## NOTES ON GROUP THEORY

## Abstract. These are the notes prepared for the course MTH 751 to be offered to the PhD students at IIT Kanpur.

## Contents

1. Binary Structure ..... 2
2. Group Structure ..... 5
3. Group Actions ..... 13
4. Fundamental Theorem of Group Actions ..... 15
5. Applications ..... 17
5.1. A Theorem of Lagrange ..... 17
5.2. A Counting Principle ..... 17
5.3. Cayley's Theorem ..... 18
5.4. The Class Equation ..... 18
5.5. Cauchy's Theorem ..... 19
5.6. First Sylow Theorem ..... 21
5.7. Second Sylow Theorem ..... 21
5.8. Third Sylow Theorem ..... 22
6. Structure Theorem for Finite Abelian Groups ..... 24
References ..... 26

## 1. Binary Structure

Let $S$ be a set. We denote by $S \times S$ the set of ordered pairs $(a, b)$, where $a, b \in S$. Thus the ordered pairs $(a, b)$ and $(b, a)$ represent distinct elements of $S \times S$ unless $a=b$.

A binary operation $\star$ on $S$ is a function from $S \times S$ into $S$. Thus for every $(a, b) \in S \times S$, the binary operation $\star$ assigns a unique element $a \star b$ of $S$. If this happens, then we say that the pair $(S, \star)$ is a binary structure.

Let us understand the above notion through examples.
Example 1.1 : We follow the standard notations to denote the set of natural numbers, integers, rationals, reals, complex numbers by $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively. If $S$ is one of the sets above, then $S^{*}$ stands for $S \backslash\{0\}$.
(1) Addition (resp. multiplication) is a binary operation on $\mathbb{Z}$ (resp. $\mathbb{Q}$ ).
(2) Division is not a binary operation on $\mathbb{Z}^{*}$.
(3) Subtraction is a binary operation on $\mathbb{Z}$ but not on $\mathbb{N}$.
(4) Division is a binary operation on $\mathbb{R}^{*}$ (resp. $\mathbb{C}^{*}$ ).

As seen in (3), it may happen that $a \star b \notin A$ for some $a, b \in A$.
Let $(S, \star)$ be a binary structure. Let $A$ be a subset of a set $S$. We say that $\star$ is an induced binary operation on $A$ if $a \star b \in A$ for every $a, b \in A$.

Exercise 1.2 : Let $\mathbb{O}$ denote the set of odd integers. Verify that the multiplication on $\mathbb{Z}$ is an induced binary operation on $\mathbb{O}$, however, addition is not so.

Let us see some geometric examples of binary structures.
Example 1.3 : Let $\mathbb{T}$ denote the unit circle. Consider the binary operation - of multiplication from $\mathbb{T} \times \mathbb{T}$ into $\mathbb{T}$. Note that the action

$$
\begin{equation*}
(z, w) \longrightarrow z \cdot w \tag{1.1}
\end{equation*}
$$

can be interpreted as rotation of $z$ about the origin through the angle $\arg (w)$ in the anticlockwise direction.

As an another interesting example of a binary operation, consider the binary operation of multiplication on an annulus centered at the origin. One may use the polar co-ordinates to interpret the action (0.1) as rotation of $z$ about the origin through the $\operatorname{angle} \arg (w)$ in the anticlockwise direction followed by a dilation of magnitude $|w|$.

Exercise 1.4 : Let $A(r, R)$ denote the annulus centered at the origin with inner radius $r$ and outer radius $R$, where $0 \leq r<R \leq \infty$. Find all values of $r$ and $R$ for which $(A(r, R), \cdot)$ is a binary structure.

Hint. If $r<1$ then $r=0$ (Use: $r<\sqrt{r}$ if $0<r<1$ ). If $R>1$ then $R=\infty$ (Use: $\sqrt{R}<R$ if $1<R<\infty$ ).

Exercise 1.5 : Let $L$ denote a line passing through the origin in the complex plane. Verify that the multiplication • on the plane is not an induced binary operation on $L$.

A binary structure $(S, \star)$ is associative if $x \star(y \star z)=(x \star y) \star z$ for every $x, y, z \in S$. We say that $(S, \star)$ is abelian if $x \star y=y \star x$ for every $x, y \in S$.

Exercise 1.6 : Let $M_{n}(\mathbb{R})$ denote the set of $n \times n$ matrices with real entries. Verify that the matrix multiplication $\circ$ is a binary operation on $M_{n}(\mathbb{R})$. Verify further the following:
(1) $\circ$ is associative.
(2) $\circ$ is abelian iff $n=1$.

Let $(S, \star)$ be a binary structure. We say that $e \in S$ is identity for $S$ if $e \star s=s=s \star e$ for every $s \in S$.

In general, $(S, \star)$ may not have an identity. For example, the infinite interval $(1, \infty)$ with multiplication is a binary structure without identity.

Proposition 1.7. Identity of a binary structure, if exists, is unique.
Proof. The proof is a subtle usage of the definition of the binary operation. Suppose $(S, \star)$ has two identities $e$ and $e^{\prime}$. By the very definition of the binary operation, the pair ( $e, e^{\prime}$ ) assigned to a unique element $e \star e^{\prime}$. However, $e \star e^{\prime}$ equals $e$ if $e^{\prime}$ is treated as identity, and $e^{\prime}$ if $e$ is treated as identity. Thus we obtain $e^{\prime}=e$ as desired.

Before we discuss the isomorphism between two binary structures, it is necessary to recall the notion of isomorphism between sets. We say that two sets $S$ and $T$ are isomorphic if there exists a bijection $\phi$ from $S$ onto $T$. Recall that $\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic.

We say that two binary structures $(S, \star)$ and $(T, *)$ are isomorphic if there exists a bijection $\phi: S \rightarrow T$, which preserves the binary operations:

$$
\phi(a \star b)=\phi(a) * \phi(b) \text { for all } a, b \in S .
$$

We will refer to $\phi$ as the isomorphism between $(S, \star)$ and ( $T, *$ ).
Remark 1.8: The set-theoretic inverse $\phi^{-1}$ of $\phi$ is an isomorphism between $(T, *)$ and $(S, \star)$.

It is not always easy to decide whether or not given binary structures are isomorphic. The following two tests are quite handy for this purpose.

Exercise 1.9 : Suppose the binary structures $(S, \star)$ and $(T, *)$ are isomorphic. Show that if $(S, \star)$ is abelian (resp. associative) then so is $(T, *)$.

Note that the binary structures $(\mathbb{R}, \cdot)$ and $\left(M_{2}(\mathbb{R}), \circ\right)$ are not isomorphic.
Proposition 1.10. Suppose there exists an isomorphism $\phi$ between the binary structures $(S, \star)$ and $(T, *)$. Fix $a \in S$. Then the following is true:
(1) The equation $x \star x=b$ has a solution in $S$ iff the equation $x * x=\phi(b)$ has a solution in $T$.
(2) There exists a bijection from the solution set $\mathcal{S}$ of $x \star x=b$ onto the solution set $\mathcal{T}$ of $x * x=\phi(b)$.

Proof. If $x_{0} \in S$ is a solution of the equation $x \star x=b$ then $\phi\left(x_{0}\right) \in T$ is a solution of the equation $x * x=\phi(b)$. The converse follows from Remark 1.8. Since $\phi: \mathcal{S} \rightarrow \mathcal{T}$ given by $\Phi\left(x_{0}\right)=\phi\left(x_{0}\right)$ is a bijection, the remaining part follows.

Example 1.11 : Consider the binary structures $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$. We already recorded that $\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic. The natural question arises whether $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$ are isomorphic ?

Let us examine the equation $x+x=1$. Note that the solution set of $x+x=1$ in $\mathbb{Z}$ is empty. On the other hand, the solution set of $x+x=1$ in $\mathbb{Q}$ equals $\{1 / 2\}$. By Proposition 1.10 , the binary structures $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$ can never be isomorphic.

Exercise 1.12 : Whether the following binary structures are isomorphic. Justify your answer.
(1) $(\mathbb{Z},+)$ and $(\mathbb{N},+)$.
$(2)(\mathbb{C}, \cdot)$ and $(\mathbb{R}, \cdot)$.
(3) $(\mathbb{C}, \cdot)$ and $\left(\mathbb{C}^{*}, \cdot\right)$.

Exercise 1.13 : Consider $\mathbb{C}^{*}$ and $\mathbb{T}$ as topological spaces with the topology inherited from the complex plane. Show that there does not exist a continuous isomorphism from $\left(\mathbb{C}^{*}, \cdot\right)$ onto $(\mathbb{T}, \cdot)$.

In view of the last exercise, one may ask: Is it true that $\left(\mathbb{C}^{*}, \cdot\right)$ and $(\mathbb{T}, \cdot)$ are isomorphic? The answer is No (refer to [2]).

Exercise 1.14 : Show that there exists no isomorphism $\phi$ between the binary structures $\left(M_{2}(\mathbb{R}), \circ\right)$ and $\left(M_{3}(\mathbb{R}), \circ\right)$ such that $\phi(I)=I$.

Hint. Consider the equation $A^{2}=I$ for invertible solutions $A$.
Recall that a matrix $A \in M_{n}(\mathbb{R})$ is orthogonal if $A^{t} A=I$. Note that $A \in M_{n}(\mathbb{R})$ is orthogonal if and only if $A$ preserves the euclidean distance, that is, $\|A X-A Y\|_{2}=\|X-Y\|_{2}$ for every $X, Y \in \mathbb{R}^{n}$, where $\|\cdot\|_{2}$ denotes the euclidean norm on $\mathbb{R}^{n}$.

