Chapter 1

Group Action and Sylow Theorems

Definition 1. Let G be a multiplicative group and X be any non-empty set. A *group action* of G on X is any mapping $(a, x) \rightarrow ax$ of $G \times X$ into X satisfying the conditions

(i) $a(bx) = (ab)x$ for all $a, b \in G$ and $x \in X$, and

(ii) $ex = x$ for all $x \in X$.

The mapping is called the action of G on X and the set X is known as $G-$set. Some authors call it as *transformation group.*

Example.

(i) Let $X = G$; each of the mappings $(a, x) \rightarrow ax$ and $(a, x) \rightarrow xa$ (where ax and xa are the products of a with x, and of x with a in the group G) is a group action.

(ii) Let $X = G$; the mapping $(a, x) \rightarrow axa^{-1}$ is a group action.

(iii) Let X be the set of all left cosets of a given subgroup H of G; then $(a, xH) \rightarrow (ax)H$ is a group action.

(iv) Let G be a group and H be a normal subgroup of G. Then the set X of all left cosets of H in G is a G-set if we define the mapping $(a, xH) \rightarrow (ax)H$ as the group action.

Proof. Please see Bhattacharjee, Jain & Nagpaul [p. 108]for the proofs. □

Definition 2. Given any group action $(a, x) \rightarrow ax$ of G on X, we define a binary relation "$\sim$" on X as follows:

$$x \sim y \Leftrightarrow \text{ there exists } a \in G \text{ such that } y = ax.$$

Example. The relation (just defined above) is an equivalence relation.

Proof. The easy proof is left to the reader. □

Definition 3. The equivalence class of $x \in X$, denoted by $\bar{x}$, for which $\bar{x} = \{ax : a \in G\}$, is called the orbit of x.

Definition 4. The number $|\bar{x}|$ of elements in the orbit $\bar{x}$ of $x \in X$ is called the *length of the orbit* of x.

Definition 5. The set $G_x = \{a \in G : ax = x\}$ is called the *stabilizer* of $x \in X$ in the group G (or sometimes, it is also known as the *isotropy group* of $x \in X$ in G).

Example. For any $x \in X$, G_x is a subgroup of G.

Proof. The easy proof is left to the reader. □

Note. When G acts on itself by conjugation, $(a, x) \to axa^{-1}$, the stabilizer of $x \in G$ is the normalizer of x in G.

Example. If $y = ax$, then $G_y = aG_xa^{-1}$.

Proof.

$$\begin{aligned} b \in G_y &\Leftrightarrow by = y \\ &\Leftrightarrow b(ax) = ax \\ &\Leftrightarrow a^{-1}(b(ax)) = a^{-1}(ax) \\ &\Leftrightarrow (a^{-1}ba)x = (a^{-1}a)x = ex = x \\ &\Leftrightarrow a^{-1}ba \in G_x \\ &\Leftrightarrow b \in aG_xa^{-1} \end{aligned}$$

□

Theorem 1.1. For any $x \in X$, $|\bar{x}|$ (the length of the orbit of x) is equal to the index of the stabilizer of x in G. In symbols, $|\bar{x}| = [G : G_x]$.

Proof. Let Y be the set of all left cosets of G_x in G.
That is, $Y = \{aG_x : a \in G\}$.
Define $f : \bar{x} \to Y$ by setting $f(ax) = aG_x$.
Recall that $\bar{x} = ax : a \in G$.
We have

$$\begin{aligned} &ax = bx \\ \Leftrightarrow\ &(a^{-1}b)x = x \\ \Leftrightarrow\ &a^{-1}b \in G_x \\ \Leftrightarrow\ &aG_x = bG_x. \end{aligned}$$

So, f is not only well-defined, it is also injective.
f is clearly surjective.
Hence, $|\bar{x}| = |Y|$,
that is $|\bar{x}| = [G : G_x]$.
This completes the proof. . □

When G acts on itself by conjugation, $|\bar{x}|$ is the conjugacy class of $x \in G$ and G_x is the normalizer of x in G.

