# Theory of Groups

## MAT511

### Prof. Dr Chandrani Nag

*Shahjalal University of Science and Technology*

Edited by
Mehedi Hasan

# Preface

This is a compilation of lecture notes with some books and my own thoughts. If there are any mistake/typing error or, for any query mail me at mehedi12@student.sust.edu.

# Contents

# Part I

# Sheet

# Chapter 1

# Automorphism

**Definition 1** (Automorphism)**.** An automorphism of a group $G$ is an isomorphism[1] of $G$ onto itself.

*Theorem* 1.1. The set $Aut(G)$ of all automorphisms of a group $G$ is a group under the operation of composition of mappings.

*Proof.* Here $Aut(G)$ is the set of all automorphisms of a group $G$ and the operation is the composition of mappings.

Let $f, g \in Aut(G)$.

Then the composite map $g \circ f$ is bijective, because $f$ and $g$ are bijective.

Using the hypotheses that $f$ and $g$ are group homomorphisms, we can conclude that $g \circ f$ is also a group homomorphism, because

$$
\begin{aligned}
(g \circ f)(ab) &= g(f(ab)) \\
&= g(f(a)f(b)) \\
&= g(f(a))g(f(b)) \\
&= (g \circ f)(a)(g \circ f)(b)
\end{aligned}
$$

So, $g \circ f \in Aut(G)$.

This is the closure property.

The associative law holds for $Map(G)$, the set of all mappings of $G$ into itself; so it holds in $Aut(G)$, because $Aut(G)$ is closed under composition of mappings.

Clearly, $1_G$ is the identity element of $Aut(G)$.

If $f \in Aut(G)$, the inverse mapping $f^{-1} : G \to G$ exists and is likewise bijective.

Let $f \in Aut(G)$ and $a, b, x, y \in G$ such that $f(a) = x$ and $f(b) - y$. Then we have $a = f^{-1}(x)$

---

[1]Homomorphism: Suppose $G$, $G'$ are multiplicative groups. A mapping $f : G \to G'$ is called a group homomorphism iff $f(ab) = f(a)f(b)$ holds for all $a, b \in G$.

Isomorphism: A bijective group homomorphism is called an isomorphism.

and $b = f^{-1}(y)$.

Since $f$ is a group homomorphism, we have $f(ab) = f(a)f(b) = xy$.

It gives, $f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$.

This implies that $f^{-1}$ is also a group homomorphism.

Hence, $f^-1 \in Aut(G)$.

Therefore, $Aut(G)$ is a group under composition of mappings. □

## 1.1   Inner Automorphisms

For any fixed $a \in G$, we define a mapping $f_a : G \to G$ by setting $f_a(x) = axa^{-1}$, $f_a \in Aut(G)$ for every $a \in G$.

*Proof.* $f_a$ is injective (by the cancellation law), for

$$f_a(x) = f_a(y) \quad \Rightarrow \quad axa^{-1} = aya^{-1} \quad \Rightarrow \quad x = y.$$

$f_a$ is surjective, because

$$f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x.$$

$f_a$ is group homomorphism, because for all $x, y \in G$, we have

$$f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y).$$

□

**Definition 2** (Inner Automorphism). For any fixed $a \in G$ the mapping $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is called the inner automorphism determined by $a$.

*Theorem* 1.2. The set $Inn(G)$ of all inner automorphisms of a group $G$ is a subgroup of $Aut(G)$.

*Proof.* The relation $f_a \circ f_b = f_{ab}$ is the key.

This is easily proved, for

$$
\begin{aligned}
(f_a \circ f_b)(x) &= f_a(f_b(x)) \\
&= f_a(bxb^{-1}) \\
&= a(bxb^{-1})a^{-1} \\
&= (ab)x(ab)^{-1} \\
&= f_{ab}(x) \qquad \text{holds for all } x \in G
\end{aligned}
$$

So, $Inn(G)$ Is closed under composition of mappings.

The identity mapping $l_G$ belongs to $Inn(G)$, because $f_e = 1_G$.

The inverse of $f_a$, which is obviously an automorphism, is the inner automorphism determined by $a^{-1}$, because

$$f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e = 1_G$$

and

$$f_{a^{-1}} \circ f_a = f_{a^{-1}a} = f_e = 1_G$$

So, $Inn(G)$ is a subgroup of $Aut(G)$. It remains to show that $Inn(G)$ is a normal subgroup of $Aut(G)$. For any $\sigma \in Aut(G)$, we have $\sigma \circ f_a \circ \sigma^{-1} = f_{\sigma(a)}$, because

$$\begin{aligned}
(\sigma \circ f_a \circ \sigma^{-1})(x) &= (\sigma \circ f_a)(\sigma^{-1}(x)) \\
&= \sigma(a\sigma^{-1}(x)a^{-1}) \\
&= \sigma(a)\sigma(\sigma^{-1}(x))\sigma(a^{-1}) \\
&= \sigma(a)x\sigma(a^{-1}) \\
&= \sigma(a)x(\sigma(a))^{-1} \\
&= f_{\sigma(a)}(x) \quad \in Inn(G)
\end{aligned}$$

So, $Inn(G)$ is a normal subgroup of $Aut(G)$ $\qquad \square$

# Chapter 2

# Conjugacy and Class Equation

**Definition 3.** Let $G$ be a group. The *normalizer* of a non-empty subset $S \subseteq G$ is defined by $N_S = \{x \in G : xS = Sx\}$.

**Definition 4.** Let $G$ be a group and $a \in G$. Then the set $N_a = \{x \in G : ax = xa\}$ is called the *normalizer* of $a \in G$ in $G$.

Thus, $N_a$ is the set of those elements of $G$ which commute with $a$.