Exercise 1.15 : Prove that any orthogonal matrix in $M_{2}(\mathbb{R})$ is either a rotation $R_{\theta}$ about the origin with angle of rotation $\theta$ or a reflection $\rho_{\theta}$ about the line passing through origin making an angle $\theta / 2$, where

$$
R_{\theta}=\left(\begin{array}{cc}
\cos \theta & -\sin \theta  \tag{1.2}\\
\sin \theta & \cos \theta
\end{array}\right), \rho_{\theta}=\left(\begin{array}{cc}
\cos \theta & \sin \theta \\
\sin \theta & -\cos \theta
\end{array}\right)
$$

Hint. Any unit vector in $\mathbb{R}^{2}$ is of the form $(\sin \theta, \cos \theta)$ for some $\theta \in \mathbb{R}$.

Here is an example of geometric nature.
Example 1.16 : Let $\Delta$ denote an equilateral triangle in the plane with origin as the centroid. For example, one may take triangle with vertices $(1,0),(-1 / 2, \sqrt{3} / 2),(-1 / 2,-\sqrt{3} / 2)$. By symmetry of $\Delta$, we understand orthogonal $2 \times 2$ matrix $A$ in $M_{2}(\mathbb{R})$ such that $A(\Delta)=\Delta$. Consider the set $S_{3}$ all symmetries of $\Delta$. It is easy to see that $\left(S_{3}, \circ\right)$ is a binary structure.

To understand this binary structure, we need a bit of plane geometry. By Exercise 1.15, any element of $S_{3}$ is a composition of rotations about the origin and reflections about a line passing through origin. Since $\Delta$ is an equilateral triangle with centroid 0 , a rotation belongs to $S$ if and only if the angle of rotation is either $2 / 3 \pi, 4 / 3 \pi, 2 \pi$. Similarly, since the axes of symmetry of $\Delta$ are precisely the lines passing through the origin and mid-point of sides of $\Delta$, a reflection belongs to $S_{3}$ if and only if the line of reflection is one of the axes of symmetry of $\Delta$. It follows that $S_{3}$ consists exactly six elements; 3 rotations and 3 reflections.

Exercise 1.17 : Describe all symmetries of a regular polygon in the plane with origin as the centroid.

## 2. Group Structure

In the last section, we discussed many examples of binary structures $(S, \star)$. We also observed that there are some "distinguished" binary structures, namely, unital pairs $(S, \star)$ for which the binary operation is associative. It is desirable to pay more attention to such structures. An axiomatic approach is often convenient for such studies.

Definition 2.1 : A binary structure $(G, \star)$ is a group if
(1) (Associativity) For all $a, b, c \in G$, we have $(a \star b) \star c=a \star(b \star c)$.
(2) (Existence of Identity) There exists $e \in G$ such that $e \star a=a=a \star e$ for all $a \in G$.
(3) (Existence of Inverse) For all $a \in G$, there exists $a^{-1} \in G$ (depending, of course, on $a$ ) such that $a \star a^{-1}=e=a^{-1} \star a$.
We say that a group structure $(G, \star)$ is abelian if
(4) (Commutativity) For all $a, b \in G$, we have $a \star b=b \star a$.

Remark 2.2 : Note that the inverse of the identity is the identity itself.
If there is no confusion, we will suppress the binary operation $\star$.
Note that $(\mathbb{R},+)$ and $\left(\mathbb{R}^{*}, \cdot\right)$ are group structures.
Example 2.3 : For a positive number $c$, consider the open interval $G=$ $(-c, c)$ of real numbers. For $x, y \in G$, define

$$
x \star y:=\frac{x+y}{1+x y / c^{2}}
$$

Notice that $1+x y / c^{2}>0$ for any $x, y \in G$, so that $x \star y \in \mathbb{R}$. To see that $\star$ is a binary operation, we should check that $-c<x \star y<c$ if $-c<x, y<c$. Note that $|x \circ y|<c$ iff $c|x+y|<c^{2}+x y$. If $x+y \geq 0$ then by $|x \circ y|<c$ iff $(c-x)(c-y)>0$. Similarly, one can treat the case $x+y<0$.

Clearly, 0 is the identity for $G$ and the inverse of $x$ is $-x$. It is easy to see that $\star$ is associative and commutative. Thus $(G, \star)$ is an abelian group structure. This example arises in Special Relativity.

Note that $\left(\mathbb{C}^{*}, \cdot\right)$ is a group structure.
Example 2.4 : For a positive integer $n$, let $\mathbb{I}_{n}$ denote the set of $n^{\text {th }}$ roots of unity:

$$
\begin{equation*}
\mathbb{I}_{n}:=\left\{\zeta \in \mathbb{C}: \zeta^{n}=1\right\} \tag{2.3}
\end{equation*}
$$

By the fundamental theorem of algebra, $\mathbb{I}_{n}$ consists of exactly $n$ elements including 1 . Geometrically, $\mathbb{I}_{n}$ consists of the vertices of the regular polygon with $n$ edges and with centroid the origin.

The binary structure $\left(\mathbb{I}_{n}, \cdot\right)$ is indeed a group structure. To see this, note first that $\mathbb{I}_{n} \subseteq \mathbb{C}^{*}$. Now $\zeta \in \mathbb{I}_{n}$ admits the inverse $1 / \zeta$. Associativity and commutativity of $\mathbb{I}_{n}$ follows from that of $\mathbb{C}^{*}$.

Exercise $2.5:$ Let $\mathbb{I}:=\cup_{n \geq 1} \mathbb{I}_{n}$. Show that $(\mathbb{I}, \cdot)$ is a group structure.
Exercise 2.6 : Fill in the blanks and justify:
(1) Let $\mathbb{A}(r, R)$ denote the annulus of inner-radius $r$ and outer-radius $R$ with the assumption that $0 \leq r<R \leq \infty$. Then the binary structure $(\mathbb{A}(r, R), \cdot)$ is a group structure if and only if $r=\cdots$ and $R=\cdots$.
(2) Let $X$ be a subset of the group structure $\left(\mathbb{C}^{*}, \cdot\right)$. Let $\mathbb{S}_{X}$ denote the set of $n \times n$ matrices $A \in M_{n}(\mathbb{C})$ such that the determinant $\operatorname{det}(A)$ of $A$ belongs to $X$. Then $\left(\mathbb{S}_{X}, \circ\right)$ is a $\cdots$ structure if and only if $(X, \cdot)$ is a $\cdots$ structure.
(3) Let $X$ be a set containing at least two elements and let $P(X)$ denote the power set of $X$. Define $A \star B$ (resp. $A * B$ ) be the symmetric difference (resp. difference) of $A$ and $B$. Then $(P(X), \star)$ (resp. $(P(X), *))$ is a $\cdots$ structure but not a $\cdots$ structure.

The following summarizes some elementary properties of the group.
Proposition 2.7. Let $G$ be a group. Every element of $G$ has a unique inverse. More generally, for $a, b, c \in G$ the following statements hold: If $a b=a c$ then $b=c$, and if $b a=c a$ then $b=c$. In particular, the inverse of $a \star b$ is given by $b^{-1} a^{-1}$.

Proof. We will only prove that if $a b=a c$ then $b=c$. Here inverse $a^{-1}$ of $a$ works as a catalyst. By the definition of binary operation, $a^{-1}(a b)$ and $a^{-1}(a c)$ define the same element of $G$. The desired conclusion now follows from the associativity of $G$.

Let us see a couple of applications of the last innocent result.
Exercise 2.8 : Let $G$ be a group and let $a \in G$. By $a^{2}$, we understand $a a$. Inductively, we define $a^{n}$ for all positive integers $n \geq 2$. Show that $(a b)^{n}=a^{n} b^{n}$ for all $a, b \in G$ if and only if $G$ is abelian.

Exercise 2.9 : Let $G$ be a group. Show that if $G$ is non-abelian then $G$ contains at least 5 elements.

Hint. Observe that there exists $x, y \in G$ such that $e, x, y, x y, y x$ are distinct elements of $G$.
Remark 2.10 : A rather extensive usage of Proposition 2.7 actually shows that a non-abelian group can not contain 5 elements. We will however deduce this fact later from a general result.

Example 2.11 : For a positive integer $n \geq 3$, consider the binary structure $D_{n}$ of all symmetries of a regular $n$-gon with origin as the centroid. As in Example 1.16, it can be seen that $D_{n}$ consists of rotations $R_{\theta}(\theta=$ $0,2 \pi / n, \cdots, 2 \pi(n-1) / n)$ and reflections $\rho_{\theta}(\theta=2 \pi / n, 4 \pi / n, \cdots, 2 \pi)$ (see (1.2)). Clearly, the rotation by 0 , the $2 \times 2$ identity matrix, plays the role of identity for $D_{n}$. Either geometrically or algebraically, observe the following:
(1) $R_{\theta}^{n}=R_{0}=\rho_{\theta}^{2}$.
(2) $R_{\theta} \rho_{\eta} R_{\theta}=\rho_{\eta}$.

In particular, the inverse of $R_{\theta}$ is $R_{\theta}^{n-1}$ and the inverse of $\rho_{\theta}$ is $\rho_{\theta}$ itself. Thus ( $D_{n}, \circ$ ) forms group structure, which is not abelian.

Remark 2.12: $\left(D_{3}, \circ\right)$ is the smallest non-abelian group structure.
Exercise 2.13 : Let $A$ be a set and let $P_{A}$ be the set of bijections $f: A \rightarrow A$. Show that $\left(S_{A}, \circ\right)$ is a group structure.

Example 2.14: For a positive integer $n$, let $A$ denote the set $\{1, \cdots, n\}$. Set $S_{n}:=S_{A}$. The group structure ( $S_{n}, \circ$ ) is known as the symmetric group. Note that $S_{n}$ contains $n$ ! elements.

A transformation $\phi$ between two group structures $(G, \star)$ and $\left(G^{\prime}, *\right)$ is said to be a group homomorphism if $\phi$ preserves the group operations: $\phi(a \star b)=$ $\phi(a) * \phi(b)$ for all $a, b \in G$. We say that $(G, \star)$ and $\left(G^{\prime}, *\right)$ are isomorphic if there exists a bijective homomorphism $\phi$ (known as isomorphism) between $(G, \star)$ and $\left(G^{\prime}, *\right)$.