Theorem 1.2. Let G be a group and let X be a set.

(i) If X is a $G-$set, then the action of G on X induces a homomorphism $\varphi : G \to S_x$

(ii) Any homomorphism $\varphi : G \to S_x$ induces an action of G onto X.

Proof. (i) We define $\varphi : G \to S_x$ by $(\varphi(a))(x) = ax$, $a \in G$, $x \in X$.
Clearly, $\varphi(a) \in S_x$, $a \in G$.
Let $a, b \in G$.
Then we have

$$\begin{aligned}(\varphi(ab))(x) &= (ab)x = a(bx)\\ =&a((\varphi(b))(x)) = (\varphi(a))((\varphi(b))(x))\\ =&(\varphi(a)\varphi(b))(x) \text{ for all } x \in X.\end{aligned}$$

Hence $\varphi(ab) = \varphi(a)\varphi(b)$.

(ii) We define $(a, x) \to (\varphi(a))(x)$; that is $ax = (\varphi(a))(x)$.
Then we have

$$\begin{aligned}(ab)x &= (\varphi(ab))(x) = (\varphi(a)\varphi(b))(x)\\ =&\varphi(a)(\varphi(b)(x)) = (\varphi(a)(bx) = a(bx).\end{aligned}$$

Also, $ex = (\varphi(e))(x) = x$.
Hence, X is a $G-$set.

□

Our purpose is here to prove the celebrated Sylow Theorems using group actions. We need a number-theoretic result here.

Theorem 1.3. Suppose $n = p^r m$, where p is prime, $r \geq 1$, $m \geq 1$ and p does not divide m. Let s be an integer with $0 \leq s \leq r$. Then $\binom{n}{p^s} = p^{r-s}mt$, where p does not divide t.

Proof. For $n \geq 1$ and $1 \leq r \leq n$, we have

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n}{r}\,\frac{(n-1)!}{(r-1)!((n-1)-(r-1))!} = \frac{n}{r}\binom{n-1}{r-1}.$$

Now, $\binom{n-1}{r-1} = \frac{(n-1)(n-2)...(n-r+1)}{(r-1)(r-2)...2\cdot 1}$, because $(n-1)-(r-1) = n-r$.
Therefore $\binom{n}{p^s} = \frac{p^r m}{p^s}\binom{n-1}{p^s-1} = p^{r-s}mt$, where $t = \binom{n-1}{p^s-1} = \frac{\prod_{i=1}^{p^s-1}(mp^r-1)}{\prod_{i=1}^{p^s-1}(p^s-1)}$
If $1 \leq i \leq p^s - 1$ and $p \,|\, i$, then let $i = p^{u_i}.t_i$, where $i \leq u_i \leq s$ and p does not divide t_i.
If p does not divide i, then $i = p_{u_i}.t_i$, where $u_i = 0$, so $t_i = i$ and does not divide t_i.
So, in either case, $\frac{mp^r-i}{p^s-i} = \frac{mp^r-p^{u_i}\cdot t_i}{p^s-p^{u_i}\cdot t_i} = \frac{mp^{r-u_i}-t_i}{p^{s-u_i}-t_i}$.
Neither the numerator nor the denominator of the fraction on the extreme right is divisible by p; so $\frac{\prod_{i=1}^{p^s-1} mp^{r-u_i}-t_i}{\prod_{i=1}^{p^s-1} p^{s-u_i}-t_i}$ is not divisible by p. □

Corollary 1.1. p^{r-s+l} does not divide $\binom{n}{p^s}$.

Corollary 1.2. If T is any subgroup of the group G of order p^s and $a \in G$, then the stabilizer of $S = Ta \in X$ is T, and the orbit length $\left|\bar{S}\right|$ is equal to $p^{r-s}m$; as such it is not divisible by p^{r-s+1}.

