8. The Sylow Theorems

In the sequel, $G$ is always a finite group.

**Definition.** For $a \in G$, the set $C(a) := \{x \in G : xax^{-1} = a\}$ is called the centralizer of $a$ in $G$.

Note that $x \in C(a)$ iff $xa = ax$, and that for any $a \in G$ we have $a \in C(a)$.

**Fact 8.1.** For any $a \in G$, $C(a) \leq G$.

**Proof.** We have to verify the axioms $(A0)$, $(A1)$ and $(A2)$.

(A0) For $x, y \in C(a)$ we have

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy),$$

hence, $xy \in C(a)$.

(A1) $ea = ae$, thus, $e \in C(a)$.

(A2) If $x \in C(a)$, then

$$x^{-1}a = x^{-1}a(x^{-1}) = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = (x^{-1}xa)x^{-1} = ax^{-1},$$

hence, $x^{-1} \in C(a)$. ⊥

**Definition.** For $a \in G$, the set orbit$(a) := \{xax^{-1} : x \in G\}$ is called the orbit of $a$.

**Fact 8.2.** For $a, a' \in G$ we either have orbit$(a) = \text{orbit}(a')$ or orbit$(a) \cap \text{orbit}(a') = \emptyset$.

Further, $|\text{orbit}(a)| = 1$ iff $a \in Z(G)$.

**Proof.** If orbit$(a) \cap \text{orbit}(a') \neq \emptyset$, then $xax^{-1} = y_{a'}y^{-1}$ (for some $x, y \in G$). Thus, $a' = y^{-1}xax^{-1}y = y^{-1}xa(y^{-1}x)^{-1} \in \text{orbit}(a)$ and $a = x^{-1}ya'y^{-1}x = x^{-1}ya'(x^{-1}y)^{-1} \in \text{orbit}(a')$, which implies that orbit$(a) = \text{orbit}(a')$.

If $|\text{orbit}(a)| = 1$, then for all $x \in G$ we have $xax^{-1} = a$, thus, for all $x \in G$ we have $xa = ax$, which implies $Z(G)$. On the other hand, if $a \in Z(G)$, then $xax^{-1} = a$ (for all $x \in G$), thus, $|\text{orbit}(a)| = 1$. ⊥

**Lemma 8.3.** For every $a \in G$ we have

$$|\text{orbit}(a)| = |G : C(a)|.$$

**Proof.** $|G : C(a)| = |G/C(a)| = |\{xC(a) : x \in G\}|$. Further, we have

$$xC(a) = yC(a) \iff x^{-1}y \in C(a) \iff (x^{-1}ya^{-1}x = a \iff yay^{-1} = xax^{-1},$$

which implies that $|\{xax^{-1} : x \in G\}| = |\{xC(a) : x \in G\}|$. ⊥

As a consequence of Fact 8.2 and Lemma 8.3 we get

**Corollary 8.4.** Let $a_1, \ldots, a_n$ be representatives for the $n$ orbits which have size larger than 1. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |\text{orbit}(a_i)| = |Z(G)| + \sum_{i=1}^{n} |G : C(a_i)|.$$

**Proposition 8.5.** If $G$ is a group of order $p^2$, where $p$ is prime, then $G$ is abelian.
Proof. Assume that G is not abelian, then, by Corollary 8.4, we can choose some \( a_1, \ldots, a_n \in G \) such that \( |\text{orbit}(a_i)| > 1 \) (for all \( a_i \in \{a_1, \ldots, a_n\} \)) and \( p^2 = |G| = |Z(G)| + \sum_{i=1}^{n} |G : C(a_i)| \). By Lemma 8.3, for each \( a_i \in \{a_1, \ldots, a_n\} \) we get \( 1 < |\text{orbit}(a_i)| = |G : C(a_i)| \), so, \( p \mid |C(a_i)| \), and therefore \( p \mid |Z(G)| \) which implies that \( |Z(G)| \geq p \).

If we assume that \( G \) is not abelian, then \( Z(G) \neq G \), thus, \( |Z(G)| = p \).

Choose some \( x \in G \setminus Z(G) \), then \( Z(G) \triangleleft C(x) \), and since \( x \in C(x) \) we get \( |C(x)| \geq p + 1 \). Now, since \( C(x) \leq G \), \( |C(x)| \mid |G| = p^2 \), and because \( |C(x)| \geq p + 1 \) we get \( C(x) = G \), thus \( x \in Z(G) \), which is absurd. Hence, we must have \( Z(G) = G \), which shows that \( G \) is abelian. \( \square \)

**Theorem 8.6 (Cauchy).** Suppose that \( p \mid |G| \) for some prime number \( p \). Then there is an element \( g \in G \) of order \( p \).