Remark 2.15 : Let $e$ and $e^{\prime}$ denote the identities of $G$ and $G^{\prime}$ respectively. Let $\phi: G \rightarrow G^{\prime}$ be a homomorphism.
(1) Then $\phi(e)=e^{\prime}$. This follows from Proposition 2.7 in view of

$$
\phi(e) * e^{\prime}=\phi(e)=\phi(e \star e)=\phi(e) * \phi(e) .
$$

(2) By uniqueness of inverse, for any $a \in G$, the inverse of $\phi(a)$ is $\phi\left(a^{-1}\right)$.

Again, whenever there is no confusion, we suppress the symbols $\star$ and $*$.
Example 2.16 : Let $m, n$ be positive integers such that $m \leq n$. Define $\phi: S_{m} \rightarrow S_{n}$ by $\phi(\alpha)=\alpha(m+1)(m+2) \cdots(n)\left(\alpha \in S_{m}\right)$. Then $\phi$ is an injective, group homomorphism. Thus $\phi$ is an isomorphism iff $m=n$.

Let us verify that $S_{n}$ is abelian if and only if $n \leq 2$. Clearly, if $n=1,2$ then $S_{n}$ is abelian. Suppose $n \geq 3$. Since $\phi\left(S_{3}\right) \subseteq S_{n}$, it suffices to check that $S_{3}$ is non-abelian. To see that, consider $\alpha=(1,2,3)$ and $\beta=(1,2)(3)$. Then $\alpha \circ \beta=(1,3)(2)$ and $\beta \circ \alpha=(1)(2,3)$.

Example 2.17 : Consider the groups $\left(D_{n}, \circ\right)$ and ( $S_{n}, \circ$ ). Since $\left|D_{n}\right|=6$ and $\left|S_{n}\right|=n!,\left(D_{n}, \circ\right)$ and $\left(S_{n}, \circ\right)$ can not be isomorphic for $n \geq 4$. Suppose $n=3$. Define $\phi: D_{3} \rightarrow S_{3}$ by setting

$$
\begin{aligned}
\phi\left(R_{0}\right) & =(1)(2)(3), \phi\left(R_{2 \pi / 3}\right)=(1,2,3), \phi\left(R_{4 \pi / 3}\right)=(1,3,2), \\
\phi\left(\rho_{\pi / 3}\right) & =(1,2)(3), \phi\left(\rho_{2 \pi / 3}\right)=(1,3)(2), \phi\left(\rho_{\pi}\right)=(1)(2,3) .
\end{aligned}
$$

Clearly, $\phi$ is a bijection. Verify that $\phi$ is a group homomorphism. Likewise one can see that $D_{n}$ embeds into $S_{n}$.

Exercise 2.18: Let $\left(G_{n}, \circ\right)$ denote the smallest group structure consisting the $2 \times 2$ complex matrices

$$
F=\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right), C_{k}=\left(\begin{array}{cc}
e^{\frac{2 \pi k i}{n}} & 0 \\
0 & e^{-\frac{2 \pi k i}{n}}
\end{array}\right) \quad(k=0, \cdots, n-1) .
$$

Show that $\phi: G_{n} \rightarrow D_{n}$ governed by

$$
\phi(F)=\rho_{\pi / n}, \phi\left(C_{k}\right)=R_{2 \pi k / n}(k=0, \cdots, n-1)
$$

defines an isomorphism between $G_{n}$ and $D_{n}$.
Recall that a fractional linear transformation is a rational function $f_{a, b, c, d}$ of the form $\frac{a z+b}{c z+d}$, where $a, b, c, d$ are complex numbers such that $c z+d$ is not a multiple of $a z+b$, and $|c|+|d| \neq 0$.

Example 2.19 : Let $\mathcal{F}$ denote the set of all fractional linear transformations. Then $(\mathcal{F}, \circ)$ is a binary structure with identity $f_{1,0,0,1}$. Consider the transformation $\phi: \mathcal{F} \rightarrow M_{2}(\mathbb{C})$ given by

$$
\phi\left(f_{a, b, c, d}\right)=\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right) .
$$

Verify that $\phi$ preserves the binary operations. In particular, the common notation o employed for both matrix multiplication and composition of functions is fully justified. Since $\phi$ is not surjective, $(\mathcal{F}, \circ)$ and $\left(M_{2}(\mathbb{C}), \circ\right)$ are not isomorphic.

Let $(G, \star)$ be a group structure and let $S$ be a subset of $G$. We say that $S$ is a subgroup of $G$ if $(S, \star)$ is a group structure in its own right.

Note that $S$ is a subgroup of $G$ iff
(1) (Binary Structure) $a b \in S$ for every $a, b \in S$.
(2) (Existence of Identity) There exists $e^{\prime} \in S$ such that $e^{\prime} a=a=a e^{\prime}$ for all $a \in S$.
(3) (Existence of Inverse) For all $a \in S$, there exists $a^{-1} \in S$ such that $a a^{-1}=e=a^{-1} a$.

Remark 2.20 : Let $e$ denote the identity of $G$. Since $e^{\prime} e^{\prime}=e^{\prime}=e e^{\prime}$, by Proposition 2.24, we have $e^{\prime}=e$.

Exercise 2.21 : Let $G$ be a group, $a \in G$, and let $H$ be a subgroup of $G$. Verify that the following sets are subgroups of $G$ :
(1) (Normalizer of $a) N(a)=\{g \in G: a g=g a\}$.
(2) (Center of $G) Z_{G}=\{a \in G: a g=g a$ for all $g \in G\}$.
(3) (Conjugate of $H$ ) $a H a^{-1}=\left\{a h a^{-1}: h \in H\right\}$.

Remark 2.22 : Note that $a \in Z_{G}$ iff $N(a)=G$.
A permutation $\alpha \in S_{n}$ is a transposition if either $\alpha$ is the identity permutation or there exist integers $i<j$ such that $\alpha(k)=k$ for $k \neq i, j$ and $\alpha(i)=j, \alpha(j)=i$, that is, $\alpha=(j, i)$. A permutation is said to be even if it is a composition of even number of transpositions.

Example 2.23 : For a positive integer $n \geq 3$, consider the set $A_{n}$ of even permutations in $S_{n}$. Then $\left(A_{n}, \circ\right)$ is a subgroup of $S_{n}$. Let us see that $\left|A_{n}\right|=$ $n!/ 2$. To see that, note that $\psi: A_{n} \rightarrow S_{n} \backslash A_{n}$ given by $\psi(\alpha)=(2,1) \circ \alpha$ is a bijection. The group $\left(A_{n}, \circ\right)$ is known as the alternating group.

Note that $A_{3}=\{(1,2,3),(2,3,1),(3,1,2)\}$. It follows that $A_{3}$ is isomorphic to the group of rotational symmetries of an equilateral triangle with centroid the origin. The elements of $\left(A_{4}, \circ\right)$ can be realized as rotations of a tetrahedron.

Recall that a matrix $A$ is diagonalizable if there exists a diagonal matrix $D$ and an invertible matrix $B$ such that $A=B D B^{-1}$. The set of invertible, diagonalizable $2 \times 2$ matrices is not a subgroup of $G L_{2}(\mathbb{R})$.

Proposition 2.24. Let $G$ and $G^{\prime}$ be two group structures. If $\phi: G \rightarrow G^{\prime}$ is homomorphism then $\operatorname{ker} \phi$ (resp. ran $\phi$ ) is a subgroup of $G$ (resp. $G^{\prime}$ ).
Proof. We will only verify the first statement. By definition, the kernel of $\phi$ consists of those elements $a \in G$ for which $\phi(a)=e^{\prime}$, where $e^{\prime}$ denotes the identity of $G^{\prime}$. Now if $a, b \in \operatorname{ker} \phi$ then $\phi(a b)=\phi(a) \phi(b)=e^{\prime} e^{\prime}=e^{\prime}$. That is, the binary operation on $G$ is an induced operation on $\operatorname{ker} \phi$. If $e$ denotes the identity of $G$ then $\phi(e)=e^{\prime}($ Remark 2.15(1)), that is, $e \in \operatorname{ker} \phi$. Since $\phi\left(a^{-1}\right)=\phi(a)^{-1}\left(\right.$ Remark 2.15(2)), if $a \in \operatorname{ker} \phi$ then so is $a^{-1}$.

Exercise 2.25 : Consider the group structures $\left(\mathbb{C}^{*}, \cdot\right)$ and $(\mathbb{T}, \cdot)$. Define $\phi: \mathbb{C}^{*} \rightarrow \mathbb{T}$ by $\phi(z)=z /|z|$ for $z \in \mathbb{C}^{*}$. Show that $\phi$ is a surjective, group homomorphism. What is the kernel of $\phi$ ?

Let us examine a few instructive examples.
Example 2.26 : Consider the set $C[0,1]$ of real-valued continuous functions defined on the interval $[0,1]$. Since addition of continuous functions is continuous, $(C[0,1],+)$ is a group structure. Also, consider the additive group structure $(\mathbb{R},+)$ of real numbers.

Consider the mapping $\phi: C[0,1] \rightarrow \mathbb{R}$ given by $\phi(f)=\int_{0}^{1} f(t) d t$, the area under the curve $y=f(x)(x \in[0,1])$. Since area is additive, $\phi$ is a group homomorphism. Given a real number $\lambda$, if one consider the constant function $\kappa$ with constant value $\lambda$, then $\phi(\kappa)=\lambda$. Thus $\phi$ is surjective. The kernel of $\phi$ consists of those continuous functions $f$ in $C[0,1]$ for which the area under the curve $y=f(x)$ is 0 . We see below by explicit construction that the kernel of $\phi$ indeed is quite large.

