1.10 The First Sylow Theorem

Named after Ludwig Sylow (1832–1918), the Sylow Theorems detail the number of subgroups of fixed order in a given finite group. They form a fundamental part of finite group theory and play a significant role in the classification of finite groups.

1.10.1 Lemma. *Let G be a group, whose order is a power of a prime number p, acting on the set X. Setting $X^G := \{x \in X \mid gx = x \text{ for all } g \in G\}$, we have $|X^G| \equiv |X| \pmod{p}$.*

Proof. Proposition 1.9.8 implies that the subset $X \setminus X^G$ is a disjoint union of G-orbits having cardinality greater than 1. Corollary 1.9.11 establishes that the cardinality of each such orbit is a power of p distinct from $p^0 = 1$ and hence divisible by p. □

1.10.2 Corollary. *The center of group, whose order is a power of a prime number p, is non-trivial.*

Proof. Let G be a group with order a power of the prime number p. The group G acts on itself by conjugation and the set of fixed points is the centre $Z(G)$. Lemma 1.10.1 demonstrates that

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}$$

whence $|Z(G)| \neq 1$ and $Z(G) \neq \{e\}$. □

A subgroup with order is a power of a prime number p is a Sylow p-subgroup if its index is not a multiple of p.

1.10.3 Definition. Given a group of order $p^r m$ where the integer m is not a multiple of the prime number p, a ***Sylow p-subgroup*** is a subgroup of order p^r.

1.10.4 Example. Any subgroup of $\mathfrak{S}_p$ generated by a cycle of length p is a Sylow p-group because p does not divide $(p-1)!$. ⋄

1.10.5 Lemma (Wielandt 1959). *For a positive integer $n = p^r m$ where p is a prime number relatively prime to m, we have $\binom{n}{p^r} \not\equiv 0 \pmod{p}$.*

Proof. Let P be a group of order p^r and let T be a set with m elements. Consider $X := P \times T$ and let $\mathcal{S}$ be the set of subsets of X with p^r elements. By construction, we have $|X| = n$ and $|\mathcal{S}| = \binom{n}{p^r}$. The group P acts on X by $p(x,t) := (px, t)$ and this action extends to $\mathcal{S}$. The fixed-point set $\mathcal{S}^P$ is the set of orbits of X. Elements in $\mathcal{S}^P$ are subsets $Y \subseteq X$ of the form $P \times \{t\}$ where $t \in T$, so $|\mathcal{S}^P| = m$. Lemma 1.10.1 implies that $\binom{n}{p^r} = |\mathcal{S}| \equiv |\mathcal{S}^P| = m \not\equiv 0 \pmod{p}$. □

A finite group, whose order is divisible by a prime number p, contains a subgroup of index relatively prime to p that has order a power of p.

1.10.6 Theorem (Sylow 1872). *Every finite group contains, for any prime number p dividing the order of the group, a Sylow p-subgroup.*

Proof. Let G be a finite group with $|G| = n = p^r m$ where m is not a multiple of p. If $\mathcal{S}$ is the set of p^r-subsets of G, then Lemma 1.10.5

shows that $|\mathcal{S}| = \binom{n}{p^r} \not\equiv 0 \pmod{p}$. Left translation on G induces an action of the group G on the set $\mathcal{S}$. Since the cardinality of $|\mathcal{S}|$ is the sum of the cardinalities of the G-orbits, there exists $U \in \mathcal{S}$ whose G-orbit has nonzero cardinality modulo p. Corollary 1.9.11 establishes that $p^r m = |G| = |\operatorname{stab}_G(U)|\,|\operatorname{orb}_G(U)|$ which means p^r divides $|\operatorname{stab}_G(U)|$. However, $\operatorname{stab}_G(U)$ consists of the elements $g \in G$ such that $gU = U$; if $u \in U$ then $\operatorname{stab}_G(U) \subseteq Uu^{-1}$ whence $|\operatorname{stab}_G(U)| \leqslant |U| = p^r$. We conclude that $|\operatorname{stab}_G(U)| = p^r$. □

1.10.7 Corollary (Cauchy 1845). *Any group whose order is divisible by a prime number p contains an element of order p.*

Proof. By the First Sylow Theorem, there exists a subgroup of order p^r for some positive integer r. Choose an element g in this subgroup other than the identity. By the Lagrange Theorem, the order of g divides p^r. Hence, there exists an integer k such that $0 < k \leqslant r$ and g has order p^k. It follows that the element $g^{p^{k-1}}$ has order p. □

The symmetric group $\mathfrak{S}_3$ must be isomorphic to the dihedral group D_3.