Proof. The stabilizer of S contains T, because

$$bS = (bT)a = Ta = S \text{ for every } b \in T.$$

On the other hand, the stabilizer of S is contained in T, for

$$b \in G_s \quad \Rightarrow b(ea) = ba \in S = Ta, \quad \text{since } ea \in Ta = S,$$

which then implies $b \in T$.
Hence the stabilizer of S is precisely T.
So the orbit pf S has length $[G : T] = p^{r-s}m$; this number is not divisible by p^{r-s+1} □

Corollary 1.3. $t \equiv 1 \pmod p$.

Proof. Multiplying out the factors in the numerator and those in the denominator of the last obtained expression for t, we get

$$t = \frac{\lambda p + v}{\mu p + v}$$

where $v = (-1)^{p^s-1} \prod_{i-1}^{p^s-1} t_i \cdot p$ does not divide $\prod_{i-1}^{p^s-1} t_i$, because p does not divide t_i for any $i = 1, 2, 3, \ldots, p^s - 1$.
So, p does not divide v.
Now, $t = \frac{\lambda p+v}{\mu p+v}$ implies

$$\begin{aligned} & v(t-1) = p(\lambda - t\mu) \\ \Rightarrow & \, p \,|\, v(t-1) \\ \Rightarrow & \, p \,|\, (t-1), \text{because } p \text{ does not divide } v. \end{aligned}$$

Hence $t \equiv 1 \pmod p$. □

1.1 Sylow's First Theorem

Theorem 1.4. A finite group G has at least one subgroup of every prime power order dividing $|G|$. That means, if $|G| = p^r m$, where p is prime, $r \geq 1$ and p does not divide m, then G has a subgroup of order p^s for every $s = 1, 2, \ldots, r$.

Note. Sylow's first theorem is a far-reaching generalization of Cauchy's theorem.

Proof. Let X be the set of all subsets of G having p^s elements; our aim is to prove that at least one of these subsets is a subgroup of G.
Clearly, X has $\binom{n}{p^s}$ elements.

Let G act on X in the obvious manner; for $a \in G$ and $S \in X$; $aS = \{ax : x \in S\}$.
Since $|aS| = |S|$, $a(bS) = (ab)S$ and $eS = S$, therefore the mapping $(a, S) \to aS$ is a group action on X.
Claim. There exists an orbit whose length is not divisible by p^{r-s+1}.
For, if every orbit had length divisible by p, then p^{r-s+1} would divide $|X|$, because $|X|$ is the sum of the lengths of all the distinct orbits, but p^{r-s+1} does not divide $\binom{n}{p^s} = |X|$.
So, this claim is proved.

Take an orbit $\bar{S}$ whose length is not divisible by p^{r-s+1}.
Since $\left|\bar{S}\right| = [G : G_s]$ divides $|G| = p^r m$, we have

$$\left|\bar{S}\right| \leq p^{r-s}m,$$

because the highest power of p dividing $\left|\bar{S}\right|$ is $\leq r - s$.
Hence, $|G_s| = \dfrac{|G|}{[G : G_s]} \geq \dfrac{p^r m}{p^{r-s}m} = p^s$.
Next we show that $|G_s| \leq p^s$, thus establishing $|G_s| = p^s$.
Take $a \in S$; for every $b \in G_s$. We have $bS = S$.
So, $ba \in S$.
Therefore,

$$(G_s)a \subseteq S$$
$$\Rightarrow |(G_s)a| \leq |S|.$$

But $|(G_s)a| = |G_s a| = |G_s|$ and $|S| = p^s$; and hence $|G_s| \leq p^s$ is established.
Since G_s is a subgroup of G, Sylow's first theorem stands proved. □

Definition 6. A Sylow $p-$subgroup of G is any subgroup of G of order p^r, where p^r $(r \geq 1)$ is the highest power of p dividing $|G|$.

Corollary 1.4. For every prime p dividing the order of a finite group G, there exists at least one Sylow $p-$subgroup of G.