Let $f \in C[0,1 / 2]$ be such that the graph of $f$ lies entirely below the X -axis and satisfies $f(1 / 2)=0$. Consider the reflection of $f$ along the line $x=1 / 2$, that is, the function $g \in C[1 / 2,1]$ given by

$$
g(x)=f(1-x)(x \in[1 / 2,1])
$$

Note that the area under $f$ is same as the area under $g$. Now define $h \in$ $C[0,1]$ as follows:

$$
\begin{aligned}
h(x) & =f(x) \text { for } x \in[0,1 / 2] \\
= & -g(x) \text { for } x \in[1 / 2,1] .
\end{aligned}
$$

Obviously, $h \in C[0,1]$ and $\phi(h)=0$.
Exercise 2.27 : Consider the map $\phi: C[0,1] \rightarrow \mathbb{R}$ given by $\phi(f)=f(0)$. Show that $\phi$ is a group homomorphism from $(C[0,1],+)$ onto $(\mathbb{R},+)$.

Example 2.28 : Consider the subgroup $G L_{n}(\mathbb{R})$ of $\left(M_{n}(\mathbb{R}), \circ\right.$ ) of real $n \times n$ matrices with non-zero determinant. Also, consider the multiplicative group $\left(\mathbb{R}^{*}, \cdot\right)$ of real numbers. Consider the mapping det : $G L_{n}(\mathbb{R}) \rightarrow \mathbb{R}^{*}$, which sends an $n \times n$ matrix to its determinant. Since determinant is multiplicative, det is a group homomorphism. If $\lambda \in \mathbb{R}^{*}$ then determinant of the diagonal matrix with diagonal entries $\lambda, 1, \cdots, 1$ is equal to $\lambda$. Thus det is surjective. The kernel of $\phi$ consists of all matrices in $G L_{n}(\mathbb{R})$ whose determinant is 1 . The kernel of $\phi$ is commonly denoted by $S L_{n}(\mathbb{R})$.

A subgroup $S$ of a group $G$ is said to be normal if for every $a \in S$ and every $b \in G$, the conjugate $b a b^{-1}$ is in $S$.

Trivially, any subgroup of an abelian group is normal.
Example 2.29 : The subgroup of rotations in $D_{n}$ is normal in $D_{n}$. This follows from the following facts:
(1) Any two rotations commute.
(2) If $r$ is a rotation and $\rho$ is a reflection then $\rho \circ r \circ \rho^{-1}=r^{-1}$
(see Example 2.11). Let us calculate the center of $D_{n}$. If follows from (2) above that a rotation $r$ commute with a reflection $\rho$ iff $r^{2}=1$ iff $r=r_{0}, r_{\pi}$. It follows that $Z_{D_{n}}=\left\{r_{0}, r_{\pi}\right\}$ if $n$ is even, and $Z_{D_{n}}=\left\{r_{0}\right\}$ otherwise.

Example 2.30 : The subgroup of invertible diagonal matrices is not normal in $\left(G L_{n}(\mathbb{R}), \circ\right)$.

Proposition 2.31. The kernel of a homomorphism is a normal subgroup.
Proof. In the notations of Proposition 2.24,

$$
\phi\left(b a b^{-1}\right)=\phi(b) \phi(a) \phi\left(b^{-1}\right)=\phi(b) e^{\prime} \phi(b)^{-1}=e^{\prime}
$$

in view of Remark 2.15(2).
Remark 2.32 : Note that $S L_{n}(\mathbb{R})$ is a normal subgroup of $\left(G L_{n}(\mathbb{R}), \circ\right)$.
Example 2.33 : The center of $\left(S L_{n}(\mathbb{R}), \circ\right)$ turns out to be the subgroup of scalar matrices. To see this, let $A \in S L_{n}(\mathbb{R})$. If $D \in S L_{n}(\mathbb{R})$ is the diagonal matrix with distinct diagonal entries then $A D=D A$ forces that $A$ must be diagonal. By interchanging the role of $A$ and $D$, one can see that the diagonal entries $A$ are identical.

Exercise 2.34 : Show that $Z_{S L_{n}(\mathbb{C})}$ is isomorphic to $\left(\mathbb{I}_{n}, \cdot\right)$ (see (2.3)).
Proposition 2.35. The center of a group is a normal subgroup.
Proof. Let $a \in Z_{G}$ and $b \in G$. For any $g \in G$, by associativity of $G$,

$$
\left(b a b^{-1}\right) g=b\left(a b^{-1} g\right)=b\left(b^{-1} g a\right)=g a
$$

By a similar argument, $g\left(b a b^{-1}\right)=a g$. Since $a \in Z_{G}$, so does $b a b^{-1}$.
Let $G$ be a group and let $a \in G$. If $H$ is a subset of $G$, then the subset $a H=\{a h: h \in H\}$ of $G$ is said to be a coset of $H$ in $G$.

Remark 2.36 : Any two cosets contain same number of elements. In fact, $\phi: a H \rightarrow H$ given by $\phi(a h)=h$ is a bijection.

Let $H$ be a subgroup of $G$. Note that $a H=b H$ iff $a^{-1} b \in H$. If one defines $a H \cong b H$ if $a^{-1} b$ then $\cong$ defines an equivalence relation on the collection of cosets of $H$. Define $G / H$ to be the collection of equivalence classes corresponding to the relation $\cong$. In particular, the cosets of $H$ in $G$ are either disjoint or identical. In case $G$ is finite, this statement becomes very interesting.

Theorem 2.37. (Lagrange) Let $H$ be a subgroup of a finite group $G$. Then $|G / H|=|G| /|H|$.

Proof. Note that $G$ is the disjoint union of $|G / H|$ number of (disjoint) cosets of $H$. Since any coset contains $|H|$ elements, $|G|=|H| \times|G / H|$.
Remark 2.38: Let $a \in G$ and let $k$ be the smallest positive integer such that $a^{k}=e$ (called the order of $a$ ). Then, since $\left\{e, a, \cdots, a^{k-1}\right\}$ is a subgroup of $G$, order of $a$ divides $|G|$. Thus the order of $a$ is at most $|G|$.

Corollary 2.39. If $|G|$ is a prime number then $G$ is cyclic, that is, there exists $a \in G$ such that $G=\left\{e, a, \cdots, a^{|G|-1}\right\}$.
Proof. Let $a \in G \backslash\{e\}$. Then the order of $a$ divides $|G|$. Since $|G|$ is prime, the order of $a$ is $|G|$, and hence $G=\left\{e, a, \cdots, a^{|G|-1}\right\}$.
Exercise 2.40 : Let $X$ be a finite set and let $\mathcal{F}$ be a collection of subsets of $X$ which is closed with respect to union and intersection. Show that there exists an integer $k$ such that $|\mathcal{F}|=2^{k}$.

Hint. $\mathcal{F}$ endowed with the symmetric difference is a group.
If $a H, b H \in G / H$ then we define $a H * b H=a b H$.
Proposition 2.41. $(G / H, *)$ is a binary structure if $H$ is normal in $G$.
Proof. We must check that $a b H$ is independent of representatives $a$ and $b$ of $a H$ and $b H$ respectively. Suppose that $a H=a^{\prime} H$ and $b H=b^{\prime} H$. Then $a^{-1} a^{\prime}, b^{-1} b^{\prime} \in H$. A simple algebra shows that

$$
(a b)^{-1} a^{\prime} b^{\prime}=b^{-1} a^{-1} a^{\prime} b^{\prime}=b^{-1} b^{\prime}\left(b^{\prime-1} a^{-1} a^{\prime} b^{\prime}\right) .
$$

It follows from the normality of $H$ that $(a b)^{-1} a^{\prime} b^{\prime} \in G / H$.
Remark 2.42 : If $H$ is normal then the binary structure $(G / H, *)$ is actually a group with identity $H$. In particular, $G / Z_{G}$ is a group.

Proposition 2.43. Let $\phi: G \rightarrow G^{\prime}$ be a group homomorphism. Then $\psi: G / \operatorname{ker} \phi \rightarrow \operatorname{ran} \phi$ given by $\psi(a \operatorname{ker} \phi)=\phi(a)$ is a group isomorphism.
Proof. Note that $\psi$ is well-defined:
$a \operatorname{ker} \phi=b \operatorname{ker} \phi$ iff $a b^{-1} \operatorname{ker} \phi$ iff $\phi(a) \phi\left(b^{-1}\right)=e$ iff $\phi(a)=\phi(b)$.
By Proposition 2.31 and Remark 2.42, $G / \operatorname{ker} \phi$ is a group. Since $\phi$ is a homomorphism, so is $\psi$. Clearly, $\psi$ is injective.

The following fact is analogous to rank-nullity theorem of Linear Algebra.
Corollary 2.44. Let $\phi: G \rightarrow G^{\prime}$ be a group homomorphism for a finite group $G$. Then

$$
|G|=|\operatorname{ker} \phi||\operatorname{ran} \phi| .
$$

Proof. By the last theorem, $G / \operatorname{ker} \phi$ is isomorphic to ran $\phi$. In particular, $|G / \operatorname{ker} \phi|=|\operatorname{ran} \phi|$. The formula now follows from Lagrange's Theorem.
Example 2.45 : Consider the group $\mathbb{Z}_{n}:=\mathbb{Z} / \bmod n$ with the binary operation addition modulo $n$. Define $\phi: \mathbb{Z}_{6} \rightarrow \mathbb{Z}_{6}$ by $\phi(k)=2 k$. Then $\operatorname{ker} \phi=$ $\{0,3\}$ and $\operatorname{ran} \phi=\{0,2,4\}$. Obviously, we have $\left|\mathbb{Z}_{6}\right|=6=|\operatorname{ker} \phi||\operatorname{ran} \phi|$.

## 3. Group Actions

Definition 3.1 : Let $X$ be a set and $G$ be a group. A group action of $G$ on $X$ is a map $*: G \times X \rightarrow X$ given by $(g, x) \longrightarrow g * x$ such that
(1) $(g h) * x=g *(h * x)$ for all $g, h \in G$ and $x \in X$.
(2) $e * x=x$ for all $x \in X$.