1.10.8 Problem. Demonstrate that, for the groups of order 6, there are two isomorphism classes: the class of the cyclic group μ_6 and the class of the symmetric group $\mathfrak{S}_3$.

$\star$	e	f	f^2	g	fg	f^2g
e	e	f	f^2	g	fg	f^2g
f	f	f^2	e	fg	f^2g	g
f^2	f^2	e	f	f^2g	g	fg
g	g	fg	f^2g	e	f	f^2
fg	fg	f^2g	g	f	f^2	e
f^2g	f^2g	g	fg	f^2	e	f

$\star$	e	f	f^2	g	fg	f^2g
e	e	f	f^2	g	fg	f^2g
f	f	f^2	e	fg	f^2g	g
f^2	f^2	e	f	f^2g	g	fg
g	g	f^2g	fg	e	f^2	f
fg	fg	g	fg	f	e	f
f^2g	f^2g	fg	g	f^2	f	e

Figure 1.9: Multiplication tables for groups of order 6

Solution. Consider a group G of order 6. Applying Corollary 1.10.7, let f be an element of order 3 and let g be an element of order 2 in G. We first claim that the six products $f^i g^j$, where $0 \leqslant i \leqslant 2$ and $0 \leqslant j \leqslant 1$, are distinct. Indeed, the equation $f^i g^j = f^r g^s$ implies that $f^{i-r} = g^{s-j}$. Every power of f except the identity has order 3 and every power of g except the identity has order 2, so we deduce that $f^{i-r} = g^{s-j} = e$, $r = i$, and $s = j$.

The first claim establishes that $G = \{1, f, f^2, g, fg, f^2g\}$. The product gf must be one of these elements. It is not possible that $gf = g$ because $f \neq e$. Similarly, we deduce that $fg \neq e, f, f^2$. Therefore, we have $gf = fg$ or $gf = f^2g$. Either of these relations, together with $f^3 = e$ and $g^2 = e$, determine the multiplication table for the group. Thus, there are at most two isomorphism classes of groups of order 6 and we already know two: μ_6 and $\mathfrak{S}_3$. □

1.10.9 Problem. Any group of order p^2, where p is a prime number, is abelian.

Solution. Let G be a group of order p^2. Its center $Z(G)$ is a subgroup, so it has order 1, p, or p^2. Corollary 1.10.2 proves that $|Z(G)| > 1$ and Corollary 1.10.7 shows that $Z(G)$ has an element f of order p. The cyclic group $H := \langle f \rangle$ is a subgroup of $C_G(g)$ for all $g \in G$. If $g \in G$ and $g \notin H$, then we have $|C_G(g)| > p$. Since $|C_G(g)|$ divides p^2, we obtain $|C_G(g)| = p^2$, $C_G(g) = G$, and $g \in Z(G)$. Since every element of G belongs to $Z(G)$, the group G must be abelian. □

1.11 The Other Sylow Theorems

The Sylow Theorems give a partial converse to the Lagrange Theorem. The First Sylow Theorem states that, for every prime factor p of the order of a finite group, there exists a Sylow p-subgroup of order p^r, the highest power of p that divides the order of the group. The Second and Third Sylow Theorems refine this existence result.

1.11.1 Theorem (Sylow 1872). *Let p be a prime number and let G be a finite group.*

(i) *Every subgroup of G whose order is a power of p is contained in a Sylow p-subgroup.*

(ii) *The Sylow p-subgroups of G are conjugate to one another and their number is congruent to* $1 \pmod{p}$.

Proof. Let H be a subgroup of G whose order is a power of p. By Theorem 1.10.6, there exists a Sylow p-subgroup P of the group G. Let X be the set of left cosets of P and consider the action of H on X by left translation. As $|X| \not\equiv 0 \pmod{p}$, Lemma 1.10.1 implies that there exists $x \in X$ such that $hx = x$ for all $h \in H$. Given $g \in G$ such that $x = gP$, we have $H \subseteq gPg^{-1}$.

When H is a Sylow p-subgroup, we obtain $|H| = |P| = |gPg^{-1}|$ and $H = gPg^{-1}$ which proves the first assertion in the second part.