**Example.** $N_a$ is a subgroup of $G$.

*Proof.* We know that $N_a = \{x \in G : ax = xa\}$ when $a \in G$. Let $x, y \in N_a$. Then $ax = xa$ and $ay = ya$.

Hence, we have
$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a.$$

Besides, we also get
$$x^{-1}(ax)x^{-1} = x^{-1}(xa)^{-1} \quad \text{which implies that} \quad x^{-1}a = ax^{-1}.$$

Thus, it follows that $xy \in N_a$ and $x^{-1} \in N_a$ for all $x, y \in N_a$.

So, $N_a$ is a subgroup of $G$. $\qquad\square$

*Note.* $N_a = G \iff a = Z$.

**Example.** $N_a$ need not be a normal subgroup[1] of $G$.

*Proof.* In order to show that $N_a$ need not be normal in $G$, consider an element $(23)$ of the symmetric group $S_3$.

It is easy to verify that $N_{(23)} = \{(1), (23)\}$ is a subgroup of $S_3$.

But $(12) \circ N_{(23)} = \{(12), (123)\}$ and $N_{(23)} \circ (12) = \{(12), (132)\}$

Thus $(12) \circ N_{(23)} \neq N_{(23)} \circ (12)$.

This shows that $N_{(23)}$ is not a normal subgroup of $S_3$. $\qquad\square$

---

[1]Normal subgroup: A subgroup $N$ of a group $G$ is called normal subgroup iff $aN = Na$ holds $\forall a \in G$. Denoted by $N \triangleleft G$.

# Chapter 3

# Group Action and Sylow Theorems

**Definition 5.** Let $G$ be a multiplicative group and $X$ be any non-empty set. A *group action* of $G$ on $X$ is any mapping $(a, x) \to ax$ 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 $(a, x) \to ax$ and $(a, x) \to xa$ (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 $(a, x) \to axa^{-1}$ is a group action.

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

*Proof.* Please see Bhattacharjee, Jain & Nagpaul [p. 108]for the proofs. $\qquad \square$

**Definition 6.** Given any group action $(a, x) \to ax$ 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. $\qquad \square$

**Definition 7.** The equivalence class of $x \in X$, denoted by $\tilde{x}$, for which $\tilde{x} = \{ax : a \in G\}$, is called the orbit of $x$.

**Definition 8.** The number $|\tilde{x}|$ of elements in the orbit $\tilde{x}$ of $x \in X$ is called the *length of the orbit* of $x$.

**Definition 9.** 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, $(a, x) \rightarrow axa^{-1}$, 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* 3.1. For any $x \in X$, $|\tilde{x}|$ (the length of the orbit of $x$) is equal to the index of the stabilizer of $x$ in $G$. In symbols, $|\tilde{x}| = [G : G_x]$.

*Proof.* Let $Y$ be the set of all left cosets of $G_x$ in $G$.
That is, $Y = \{aG_x : a \in G\}$.
Define $f : \tilde{x} \rightarrow Y$ by setting $f(ax) = aG_x$.
Recall that $\tilde{x} = ax : a \in G$.
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, $|\tilde{x}| = |Y|$,
that is $|\tilde{x}| = [G : G_x]$.
This completes the proof. . □

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

**Theorem 3.2.** 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

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

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

$$(ab)x = (\varphi(ab))(x) = (\varphi(a)\varphi(b))(x)$$
$$= \varphi(a)(\varphi(b)(x)) = (\varphi(a)(bx) = a(bx).$$

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 3.3.** 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 $p \mid i$, 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* 3.1. $p^{r-s+l}$ does not divide $\binom{n}{p^s}$.

*Corollary* 3.2. 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 $|\bar{S}|$ 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

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

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* 3.3. $t \equiv 1(\mod p)$.

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

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

□

## 3.1 Sylow's First Theorem

*Theorem* 3.4. 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, $|G_s| = \frac{|G|}{[G:G_s]} \geq \frac{p^r m}{p^{r-s}m} = p^s$.

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 10.** 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* 3.4. For every prime $p$ dividing the order of a finite group $G$, there exists at least one Sylow $p-$subgroup of $G$.

*Corollary* 3.5. 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 $G$.

## 3.2   Sylow's Second Theorem

*Theorem* 3.5. 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:

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

Since $((Pa)fa)c = (Pa)(bc)$ and $(Pa)e = Pa$, the mapping $(b, Pa) \rightarrow P(ab)$ 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

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

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

*Corollary* 3.6. 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* 3.7. $G$ has a normal Sylow $p-$subgroup iff $G$ has only one Sylow $p-$subgroup.

*Proof.* This follows from Corollary 3.7 and the fact that a subgroup is normal if and only if it coincides with each of its conjugate subgroups. □

## 3.3 Sylow's Third Theorem

*Theorem* 3.6. 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 3.2, every right coset of $T$ lies in orbit of length $p^{r-s}m$.

Conversely, Corollary 3.5 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 $|\bar{S}|$ is then $= p^{r-s}m$.

Let $\lambda$ 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 $Ta = Ta'$ 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 $p^{r-s}mt - p^{r0s}m\lambda = p^{r-s}m(t - \lambda)$ 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

$$p^{r-s}m(t - \lambda) = k \cdot p^{r-s+1}$$
$$\Rightarrow m(t - \lambda) = kp$$
$$\Rightarrow p \,|\, m(t - \lambda)$$
$$\Rightarrow p \,|\, (t - \lambda), \text{ because } p \text{ does not divide } m$$
$$\Rightarrow \lambda \equiv t (\mod p)$$
$$\Rightarrow \lambda \equiv 1 (\mod p), \text{ because } t \equiv 1 (\mod p); \text{ by Corollary 3.3.}$$

$\square$