If this happens then we say that $G$ acts on $X$ and $X$ is a $G$-set.
Definition 3.2 : Let $*$ be a group action of $G$ on $X$. For $x \in X$, let $G x$ denote the subset $\{g * x: g \in G\}$ of $X$. Define an equivalence relation $\backsim$ on $X$ by setting $x \backsim y$ iff $G x=G y$. The equivalence class of $x$ is known as the orbit $\mathcal{O}_{x}$ of $x$.

Remark 3.3: Note that

$$
\mathcal{O}_{x}=\{y \in X: x \backsim y\}=\{y \in X: y=g * x \text { for some } g \in G\}=G x .
$$

Note that $X$ is the disjoint union of orbits of elements of $X$.
For $x \in X$, consider the function $\phi_{x}: G \rightarrow G x$ given by $\phi_{x}(g)=g * x$. Clearly, $\phi_{x}$ is surjective. Note that $\phi_{x}$ is bijective iff $\{g \in G: g * x=x\}=$ $\{e\}$. This motivates the following definition.
Definition 3.4: Let $*$ be a group action of $G$ on $X$. For $x \in X$, the stabiliser $\mathcal{S}_{x}$ of $x$ is defined by $\{g \in G: g * x=x\}$.

Remark 3.5 : Note that $e \in \mathcal{S}_{x}$ in view of (2) of Definition 3.1. Also, if $g, h \in \mathcal{S}_{x}$ then $(g h) * x=g *(h * x)=g * x=x$ by (1) of Definition 3.1. Further, if $g \in \mathcal{S}_{x}$ then by the same argument $g^{-1} * x=g^{-1} *(g * x)=x$. Thus $\mathcal{S}_{x}$ is a subgroup of $G$.

In view of the discussion prior to the definition, $\left|\mathcal{O}_{x}\right|=|G|$ if $\left|\mathcal{S}_{x}\right|=1$.
We try to understand the notions of group action, orbit and stabiliser through several examples.
Exercise 3.6 : Show that $\mathbb{R}^{n}$ acts on itself by translations: $x * y=x+y$. Find orbits and stabilisers of all points in $\mathbb{R}^{n}$.

Example 3.7 : Consider the group $\left(\mathbb{R}^{*}, \cdot\right)$ and the set $\mathbb{R}^{n}$. Consider the $\operatorname{map} \alpha *\left(x_{1}, \cdots, x_{n}\right):=\left(\alpha \cdot x_{1}, \cdots, \alpha \cdot x_{n}\right)$. By the associativity of $\mathbb{R}$, $(\alpha \cdot \beta) *\left(x_{1}, \cdots, x_{n}\right)=\left((\alpha \cdot \beta) \cdot x_{1}, \cdots,(\alpha \cdot \beta) \cdot x_{n}\right)=\alpha *\left(\beta *\left(x_{1}, \cdots, x_{n}\right)\right)$ for $\alpha, \beta \in \mathbb{R}^{*}$ and $\bar{x}=\left(x_{1}, \cdots, x_{n}\right) \in \mathbb{R}^{n}$. Clearly, $1 * \bar{x}=\bar{x}$ for every $\bar{x} \in \mathbb{R}^{n}$. Thus $\mathbb{R}^{*}$ acts on $\mathbb{R}^{n}$.

Let $\bar{x} \in \mathbb{R}^{n}$. The orbit $\mathcal{O}_{\bar{x}}$ is the punctured line in $\mathbb{R}^{n}$ passing through $\bar{x}$ and the origin 0 . Note that $\mathcal{S}_{\bar{x}}=\{1\}$ of $\mathbb{R}^{*}$ if $\bar{x} \neq 0$, and $S_{0}=\mathbb{R}^{*}$.

Example 3.8 : Consider the group structure ( $\mathbb{T}, \cdot)$ and the unit ball $\mathbb{B}$ centered at the origin. Then $t \cdot z \in \mathbb{B}$ for every $t \in \mathbb{T}$ and $z \in \mathbb{B}$. Since
multiplication is associative and $1 \cdot z=z$, the unit circle $\mathbb{T}$ acts on $\mathbb{B}$ via the complex multiplication.

The orbit $\mathcal{O}_{z}$ is the circle of radius $|z|$ with origin as the center. The stabiliser of all points except the origin is $\{1\}$. Clearly, $S_{0}=\mathbb{T}$.

Exercise 3.9 : Find all subsets $X$ of the complex plane such that the complex multiplication $\cdot$ is a group action of $(\mathbb{T}, \cdot)$ on $X$.

Exercise 3.10: Consider the power series $f(z, w)=\sum_{k, l=0}^{\infty} c_{k, l} z^{k} w^{l}$ in the complex variables $z$ and $w$. The domain of convergence $\mathcal{D}_{f}$ of $f$ is given by

$$
\left\{(z, w) \in \mathbb{C}^{2}: \sum_{k, l=0}^{\infty}\left|c_{k, l}\right||z|^{k}|w|^{l}<\infty\right\} .
$$

Show that the multiplicative group torus $\mathbb{T} \times \mathbb{T}$ acts on $\mathcal{D}_{f}$ via

$$
\left(\lambda_{1}, \lambda_{2}\right) *(z, w)=\left(\lambda_{1} z, \lambda_{2} w\right) .
$$

Discuss orbits and stabilizers.
Let $*$ be a group action of $G$ on $X$. We say that $*$ is transitive if there is only one (disjoint) orbit in $X$, and that $*$ is free if every point in $X$ has trivial stabilizer.

Exercise 3.11 : Show that the symmetric group $S_{n}$ acts on $X=\{1, \cdots, n\}$ via the action $*:(\sigma, j) \longrightarrow \sigma(j)$. Show that $*$ is transitive. Find the stabiliser of $j$.

Exercise 3.12 : Show that the symmetric group $S_{n}$ acts on $\mathbb{R}^{n}$ via

$$
\sigma *\left(x_{1}, \cdots, x_{n}\right)=\left(x_{\sigma(1)}, \cdots, x_{\sigma(n)}\right) .
$$

Describe orbits and stabilisers of $x \in \mathbb{R}^{n}$ such that $x_{1}=0, \cdots, x_{k}=0$ for some $1 \leq k \leq n$.

Exercise 3.13 : For an $n \times n$ matrix $A$ and $\bar{x} \in \mathbb{R}^{n}$, define $*$ by $A * \bar{x}=A \bar{x}$. For the group $G$ and set $X$, verify that $*$ defines a group action:
(1) $G L_{n}(\mathbb{R})$ and $\mathbb{R}^{n}$.
(2) $O_{n}(\mathbb{R})$ (group of orthogonal matrices) and $\mathbb{S}$ (unit sphere in $\mathbb{R}^{n}$ ).

Find orbits and stabilisers of all points in $X$ in both the cases.
Example 3.14 : Let us see an easy deduction of the following fact using group action: $S=\left\{A=\left(a_{i j}\right) \in G L_{2}(\mathbb{R}): a_{i 1}+a_{i 2}=1\right.$ for $\left.i=1,2\right\}$ is a subgroup of $G L_{2}(\mathbb{R})$. To see that, consider the group action of $G L_{2}(\mathbb{R})$ on $\mathbb{R}^{2}$ as discussed in the preceding exercise, and note that $S$ is precisely the stabilizer of the column vector $(1,1)^{T}$.

Example 3.15 : For a function $f: \mathbb{R} \rightarrow \mathbb{R}$ and $x \in \mathbb{R}$, consider the map $f * x=f(x)$. Note that $*$ is not a group action of the group $(C(\mathbb{R}),+)$ on $\mathbb{R}$.

Exercise 3.16 : Consider the automorphism group $A(\mathbb{D})$ of the unit disc $\mathbb{D}$ endowed with the composition:

$$
A(\mathbb{D})=\{f: \mathbb{D} \rightarrow \mathbb{D}: f \text { is a biholomorphism }\} .
$$

Show that the action $f * z=f(z)$ of $A(\mathbb{D})$ on $\mathbb{D}$ is transitive but not free.
Hint. Schwarz Lemma from Complex Analysis.
Exercise 3.17 : Let $\mathcal{B}$ denote the set of ordered bases $\left(e_{1}, e_{2}\right)$ of $\mathbb{R}^{2}$. Show that $G L_{2}(\mathbb{R})$ acts $\mathcal{B}$ via $A *\left(e_{1}, e_{2}\right)=\left(A e_{1}, A e_{2}\right)$. Describe the orbit and stabiliser of $\left(e_{1}, e_{2}\right)$.

Example 3.18 : Consider the group $\mathbb{Z}_{2}$ and the unit sphere $\mathbb{S}_{n}$ in $\mathbb{R}^{n}$. Define $*$ by $0 * x=x$ and $1 * x=-x$. Verify that $*$ is a free action of $\mathbb{Z}_{2}$ on $\mathbb{S}_{n}$.

Note that $\mathcal{O}_{x}=\{x,-x\}$ for any $x \in \mathbb{S}_{n}$. Clearly, $\mathcal{S}_{x}=\{0\}$. Although, we do not required this fact, note that the real projective $n$-space $\mathbb{R} P^{n}$ is the space of orbits $\mathcal{O}_{x}$ endowed with the quotient topology.

The following example arises in the dynamics of projectile.
Exercise 3.19 : Verify that

$$
t *\left(x, y, z, v_{1}, v_{2}, v_{3}\right)=\left(x+v_{1} t, y+v_{2} t, z-g t^{2} / 2+v_{3} t, v_{1}, v_{2}, v_{3}-g t\right)
$$

is a group action of the additive group $\mathbb{R}$ on $\mathbb{R}^{6}$, where $g$ is a real constant. Discuss orbits and stabilizers.