**Proof.** The proof is by induction on \( |G| \). If \( |G| = 1 \), then the result is vacuously true. Now, let us assume that \( |G| > 1 \) and that for every proper subgroup \( H < G \) we have \( p \nmid |H| \), (in other words, \( p \nmid |G : H| \)), else we are home by induction. By Corollary 8.4 and by our assumptions we get \( p \mid |Z(G)| \), so, \( G = Z(G) \) which implies that \( G \) is abelian. A proper subgroup \( H \triangleleft G \) is called maximal if \( H \leq H' \leq G \) implies \( H' = H \) or \( H' = G \). If \( H, K \) are distinct maximal proper subgroups of \( G \), then \( HK \leq G \) (since \( G \) is abelian) and by maximality of \( H \) and \( K \) we get \( HK = G \) (since \( H, K \leq HK \)).

Now, \( |G| = |HK| = \frac{|H||K|}{|H \cap K|} \), but because \( p \nmid |H| \) and \( p \nmid |K| \), this implies \( p \nmid |G| \), which is a contradiction. Therefore, \( G \) has a unique maximal proper subgroup, say \( M \). Since \( M \) is the only maximal proper subgroup of \( G \), all proper subgroups \( H < G \) are subgroups of \( M \). Choose \( g \in G \) with \( g \notin M \), then \( \langle g \rangle = G \), (since otherwise, \( \leq g \triangleleft M \) ), and hence, \( G \) is cyclic. The order of \( g \) is \( |G| \), and if we put \( n = \frac{|G|}{p} \), then \( \langle g^n \rangle \) is a subgroup of \( G \) of order \( p \), which completes the proof. \( \square \)

**Definition.** Let \( H \leq G \), then the set \( N(H) := \{ x \in G : xHx^{-1} = H \} \) is called the **normalizer** of \( H \) in \( G \), and \( \text{orbit}(H) := \{ xHx^{-1} : x \in G \} \) is called the **orbit** of \( H \).

**Fact 8.7.** For every \( H \leq G \), \( N(H) \leq G \) and \( |\text{orbit}(H)| = |G : N(H)| \).

**Proof.** Just follow the proofs of Fact 8.1 and Lemma 8.3. \( \square \)

**Fact 8.8.** For every \( H \leq G \), \( H \leq N(H) \).

**Proof.** By definition, for every \( x \in N(H) \) we have \( xHx^{-1} = H \), thus, \( H \leq N(H) \). \( \square \)

**Lemma 8.9.** Let \( G \) be such that \( |G| = p^m n \), where \( p \) is prime, \( m, n > 0 \) and \( p \nmid n \), and let \( P, Q \leq G \) be such that \( |P| = |Q| = p^m \). Then \( Q \leq N(P) \) if and only if \( Q = P \).

**Proof.** Of course, \( Q = P \) implies \( Q \leq N(P) \). On the other hand, if \( Q \leq N(P) \), then, since \( P \leq N(P) \) (by Fact 8.8), \( PQ \leq N(P) \leq G \). Thus,

\[
|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{p^m \cdot p^m}{|P \cap Q|}
\]

must divide \( |G| = p^m n \), which implies \( |P \cap Q| = p^m \), hence, \( Q = P \). \( \square \)
Definition. Let $G$ be a finite group of order $p^m n$, where $p$ is prime and does not divide $n$. Then any subgroup of $G$ of order $p^m$ is called a Sylow $p$-subgroup of $G$, and the set of all such subgroups of $G$ is denoted $\text{Syl}_p(G)$.

In order to state Sylow’s Theorem, we need one more definition.

Definition. Two subgroups $H_1$ and $H_2$ of a group $G$ are called conjugate in $G$ if $H_1 = xH_2x^{-1}$ for some $x \in G$.

Theorem 8.10 (Sylow). Let $G$ be a finite group of order $p^m n$, where $p$ is prime and does not divide $n$.

(i) There is a Sylow $p$-subgroup $P$ of $G$.

(ii) All elements of $\text{Syl}_p(G)$ are conjugate in $G$.

(iii) $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$.

(iv) $|\text{Syl}_p(G)| | n$.