Let $\mathcal{S}$ be the set of Sylow p-subgroups in G and let P act on $\mathcal{S}$ by conjugation. The element $P \in \mathcal{S}$ is a fixed point undet this action; we claim that it is the only one. Suppose that $Q \in \mathcal{S}$ be a fixed point. It follows that Q is a Sylow p-subgroup of G normalized by P, so the subgroup P is contained in the normalizer $N_G(Q)$. Both P and Q are Sylow p-subgroups of $N_G(Q)$, so the first assertion in the second part shows that there exists $n \in N_G(Q)$ such that $P = nQn^{-1} = Q$. By the Lemma 1.10.1, we have $|\mathcal{S}| \equiv |\mathcal{S}^P| = 1 \pmod{p}$. □

1.11.2 Example. The symmetric group $\mathfrak{S}_3$ of order 6 has a normal Sylow 3-subgroup: $\{\mathrm{id}_3, (3\ 1\ 2), (3\ 2\ 1)\}$. It also contains three Sylow 2-subgroups of order 2: $\{\mathrm{id}_3, (2\ 1)\}$, $\{\mathrm{id}_3, (3\ 1)\}$, and $\{\mathrm{id}_3, (3\ 2)\}$. ⋄

1.11.3 Example. For an odd positive integer n, the dihedral group D_n has n Sylow 2-subgroups of order 2. Each of these groups is generated by a reflection and they are all conjugate under rotations.

For an even positive integer n, the dihedral group D_n also has n Sylow 2-subgroups. Each Sylow 2-subgroup is isomorphic to $\mu_2 \times \mu_2$ because the dihedral group D_n contains no element of order 4. Each of these groups is generated by a reflection and a rotation by π. ⋄

1.11.4 Corollary. *Let p be a prime number and let $\varphi : G_1 \to G_2$ be a group homomorphism between finite groups. For every Sylow p-subgroup P_1 in G_1, there exists a Sylow p-subgroup P_2 in G_2 such that $\varphi(P_1) \subseteq P_2$.*

Proof. Apply the Second Sylow Theorem to $\varphi(P_1)$. □

1.11.5 Corollary. *Let H be a subgroup of G. For every Sylow p-subgroup P in the group H, there exists a Sylow p-subgroup Q in the group G such that $P = Q \cap H$. Conversely, if Q is a Sylow p-subgroup of G and H is normal in G, then group $Q \cap H$ is a Sylow p-subgroup of H.*

Proof. The subgroup P is contained in a Sylow p-group Q of G and $Q \cap H$ is a maximal subgroup of H whose order a prime power of p containing P. Hence, the intersection $Q \cap H$ is equal to P.

Let P' be a Sylow p-subgroup of H. There is an element $g \in G$ such that $gP'g^{-1} \subseteq Q$. Since H is normal, the conjugate subgroup $P = gP'g^{-1}$ is contained in H, whence in $Q \cap H$. As the order of $Q \cap H$ is a power of the prime p of H and P is a Sylow p-subgroup of H, we deduce that $P = Q \cap H$. □

1.11.6 Corollary. *Let K be a normal subgroup of a group G. The image in the quotient G/K of a Sylow p-subgroup of G is a Sylow p-subgroup and every Sylow p-subgroup of the quotient G/K is obtained this way.*

Proof. Let $G' := G/K$ and let P' be the image in the quotient group G' of a Sylow p-subgroup P in G. The group G acts transitively on the quotient G'/P', so the quotient G'/P' has the same cardinality as G/H for some subgroup H of G containing P. It follows that $[G' : P']$ divides $[G : P]$ and hence is not a multiple of p. We deduce that P' is a Sylow p-subgroup of G'. Let Q' be another Sylow p-subgroup of G'. The Third Sylow Theorem implies that $Q' = g'P'(g')^{-1}$ for some $g' \in G'$. Choose an element $g \in G$ as a representative for the left coset g', we see that Q' is the image of $Q = gPg^{-1}$. □

1.11.7 Proposition. *Let p be a prime number. For any $r \in \mathbb{N}$, a group of order p^r has a normal subgroup of order p^k for all $0 \leqslant k \leqslant r$.*

Proof. Let G be a group of order p^r. We proceed by induction on r. The case $r = 0$ is trivial. Corollary 1.10.2 shows that the center of G is nontrivial. By Corollary 1.10.7, there exists a subgroup Z of $Z(G)$ of order p. Since the elements in $Z(G)$ commute with every element in G, the subset Z forms a normal subgroup of G. Given $1 < k \leqslant r$, we have $p^{k-1} \leqslant p^{r-1} = |G/Z|$ The induction hypothesis establishes that the quotient group G/Z has a normal subgroup H' of order p^{k-1}. Hence, the Correspondence Theorem shows that there is a normal subgroup H of G containing Z with $H' = H/Z$. As $|H/Z| = p^{k-1}$, we deduce that $|H| = p^k$. □