Corollary 1.5. If the length of the orbit of $S \in X$ is not divisible by $p^{r-s}m$, then $S = Ta$ holds for some subgroup T of G of order p^s and any $a \in S$.

The proof of the last theorem reveals that $T = G_s$ is a subgroup of order p^s and $Ta \subseteq S$ holds for any $a \in S$. Since $|Ta| = |T| = p^s = |S|$, it follows that $S = Ta$.

If P is any Sylow $p-$subgroup of G, then $a^{-1}Pa$ is a Sylow $p-$subgroup of G for every $a \in G$, because $|a^{-1}Pa| = |P|$.

Sylow's second theorem asserts that any two Sylow $p-$subgroups are conjugate in G.

1.2 Sylow's Second Theorem

Theorem 1.5. Suppose P is any Sylow $p-$subgroup of G; H is any subgroup of G of order p^s, $0 \leq s \leq r$, where r is the highest power of p dividing $|G|$. Then H is a subgroup of a Sylow $p-$subgroup of G which is conjugate to P.

Proof. Let X be the set of all right cosets of P in G; so $|X| = [G : P] = \frac{p^r m}{p^r} = m$.
Let H act on X in the manner:

$$(b, Pa) \to P(ab).$$

Since $((Pa)b)c = (Pa)(bc)$ and $(Pa)e = Pa$, the mapping $(b, Pa) \to P(ab)$ is a group action.

Claim. There is at least one orbit whose length is not divisible by p.

For, if every orbit had length divisible by p, then the sum of lengths of all distinct orbits, which is $|X|$, would be divisible by p, which is not true.
Consider an orbit whose length is not divisible by p.
This length is equal to the index in H of the stabilizer of any element belong to the orbit; so it is a divisor of $|H| = p^s$.
So this length must be 1.
It follows that

$$\begin{aligned} & Pa \in X \text{ belongs to an orbit of length } 1 \\ \Leftrightarrow\ & (Pa)b = Pa \text{ for every } b \in H \\ \Leftrightarrow\ & P(aba^{-1}) = P \text{ for every } b \in H \\ \Leftrightarrow\ & aba^{-1} \in P \text{ for every } b \in H \\ \Leftrightarrow\ & b \in a^{-1}Pa \text{ for every } b \in H \\ \Leftrightarrow\ & H \subseteq a^{-1}Pa. \end{aligned}$$

This proves the theorem, because $a^{-1}Pa$ is a subgroup conjugate to P. □

Corollary 1.6. Any two Sylow $p-$subgroups are conjugate.

Proof. If P, Q are Sylow $p-$subgroups, then applying Sylow's second theorem to $H = Q$, we get

$$Q \subseteq a^{-1}Pa \text{ for some } a \in G.$$

Then $Q = a^{-1}Pa$, because $|a^{-1}Pa| = |P| = |Q|$. □

Corollary 1.7. G has a normal Sylow $p-$subgroup iff G has only one Sylow $p-$subgroup.

Proof. This follows from Corollary 1.7 and the fact that a subgroup is normal if and only if it coincides with each of its conjugate subgroups. □

1.3 Sylow's Third Theorem

Theorem 1.6. If p is any prime dividing $|G|$, then the number of subgroups of order p^s (where $0 \leq s \leq r$) is congruent to 1 modulo p.

Proof. Let X be the set of all subsets of G having p^s elements; let G act on X in the obvious manner $(a, S) \to aS = \{ax : x \in S\}$.
If T is any subgroup of order p^s, then by Corollary 1.2, every right coset of T lies in orbit of length $p^{r-s}m$.
Conversely, Corollary 1.5 shows that every $S \in X$ whose orbit length is not divisible by p^{r-s+1}, is a right coset of a subgroup of G of order p^s; as such $\left|\bar{S}\right|$ is then $= p^{r-s}m$.
Let λ be the number of distinct subgroups of order p^s.

So, by the preceding observation, there are precisely $p^{r-s}m$ sets whose orbit lengths are not divisible by p^{r-s+1}.