## 4. Fundamental Theorem of Group Actions

Theorem 4.1. Let $G$ be a finite group acting on a set $X$. Then:
(1) If $X$ is finite then there exist disjoint orbits $\mathcal{O}_{x_{1}}, \cdots, \mathcal{O}_{x_{k}}$ such that

$$
|X|=\left|\mathcal{O}_{x_{1}}\right|+\cdots+\left|\mathcal{O}_{x_{k}}\right|
$$

(2) The stabilizer $\mathcal{S}_{x}$ of $x$ is a subgroup of $G$ for every $x \in X$.
(3) (Orbit-Stabilizer Formula) For each $x \in X$,

$$
\left|G / \mathcal{S}_{x}\right|=\left|\mathcal{O}_{x}\right| \text { and }|G|=\left|\mathcal{O}_{x}\right|\left|\mathcal{S}_{x}\right| .
$$

(4) If $y \in \mathcal{O}_{x}$ then there exists $h \in G$ such that $\mathcal{S}_{x}=h \mathcal{S}_{y} h^{-1}$.
(5) The map $\phi: G \rightarrow S_{X}$ given by $\phi(g)=M_{g}$ is a group homomorphism, where $M_{g} \in S_{X}$ is defined by $M_{g}(x)=g * x$.
(6) $\operatorname{ker}(\phi)=\cap_{x \in X} \mathcal{S}_{x}$.

Proof. (1) This part follows from Remark 3.3.
(2) This is already noted in Remark 3.5.
(3) By (2) and the Lagrange's Theorem, $|G|=\left|G / \mathcal{S}_{x}\right|\left|\mathcal{S}_{x}\right|$. Thus it suffices to check that $\left|G / \mathcal{S}_{x}\right|=\left|\mathcal{O}_{x}\right|$. To see that, we define $\psi: G / \mathcal{S}_{x} \rightarrow \mathcal{O}_{x}$ by $\psi\left(g \mathcal{S}_{x}\right)=g * x$.
$\psi$ is well-defined and bijective: Note that $g \mathcal{S}_{x}=h \mathcal{S}_{x}$ iff $h^{-1} g \in \mathcal{S}_{x}$ iff $\left(h^{-1} g\right) * x=x$ iff $g * x=h * x$. Clearly, $\psi$ is surjective.
(4) Let $y \in \mathcal{O}_{x}$. Then $x=h * y$ for some $h \in G$, and hence by condition (1) of Definition 3.1,

$$
\begin{aligned}
\mathcal{S}_{x} & =\{g \in G: g * x=x\}=\{g \in G: g *(h * y)=h * y \text { for some } h \in G\} \\
& =\left\{g \in G: h^{-1} g h \in \mathcal{S}_{y}\right\}=h \mathcal{S}_{y} h^{-1} .
\end{aligned}
$$

(5) First note that $\phi$ is well-defined since $M_{g}$ is bijective with inverse $M_{g^{-1}}$. Since $M_{g h}=M_{g} \circ M_{h}, \phi$ is a group homomorphism.
(6) Note that
$\operatorname{ker}(\phi)=\left\{g \in G: M_{g}=M_{e}\right\}=\{g \in G: g * x=x$ for all $x \in X\}=\cap_{x \in X} \mathcal{S}_{x}$.
This completes the proof of the theorem.
Corollary 4.2. Let $*$ be a group action of $G$ on $X$. If $*$ is transitive then $\left|\mathcal{S}_{x}\right|=|G| /|X|$ for every $x \in X$. If $*$ is free then $\left|\mathcal{O}_{x}\right|=|G|$ for every $x \in X$.

We will refer to $\phi$ as the permutation representation of $G$ on $X$. We say that $\phi$ is faithful if $\operatorname{ker}(\phi)=\{e\}$.

Example 4.3 : Consider the square $S$ with vertices $v_{1}=(1,1), v_{2}=$ $(-1,1), v_{3}=(-1,-1), v_{4}=(1,-1)$. Consider the dihedral group $D_{4}$ of symmetries of $S$ and the set $X=\left\{\left(v_{1}, v_{3}\right),\left(v_{2}, v_{4}\right)\right\}$ of unordered pairs. Then $A *(u, v)=(A u, A v)$ defines a group action of $D_{4}$ on $X$.

Clearly, the orbit of any point is $X$, and hence $*$ is transitive. Also, $r_{\pi} \in \mathcal{S}_{\left(v_{1}, v_{3}\right)} \cap \mathcal{S}_{\left(v_{2}, v_{4}\right)}$. In particular, the action $*$ is not faithful.

If $X$ is finite then $S_{X}$ is isomorphic to $S_{|X|}$. Thus we have:
Corollary 4.4. Let $\phi$ be a permutation representation of $G$ on $X$. If $\phi$ is faithful then $G$ is isomorphic to a subgroup of the permutation group $S_{|X|}$.
Example 4.5 : Consider the group $G L_{2}\left(\mathbb{Z}_{2}\right)$ of invertible matrices with entries from the field $\mathbb{Z}_{2}$. Then $\left|G L_{2}\left(\mathbb{Z}_{2}\right)\right|=6$. Consider the set $X=$ $\left\{e_{1}, e_{2}, e_{1}+e_{2}\right\}$, where $e_{1}=\left[\begin{array}{ll}1 & 0\end{array}\right]^{T}$ and $e_{2}=\left[\begin{array}{ll}0 & 1\end{array}\right]^{T}$. Then $G L_{2}\left(\mathbb{Z}_{2}\right)$ acts on $X$ via $A * \bar{x}=A \bar{x}$.

Let $\phi$ denote the permutation representation of $G L_{2}\left(\mathbb{Z}_{2}\right)$ on $X$. If $A \in$ ker $\phi$ then $A \bar{x}=\bar{x}$ for every $\bar{x} \in X$. However, $A e_{i}$ is the $i$ th column of $A$ for $i=1,2$. Therefore $A$ is the identity matrix, and $\phi$ is faithful. By Corollary 4.4, $G L_{2}\left(\mathbb{Z}_{2}\right)$ isomorphic to $S_{3}$.

Let $p$ be a prime number. A group $G$ is said to be a $p$-group if $|G|=p^{k}$ for some positive integer $k$.
Corollary 4.6. Let $G$ be a p-group acting on $X$. If

$$
S=\left\{x \in X: \mathcal{O}_{x} \text { is singleton }\right\},
$$

then $|S|=|X| \bmod p$.
Proof. Let $\mathcal{O}_{x_{1}}, \cdots, \mathcal{O}_{x_{r}}$ be all disjoint orbits of $X$ of size bigger than 1 . Then $|X|=|S|+\left|\mathcal{O}_{x_{1}}\right|+\cdots+\left|\mathcal{O}_{x_{r}}\right|$. By Theorem 4.1, each $\left|\mathcal{O}_{x_{i}}\right|$ divides $|G|$, and hence a multiple of $p$. This gives $|S|=|X| \bmod p$.

## 5. Applications

In this section, we discuss several applications of the fundamental theorem of group actions to the group theory.

### 5.1. A Theorem of Lagrange.

Example 5.1 : The symmetric group $S_{n}$ acts on the set $\mathbb{C}\left[z_{1}, \cdots, z_{n}\right]$ of complex polynomials in $n$ variables $z_{1}, \cdots, z_{n}$ via

$$
\sigma * p\left(z_{1}, \cdots, z_{n}\right)=p\left(z_{\sigma(1)}, \cdots, z_{\sigma(n)}\right) .
$$

Let $p$ be in $\mathbb{C}\left[z_{1}, \cdots, z_{n}\right]$. Clearly, the identity permutation fixes $p$. Also,

$$
\begin{aligned}
(\sigma \tau) * p\left(z_{1}, \cdots, z_{n}\right) & \left.=p\left(z_{\sigma \tau(1)}, \cdots, z_{\sigma \tau(n)}\right)=p\left(z_{\sigma(\tau(1))}, \cdots, z_{\sigma(\tau(n)}\right)\right) \\
& =\sigma * p\left(z_{\tau(1)}, \cdots, z_{\tau(n)}\right)=\sigma *\left(\tau * p\left(z_{1}, \cdots, z_{n}\right)\right) .
\end{aligned}
$$

The orbit of $p$ is $\left\{p\left(z_{\sigma(1)}, \cdots, z_{\sigma(n)}\right) \in \mathbb{C}\left[z_{1}, \cdots, z_{n}\right]: \sigma \in S_{n}\right\}$ and the stabilizer of $p$ is $\left\{\sigma \in S_{n}: p\left(z_{\sigma(1)}, \cdots, z_{\sigma(n)}\right)=p\left(z_{1}, \cdots, z_{n}\right)\right\}$.

Theorem 5.2. For any polynomial $p \in \mathbb{C}\left[z_{1}, \cdots, z_{n}\right]$, the number of different polynomials we obtain from $p$ through permutations of the variables $z_{1}, \cdots, z_{n}$ is a factor of $n$ !.

### 5.2. A Counting Principle.

Example 5.3: Let $H, K$ be two subgroups of the group $G$. Then $K$ acts on the collection $\{a H: a \in G\}$ of cosets of $H$ by $k *(a H):=(k a) H$.

The orbit of $a H$ is $\{k a H: k \in K\}$. The stabiliser of $a H$ is the subgroup $\left(a^{-1} H a\right) \cap K$.

Suppose $H=K$. Then $H$ is normal in $G$ iff the orbit of $a H$ is singleton for every $a \in G$.

Theorem 5.4. For subgroups $H, K$ of a finite group $G$, let $K H:=\{k h$ : $k \in K, h \in H\}$. Then

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

Proof. Consider the group action $K$ on the cosets of $H$ as discussed in Example 5.3. Then $\mathcal{O}_{H}=\{k H: k \in K\}$ and $\mathcal{S}_{H}=H \cap K$. By Theorem 4.1, $|K|=\left|\mathcal{O}_{H}\right||H \cap K|$. Also, since $K H$ is the disjoint union of cosets in $\mathcal{O}_{H}$ and since $|k H|=|H|$,

$$
|K H|=\left|\mathcal{O}_{H}\right||H|=\frac{|K||H|}{|H \cap K|} .
$$

This completes the proof of the corollary.

