. Let H be the Sylow-p subgroup, and let $g \in G$. We know that gHg^{-1} is also a Sylow-p subgroup. But, since $n_p = 1$, we find that $gHg^{-1} = H$. Hence, H is normal in G.

Now, assume that $H \leq G$ is a Sylow-p subgroup that is normal in G. Let K be a Sylow-p subgroup. By Sylow II, we find that H and K are conjugate. But, since H is normal, we find that $K = H$. So, $n_p = 1$. □

Proposition 2.2.8. *Let G be a finite group, and let $H \leq G$ such that $(|H|, [G : H]) = 1$. Then, $H \lhd G$ if and only if H is the unique subgroup of order $|H|$.*

Proof. First, assume that H is the unique subgroup of order $|H|$, and let $g \in G$. We know that gHg^{-1} is also a subgroup of order $|H|$. Hence, we have $gHg^{-1} = H$. So, H is normal in G.

Now, assume that $H \lhd G$. Let K be a subgroup of order $|H|$. Consider the restriction of the quotient map $q : K \to G/H$. This is a homomorphism. Moreover, since $|K|$ and $|G/H|$ are coprime, the first isomorphism theorem tells us that q is the trivial homomorphism. Hence, for all $k \in K$, $kH = H$, and so $K \subseteq H$. Since K and H have the same cardinality, this implies that $K = H$. So, H must be the unique subgroup of order $|H|$. □

2.3 Consequence of Sylow Theorems

Proposition 2.3.1. *A group of order 15 is cyclic.*

Proof. Let G be a group of order $15 = 3 \cdot 5$. Let G have n_3 Sylow-3 subgroups and n_5 Sylow-5 subgroups. By Sylow III, we know that $n_3 \equiv 1 \bmod 3$ and $n_3 \in \{1, 5\}$, and $n_5 \equiv 1 \bmod 5$ and $n_5 \in \{1, 3\}$. This implies that both $n_3 = 1$ and $n_5 = 1$. So, let H be the Sylow-3 subgroup and K be the Sylow-5 subgroup. We know that both H and K are normal in G. Moreover, $H \cap K = \{e\}$. This implies that $HK \leq G$ with $HK \cong H \times K$. Since $|H| = 3$ and $|K| = 5$, we find that $G = HK$. Since H and K are cyclic groups of coprime order, we know that $G \cong H \times K$ must be cyclic. □

Proposition 2.3.2. *Let p and q be primes with $p < q$ and $q \not\equiv 1 \bmod p$. Then, a group of order pq is cyclic.*

Proof. Let G be a group of order pq. Let G have n_p Sylow-p subgroups and n_q Sylow-q subgroups. By Sylow III, we know that $n_p \equiv 1 \bmod p$ and $n_p \in \{1, q\}$. Since $q \not\equiv 1 \bmod p$, we find that $n_p = 1$. Similarly, $n_q \equiv 1 \mod q$ and $n_q \in \{1, p\}$. Since $p < q$, we find too that $n_q = 1$. Hence, $G \cong H \times K$ must be cyclic. □

Proposition 2.3.3. *A group of order 45 is abelian.*

Proof. Let G be a group of order $45 = 3^2 \cdot 5$. Let G have n_3 Sylow-3 subgroups and n_5 Sylow-5 subgroups. By Sylow III, we know that both $n_3 = 1$ and $n_5 = 1$. So, let H be the Sylow-3 subgroup and K be the Sylow-5 subgroup. We find that $G \cong H \times K$. A group of order 5 or $9 = 3^2$ must be abelian. Hence, G is abelian. □

Proposition 2.3.4. *A group of order 18 is not simple.*

Proof. Let G be a group of order $18 = 2 \cdot 3^2$. Let G have n_2 Sylow-2 subgroups and n_3 Sylow-3 subgroups. By Sylow III, we know that $n_2 \in \{1, 3, 9\}$ and $n_3 = 1$. In that case, there exists a proper, non-trivial normal subgroup of G, with order 9. Hence, G is not simple. □