Proof. We prove (i) by induction on $|G|$. If $|G| = 1$, then the result is vacuously true, and therefore we may assume that $|G| > 1$. By Corollary 8.4 we have $|G| = |Z(G)| + \sum_{j=1}^{s} |G : C(x_j)|$, where the $x_j$ are a collection of representatives for those orbits which are not singletons. Thus, each $C(x_j)$ is a proper subgroup of $G$. If $p \nmid |G : C(x_j)|$ for every $1 \leq j \leq s$, then $p \nmid |Z(G)| \neq 1$. Thanks to Cauchy’s Theorem 8.6 we can choose $z \in Z(G)$ of order $p$, so, since $z \in Z(G)$, $\langle z \rangle \leq G$. Let $\pi : G \rightarrow G/\langle z \rangle$ be the natural projection. By induction, there is a Sylow $p$-subgroup $P_1$ of $G/\langle z \rangle$. This group has order $p^{m-1}$, since $|G/\langle z \rangle| = p^{m-1} n$. The preimage of $P_1$ under $\pi$ is $P \leq G$, where $P/\langle z \rangle$ has order $p^{m-1} = \frac{|P|}{p}$. Thus, $|P| = p^m$ and we have found a Sylow $p$-subgroup $P$ of $G$. The other possibility is that there is some $x_j$ with $p \nmid |G : C(x_j)|$, so, $|G : C(x_j)| = p^m k$ with $k < n$ and $p \nmid k$. By induction, $C(x_j)$ has a Sylow $p$-subgroup $P$ of order $p^m$, and since $P \leq G$, $P$ is a Sylow $p$-subgroup of $G$.

For part (ii) and (iii), let $P$ be a Sylow $p$-subgroup of $G$. Let $\Omega = \{xPx^{-1} : x \in G\}$ denote the set of all $G$-conjugates of $P$. Now, by Fact 8.7 we have $|\Omega| = |G : N(P)|$.

Further, for $P_i \in \Omega$, let $\Omega_i = \{yP_iy^{-1} : y \in P\}$, then $\Omega$ is the disjoint union of some $\Omega_i$’s, so, $|\Omega| = \sum_i |\Omega_i|$. Again by Fact 8.7 we get $|\Omega_i| = |P : N(P_i) \cap P|$, which tells us that the orbits $\Omega_i$ have size divisible by $p$, unless $P \leq N(P_i)$, in which case $|\Omega_i| = 1$ and $P = P_i$ (by Lemma 8.9). Hence, of the orbits $\Omega_i$ there is exactly one of length 1 and all the others have size divisible by $p$, thus, $|\Omega| = \sum_i |\Omega_i| \equiv 1 \pmod{p}$. If we can show that $\Omega = \text{Syl}_p(G)$, then we are done. So, assume towards a contradiction that $\Omega \neq \text{Syl}_p(G)$, which means that there is a Sylow $p$-subgroup $Q$ which is not a conjugate of $P$. Now, all $Q$-orbits $\Omega_i = \{yP_iy^{-1} : y \in Q\}$, where $P_i \in \Omega$ have size divisible by $p$, since otherwise, $Q \leq N(P_i)$ (for some $i$) and therefore $Q = P_i$ (by Lemma 8.9), which implies that $Q$ is a conjugate of $P$. Since $\Omega$ is a disjoint union of sets – namely the $\Omega_i$’s – of size divisible by $p$ we deduce that $|\Omega| \equiv 0 \pmod{p}$. However, we already know that $|\Omega| \equiv 1 \pmod{p}$ so this is absurd. Thus, $\Omega = \text{Syl}_p(G)$, which implies that all Sylow $p$-subgroups of $G$ are conjugate and $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$.

To verify (iv), let $P \in \text{Syl}_p(G)$. Then, by (ii), $\text{Syl}_p(G) = \{xPx^{-1} : x \in G\}$, and by Fact 8.7 we get $|\text{Syl}_p(G)| = |G : N(P)|$. Since $P \leq N(P)$ it follows that $p^m | |N(P)|$, and so $|G : N(P)|$ must divide $n$. $\square$
As a consequence of Theorem 8.10 (ii) we get

**Corollary 8.11.** Let $G$ be a finite group of order $p^mn$, where $n,m > 0$ and $p$ is prime and does not divide $n$. Then $|\text{Syl}_p(G)| = 1$ if and only if the unique Sylow $p$-subgroup is a normal subgroup of $G$. In particular, $|\text{Syl}_p(G)| = 1$ implies that $G$ is not simple.