### 5.3. Cayley's Theorem.

Example 5.5 : Consider the group action of $K$ on $\{a H: a \in G\}$ as discussed in Example 5.3. The choice $H=\{e\}$ and $K=G$ gives the left multiplication action of $G$ on itself: $(g, h) \longrightarrow g h$. Note that $\mathcal{O}_{g}=G$ and $\mathcal{S}_{g}=\{e\}$ for any $g \in G$. In particular, the permutation representation of $G$ on $G$ is transitive and faithful.

Theorem 5.6. Every finite group is isomorphic to a subgroup of a symmetric group.

Proof. Consider the left multiplication action of $G$ on itself. Let $\phi$ be the corresponding permutation representation of $G$ on $X$. By Corollary 4.4, it suffices to check that $\phi$ is faithful. This is noted in the last example.

Exercise 5.7 : Let $G$ be a group of order $n$. Prove:
(1) Let $g_{1}, g_{2}, \cdots, \in G$ be such that $g_{1} \neq e$ and $H_{i} \subsetneq H_{i+1}$, where $H_{i}$ is the subgroup generated by $g_{1}, \cdots, g_{i}$. Then $\left|H_{i}\right| \geq 2^{i}$ for each $i$.
(2) $G$ can be generated by at most $\log _{2} n$ elements.

Use the Cayley's Theorem to conclude that the number of non-isomorphic groups of order $n$ does not exceed $(n!)^{\log _{2} n}$.
5.4. The Class Equation. Let us discuss another important group action of $G$ on itself.

Example 5.8 : Let $G$ be a group. Define $*: G \times G \rightarrow G$ by $g * x=g x g^{-1}$. By Proposition 2.7 and associativity of $G$,

$$
(g h) * x=(g h) x(g h)^{-1}=g\left(h x h^{-1}\right) g^{-1}=g(h * x) g^{-1}=g *(h * x)
$$

for every $g, h, x \in G$. Also, since $e * x=e x e^{-1}=x$ for every $x \in G$, the map * defines a group action of $G$ onto itself.

Note that $\mathcal{O}_{x}$ is the set of all conjugate elements of $x$. The stabiliser $\mathcal{S}_{x}$ of $x$ is the normalizer $N(x)$ of $x$.

We will refer to the group action of the last example as the conjugate group action of $G$. The orbit $\mathcal{O}_{x}$ will be referred as the conjugacy class of $G$.

Exercise 5.9 : Consider the conjugate group action $*$ of $G$ on itself. Verify:
(1) If $x, y \in Z_{G}$ then $x=g * y$ for some $g \in G$ iff $x=y$.
(2) $\mathcal{O}_{a}=\{a\}$ iff $a \in Z_{G}$.

Theorem 5.10. Let $G$ be a p-group. Then $\left|Z_{G}\right|$ is divisible by $p$.
Proof. Apply Corollary 4.6 to the conjugate group action of $G$ on itself.
Exercise 5.11 : Let $G$ be a $p$-group such that $|G|=p^{2}$. Show that $G$ is abelian. Conclude that $G$ is isomorphic either to $\mathbb{Z}_{p^{2}}$ or $\mathbb{Z}_{p} \times \mathbb{Z}_{p}$.

Theorem 5.12. Let $G$ be a finite group. Then

$$
|G|=\left|Z_{G}\right|+\sum \frac{|G|}{|N(x)|},
$$

where this sum runs over one element $x$ from each conjugacy class with $N(x) \neq G$.
Proof. Consider the conjugate group action $*$ of $G$ onto itself. We observed in Example 5.8 that $\mathcal{S}_{x}=N(x)$. By Theorem 4.1, there exist disjoint orbits of $\mathcal{O}_{x_{1}}, \cdots, \mathcal{O}_{x_{k}}$ such that
$|G|=\left|\mathcal{O}_{x_{1}}\right|+\cdots+\left|\mathcal{O}_{x_{k}}\right|=\frac{|G|}{\left|\mathcal{S}_{x_{1}}\right|}+\cdots+\frac{|G|}{\left|\mathcal{S}_{x_{k}}\right|}=\frac{|G|}{\left|N\left(x_{1}\right)\right|}+\cdots+\frac{|G|}{\left|N\left(x_{k}\right)\right|}$.
Now if $x_{i} \in Z_{G}$ then $N\left(x_{i}\right)=G$, and if $x_{i}, x_{j} \in Z_{G}$ for $i \neq j$ then the conjugacy classes of $x_{i}$ and $x_{j}$ are disjoint (Exercise 5.9). The desired conclusion follows immediately.

Remark 5.13 : One may derive Theorem 5.10 from the class equation: $\left|Z_{G}\right|=|G|-\sum|G| /|N(x)|$, where $N(x)$ is a proper subgroup of $G$.

Example 5.14 : Consider the conjugate group action of the dihedral group $D_{4}$ on itself. We already noted in Example 2.29 that $Z_{D_{4}}=\left\{r_{0}, r_{\pi}\right\}$. In particular, $N\left(r_{0}\right)=D_{4}=N\left(r_{\pi}\right)$.

Note that the normalizer of any rotation $x$ contains exactly 4 elements (all the rotations in $D_{4}$ ). Note further that the normalizer of any reflection $x$ contains exactly 4 elements ( 2 elements in $Z_{D_{4}}, x=\rho_{\theta}$ and $\rho_{\theta+\pi}$ ). Note also that $r_{\pi / 2}$ and $r_{3 \pi / 2}$ are conjugate to each other, and hence belong to same conjugacy class. Note next that $\rho_{\pi / 2}$ and $\rho_{\pi}$ (resp. $\rho_{3 \pi / 2}$ and $\rho_{2 \pi}$ ) are conjugates. Hence the class equation for $D_{4}$ is

$$
\left(\left|D_{4}\right|=8\right)=\left(\left|Z_{D_{4}}\right|=2\right)+\left(\left|\mathcal{O}_{r_{\pi / 2}}\right|=2\right)+\left(\left|\mathcal{O}_{\rho_{\pi / 2}}\right|=2\right)+\left(\left|\mathcal{O}_{\rho_{3 \pi / 2}}\right|=2\right) .
$$

Exercise 5.15 : Verify that the conjugacy classes of the permutation group $S_{3}$ are $\{(1)\},\{(1,2),(1,3),(2,3)\},\{(1,2,3),(1,3,2)\}$. Conclude that the class equation of $S_{3}$ is

$$
\left(\left|S_{3}\right|=6\right)=\left(\left|Z_{S_{3}}\right|=1\right)+\left(\left|\mathcal{O}_{(1,2)}\right|=3\right)+\left(\left|\mathcal{O}_{(1,2,3)}\right|=2\right) .
$$

### 5.5. Cauchy's Theorem.

Example 5.16 : Let $G$ be a group and let $H$ be the multiplicative group $\{1,-1\}$. Consider the action $1 * g=g$ and $(-1) * g=g^{-1}$ of $H$ on $G$. It is easy to verify that $*$ is a group action.

Let $g \in G$. The orbit of $g$ is $\left\{g, g^{-1}\right\}$ if $g \neq e$, and $\{e\}$ otherwise. The stabiliser of $g$ is $\{1\}$ if $g^{2} \neq e$, and $\{1,-1\}$ otherwise.

Here is a particular case of the Cauchy's Theorem.
Exercise 5.17 : Prove that there exist odd number of elements of order 2 in a group of even order.

Hint. Apply Theorem 4.1 to the action discussed in Example 5.16.
Example 5.18 : Let $G$ be a group and let $p$ be a prime number. Let $H$ denote the group generated by the permutation $\sigma \in S_{p}$ given by $\sigma(j)=j+1$ for $j=1, \cdots, p-1$ and $\sigma(p)=1$. Note that $|H|=p$. Consider the set

$$
X=\left\{\left(g_{1}, \cdots, g_{p}\right): g_{1}, \cdots, g_{p} \in G, g_{1} \cdots g_{p}=e\right\} .
$$

Since there are $p$ parameters and 1 equation, $p-1$ variables are free, and hence $|X|=|G|^{p-1}$.

Suppose $\left(g_{1}, \cdots, g_{p}\right) \in X$. Then $g_{1}$ commutes with $g_{2} \cdots g_{p}$, and hence $\left(g_{\sigma(1)}, \cdots, g_{\sigma(p)}\right) \in X$. By finite induction, we get $\left(g_{\sigma^{j}(1)}, \cdots, g_{\sigma^{j}(p)}\right) \in X$ for $j=1, \cdots, p$. This enables us to define

$$
\tau *\left(g_{1}, \cdots, g_{p}\right)=\left(g_{\tau(1)}, \cdots, g_{\tau(p)}\right)\left(\tau \in H,\left(g_{1}, \cdots, g_{p}\right) \in X\right)
$$

Then $*$ is indeed a group action of $H$ on $X$. We verify only condition (2) of Definition 3.1:

$$
\begin{aligned}
(\sigma \tau) *\left(g_{1}, \cdots, g_{p}\right) & \left.=\left(g_{\sigma \tau(1)}, \cdots, g_{\sigma \tau(p)}\right)=\left(g_{\sigma(\tau(1))}, \cdots, g_{\sigma(\tau(p)}\right)\right) \\
& =\sigma *\left(g_{\tau(1)}, \cdots, g_{\tau(p)}\right)=\sigma *\left(\tau *\left(g_{1}, \cdots, g_{p}\right)\right) .
\end{aligned}
$$

The orbit of $(e, \cdots, e)$ is $\{(e, \cdots, e)\}$. More generally, $\left|\mathcal{O}_{\left(g_{1}, \cdots, g_{p}\right)}\right|=1$ iff $g_{1}=\cdots=g_{p}$ and $g_{1}^{p}=e$. Finally, the stabiliser of any element in $X$ consists only the identity permutation in $S_{p}$.