Proposition 2.3.5. *A group of order 12 is not simple.*

Proof. Let G be a group of order $12 = 2^2 \cdot 3$. Let G have n_2 Sylow-2 subgroups and n_3 Sylow-3 subgroups. By Sylow III, we know that $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4\}$. If $n_3 = 1$, then G has a normal Sylow-3 subgroup. Otherwise, we have $n_3 = 4$ subgroups of order 3. In that case, there exist $4 \cdot 2 = 8$ elements of order 3 in G. Since $n_2 \geq 1$, we must have that the remaining 4 elements form the single Sylow-2 subgroup. So, $n_2 = 1$. Hence, either $n_3 = 1$ or $n_2 = 1$. Therefore, there exists a proper, non-trivial normal subgroup of G, with order either 4 or 3. Hence, G is not simple. □

Proposition 2.3.6. *A group of order 48 is not simple.*

Proof. Let G be a group of order $48 = 2^4 \cdot 3$. By Sylow III, we know that $n_3 \in \{1, 3\}$. If $n_3 = 1$, then we have a normal Sylow-3 subgroup. Otherwise, we have $n_3 = 3$. Let H and K be two of the Sylow-3 subgroups. We know that

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{2^4 \cdot 2^4}{|H \cap K|} \leq 2^4 \cdot 3.$$

Since $H \neq K$, we must have $|H \cap K| = 8$. So, we have $[H : H \cap K] = 2 = [K : H \cap K]$. This implies that $H, K \lhd H \cap K$. Hence, $H, K \leq N_G(H \cap K)$. Therefore, $HK \subseteq N_G(H \cap K)$. We know that

$$|HK| = \frac{|H||K|}{|H \cap K|} = 32.$$

So, Lagrange's theorem tells us that $N_G(H \cap K) = G$. That is, $H \cap K \lhd G$. This implies that G has a normal subgroup of order 8. So, G is not simple. □

Proposition 2.3.7. *A group of order 255 is abelian. In particular, it is cyclic.*

Proof. Let G be a group of order $255 = 3 \cdot 5 \cdot 17$. By Sylow III, we have $n_{17} = 1$. So, let H be the Sylow-17 subgroup. In that case, G/H is a group of order 15. Since $5 \not\equiv 1 \mod 3$, we find that G/H is abelian. Hence, the commutator $[G, G] \leq H$. Now, by Sylow III, we have $n_3 \in \{1, 85\}$ and $n_5 \in \{1, 51\}$. If $n_3 = 85$ and $n_5 = 51$, then there are at least

$$85 \cdot 2 + 51 \cdot 4 = 374$$

elements in G- this is a contradiction. So, we must have either $n_3 = 1$ or $n_5 = 1$. So, let K be the unique Sylow-3 or the Sylow-5 subgroup. Since both $17 \not\equiv 1 \mod 3$ and $17 \not\equiv 1 \mod 5$, we find that G/K is abelian. Hence, $[G, G] \leq K$. So, $[G, G] \leq H \cap K$. By Lagrange, we find that $H \cap K = \{e\}$. This implies that G is abelian. □

Proposition 2.3.8. *A p-group is solvable.*

Proof. Let $|G| = p^n$, for some prime p. By Cauchy's Theorem, we know that G has a subgroup $H_1 \leq G$ of order p. By Sylow I, there exists a subgroup $H_2 \leq G$ of order p^2 such that $H_2 \lhd H_1$. We can keep applying Sylow I to find subgroups $H_i \leq G$ of order p^i such that $H_i \lhd H_{i-1}$, for $2 \leq i \leq n$. Then, the following is a normal series for G:

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G.$$

We have $|H_{i+1}/H_i| = p$, so the quotient is abelian. Hence, G is solvable. □

Proposition 2.3.9. *Let G be a finite abelian group and let $m \in \mathbb{Z}_{\geq 1}$ divide $|G|$. Then, G has a subgroup of order m.*

Proof. Let the prime factorisation of m be:

$$m = p_1^{\alpha_1} \ldots p_n^{\alpha_n}.$$

By Sylow I, we know that G has a subgroup $P_i \leq G$ of order $p_i^{\alpha_i}$ for all $1 \leq i \leq n$. Since G is abelian, we know that $P_i \lhd G$. So, we find that

$$P = P_1 P_2 \ldots P_n$$

is a (normal) subgroup of G. By Lagrange, we find that for $1 \leq i, j \leq n$, if $i \neq j$, then $P_i \cap P_j = \{e\}$. So, it follows that $|P| = p_1^{\alpha_1} \ldots p_n^{\alpha_n} = m$. $\square$