Note that for distinct subgroups T, T' it cannot happen that $Ta = T'a'$ holds for some $a, a' \in G$; for then $a' \in Ta$, implies $Ta = Ta' = T'a'$, whence $T = T'$ would follow.

So, there are precisely $p^{r-s}m$ different $S \in X$ whose orbits have length not divisible by p^{r-s+1}. The total number of elements in all these orbits is $p^{r-s}m\lambda$.

The remaining $p^{r-s}mt - p^{r-s}m\lambda = p^{r-s}m(t-\lambda)$ elements (if any) of X all have orbit lengths divisible by p^{r-s+1}; so the total number of elements in all these orbits is $k \cdot p^{r-s+1}$, where $k \geq 0$ is an integer.

Therefore, we have

$$\begin{aligned}
&p^{r-s}m(t-\lambda) = k \cdot p^{r-s+1} \\
\Rightarrow\ & m(t-\lambda) = kp \\
\Rightarrow\ & p \,|m(t-\lambda) \\
\Rightarrow\ & p \,|(t-\lambda), \text{ because } p \text{ does not divide } m \\
\Rightarrow\ & \lambda \equiv t \pmod p \\
\Rightarrow\ & \lambda \equiv 1 \pmod p, \text{ because } t \equiv 1 \pmod p; \text{ by Corollary 1.3.}
\end{aligned}$$

□

Corollary 1.8. The number of distinct Sylow $p-$subgroups divides the $p-$free part of $|G|$. That is, if $|G| = p^r m$, where p does not divide m,then λ (the number of distinct Sylow $p-$subgroups of G) divides m.

Proof. Let G be a group with $|G| = p^r m$ (where p does not divide m) and λ is the number of distinct Sylow $p-$subgroups of G. If P is any fixed Sylow $p-$subgroups of G, then any other

Sylow $p-$subgroup of G is a conjugate of G. So, $\lambda = [G : N_p]$ is the index of the normalizer of P in G. N_p contains P, because P is a subgroup. Since, $|N_p|$ divides $|G| = p^r m$ and is $\geq |P| = p^r$, it follows that $|N_p| = p^r m'$, where p does not divide m'. So,

$$\lambda = [G : N_p] = \frac{p^r m}{p^r m'} = \frac{m}{m'}$$

$$\Rightarrow \lambda m' = m$$

$$\Rightarrow \lambda \text{ divides } m.$$

Thus, not only is the number of distinct Sylow $p-$subgroups a number of the very special form $1 + kp$, $k \geq 0$, but it is also a divisor of m. □

Note (Historical Note). Sylow (Ludyig Sylow, 1832-1918) stated and proved his theorems in the context of permutation groups (1872). Frobenius (1884) proved Sylow's first theorem for abstract groups, which entailed the derivation of the class equation. The elegant proof given here was published by H. Wielandt in 1959. E. Artin presented the proofs of Sylow's second and third theorems and that of Theorem 1.5 via group actions in his lectures in the summer of 1961. See S. Chakraborty & M. R. Chowdhury, The Sylow Theorems from Frobenius to Wielandt, GANIT Journal of Bangladesh Math. Society, 25 (2005), 85-108. We use group action to prove an analogue of Sylow's first and third theorems concerning normal subgroups of p-group due to Frobenius (1895).

Theorem 1.7 (Frobenius). Every $p-$group G has normal subgroups of every order dividing $|G|$, and their number is $\equiv 1 \pmod p$.

Proof. Let G be a group with $|G| = p^r$, where $r \geq 1$ is a natural number.
By Sylow's first theorem, G has subgroups of every order p^k dividing $|G| = p^r$. For any fixed k, $1 \leq k \leq r$, let X be the set of k subgroups of order p^k. Let G act on X by conjugation, $(a, H) \to aHa^{-1}$, $a \in G$ and $H \in X$. Every orbit $\bar{H}$ has a length which divides $|G| = p^r$; □