Theorem 5.19. Let $G$ be a finite group and $p$ be a prime such that $p$ divides $|G|$. If $P$ denotes the set of elements of $G$ of order $p$, then $|P| \equiv-1 \bmod p$.

Proof. Consider the action of $H$ on $X$ as discussed in Example 5.18. Recall that $|H|=p,|X|=|G|^{p-1}$, and the fact that $\left|\mathcal{O}_{\left(g_{1}, \cdots, g_{p}\right)}\right|=1$ iff $g_{1}=g_{2}=$ $\cdots=g_{p}$ and $g_{1}^{p}=e$.

By Theorem 4.1, there exist disjoint orbits of $\mathcal{O}_{x_{1}}, \cdots, \mathcal{O}_{x_{k}}$ such that

$$
|X|=\left|\mathcal{O}_{x_{1}}\right|+\cdots+\left|\mathcal{O}_{x_{k}}\right|=1+\sum_{\mathcal{O}_{x_{i}} \neq \mathcal{O}_{(e, \cdots, e)}}\left|\mathcal{O}_{x_{i}}\right| .
$$

Since $|X|=|G|^{p-1}$ and $G$ is a $p$-group, $1+\sum_{x_{i} \neq(e, \cdots, e)}\left|\mathcal{O}_{x_{i}}\right|=l p$ for some positive integer $l$. Again, by Theorem 4.1, $\left|\mathcal{O}_{x_{i}}\right|$ divides $|H|=p$, and hence $\left|\mathcal{O}_{x_{i}}\right|$ is either 1 or $p$. Let $Y=\left\{x_{i}: \mathcal{O}_{x_{i}} \neq \mathcal{O}_{(e, \cdots, e)},\left|\mathcal{O}_{x_{i}}\right|=1\right\}$. It follows that $1+|Y|+(k-1-|Y|) p=l p$. Thus we have $|Y|=-1 \bmod p$.

Define $\phi: P \rightarrow Y$ by $\phi(g)=(g, \cdots, g)$. Clearly, $\phi$ is injective. If $\left(g_{1}, \cdots, g_{p}\right) \in Y$ then $\left|\mathcal{O}_{\left(g_{1}, \cdots, g_{p}\right)}\right|=1$. Then we must have $g_{1}=\cdots=g_{p}$ and $g_{1}^{p}=e$. Thus $\phi\left(g_{1}\right)=\left(g_{1}, \cdots, g_{p}\right)$, and hence $\phi$ is surjective.
Remark 5.20 : A group of order 6 must contain an element of order 3. In particular, there exists no group of order 6 containing identity and 5 elements of order 2 .

Example 5.21: Let $G$ be a group of order 6 . Then $G$ contains an element $x$ of order 3 and an element $y$ of order 2. If $i$ is not a multiple of 3 then
$\left(x^{i}\right)^{3}=\left(x^{3}\right)^{i}=e$ and $\left(x^{i}\right)^{2} \neq e$. Similarly, the order of $y^{j}$ is 3 if $j$ is not a multiple of 2 . Now if $x^{i} y^{j}=x^{r} y^{s}$ then $x^{i-r}=y^{s-j}$, and hence $i=r$ $\bmod 3$ and $s=j \bmod 2$. Thus $G=\left\{x^{i} y^{j}: 0 \leq i \leq 2,0 \leq j \leq 1\right\}$. Now $y x \in G$, and clearly, $y x \notin\left\{e, x, y, x^{2}\right\}$. Hence there are only two choices of $y x$, namely, $x y$ or $x^{2} y$. If $x y=y x$ then $G$ is the cyclic group of order 6 . If $y x=x^{2} y$ or $y x y^{-1}=x^{-1}$ then $G$ is isomorphic to the dihedral group $D_{3}$.

### 5.6. First Sylow Theorem.

Example 5.22 : Let $G$ be a group. For a positive integer $n \leq|G|$, let $\mathcal{F}_{n}$ denote the collection of all subsets $A$ of $G$ such that $|A|=n$. Note that $\left|\mathcal{F}_{n}\right|=\binom{|G|}{n}$. Then $G$ acts on $\mathcal{F}_{n}$ by $(g, A) \longrightarrow g A$. Indeed, $|g A|=|A|$, $e A=A$ and $\left(g_{1} g_{2}\right) * A=g_{1} *\left(g_{2} A\right)$.

The orbit $\mathcal{O}_{A}$ of $A$ equals $\{g A: g \in G\}$ and the stabilizer $\mathcal{S}_{A}$ of $A$ equals $\{g \in G: g A=A\}$. If $a \in A$ then $\mathcal{S}_{A} a=\{g a: g A=A\} \subseteq A$.

Suppose $|G|=p^{n} q$, where $p$ is a prime not dividing $q$. Then a Sylow $p$ subgroup is a subgroup of order $p^{n}$. A subgroup is called $p$-subgroup if it is a $p$-group.

Remark 5.23 : Let $a$ belong to a Sylow $p$-subgroup such that $a \neq e$. By the Lagrange's Theorem, the order $a$ is $p^{r}$ for some positive integer $r$. Then the order of $a^{p^{r-1}}$ is precisely $p$.

The First Sylow Theorem partly generalizes the Cauchy's Theorem.
Theorem 5.24. Let $G$ be a finite group. If $p$ is a prime divisor of $|G|$ then $G$ has a Sylow p-subgroup.

Proof. Suppose $|G|=p^{n} q$, where $q$ is not divisible by $p$. Consider the group action of $G$ on $X:=\mathcal{F}_{p^{n}}$ as discussed in Example 5.22 . We need the fact that $\left|\mathcal{F}_{p^{n}}\right|=\binom{p^{n} q}{p^{n}}$ is not divisible by $p$. Then by Theorem $4.1(1)$, there exists $A \in \mathcal{F}_{p^{n}}$ such that $\left|\mathcal{O}_{A}\right|$ is not divisible by $p$. By the orbit-stabilizer formula, $p^{n} q=\left|\mathcal{S}_{A}\right|\left|\mathcal{O}_{A}\right|$, and hence $\left|\mathcal{S}_{A}\right|$ is divisible by $p^{n}$. Also, $\left|\mathcal{S}_{A}\right|=\left|\mathcal{S}_{A} a\right|$ and $\mathcal{S}_{A} a \subseteq A$ for any $a \in A$. It follows that $\left|\mathcal{S}_{A}\right|=p^{n}$.

### 5.7. Second Sylow Theorem.

Remark 5.25 : Since $\left|a H a^{-1}\right|=|H|$, if $H$ is a Sylow $p$-subgroup of $G$ then so is the conjugate $a H a^{-1}$ of $H$. If $G$ has only one Sylow $p$-subgroup $H$ then $H$ is necessarily normal in $G$.

Theorem 5.26. Let $G$ be a finite group and let $p$ be a prime divisor of $|G|$. If $H$ is a Sylow p-subgroup of $G$ and $K$ is a $p$-subgroup of $G$ then there exists $a \in G$ such that $K \subseteq a H a^{-1}$.

In particular, any two Sylow p-subgroups are conjugate.
Proof. Consider the group action of $K$ on the collection $X=\{a H: a \in G\}$ of cosets of $H$ by $k *(a H):=(k a) H$ (see Example 5.3). Let $S$ denote the set of
cosets $a H$ with single-ton orbits. Since $K$ is a $p$-subgroup, by Corollary 4.6, $|S|=|X| \bmod p$. However, by the Lagrange's Theorem, $|X|=|G| /|H|=q$, where $q$ is not divisible by $p$. This implies that $|S|=q \bmod p$, and hence $S$ is non-empty. Let $a H \in S$. Then $k a H=a H$ for every $k \in K$, that is, $a^{-1} k a \in H$ for every $k \in K$. This completes the proof of the first part.

If in addition $K$ is also a $p$-Sylow subgroup then $|K|=p^{n}=|H|=$ $\left|a H a^{-1}\right|$. By the first part, we must have $K=a H a^{-1}$ in this case.

Remark 5.27 : Let $H$ be a Sylow $p$-subgroup of $G$. Then $H$ is a unique Sylow $p$-subgroup of $G$ iff $H$ is normal in $G$.

### 5.8. Third Sylow Theorem.

Example 5.28 : Let $G$ be a group and $H, K$ be subgroups of $G$. Let $X:=$ $\left\{a H a^{-1}: a \in G\right\}$ be a collection of subgroups of $G$. Then $K$ acts on $X$ by $(g, L) \longrightarrow g L g^{-1}$. We just check condition (2) of Definition 3.1:

$$
(g h) * L=(g h) L(g h)^{-1}=g\left(h L h^{-1}\right) g^{-1}=g *(h * L)
$$

for any $g, h \in K$ and $L \in X$.
Suppose $K:=G$. Then the orbit of any element in $X$ is the entire $X$. Also, the stabiliser of $K \in X$ is the subgroup $\{g \in G: g K=K g\}$, the normalizer $N(K)$ of $K$.

Theorem 5.29. Let $G$ be a group such that $|G|=p^{n} q$, where $p$ is a prime number which does not divide $q$. Then the number $N_{p}$ of Sylow $p$-subgroups of $G$ divides $q$. Moreover, $N_{p}=1+k p$ for some non-negative integer $k$.

Proof. Let $H$ be a Sylow $p$-subgroup of $G$. Consider the group action of $K:=G$ on $X$ as discussed in Example 5.28. By the Second Sylow Theorem, $X$ consists of all Sylow $p$-subgroups of $G$. Thus $N_{p}=|X|$. Recall that $\mathcal{O}_{H}=$ $X$ and $\mathcal{S}_{H}=N(H)$. By the orbit-stabilizer formula, $|G|=|X||N(H)|$. In particular, $N_{p}$ divides $|G|$. Since $H \subseteq N(H)$, by the Lagrange's Theorem, $|H|$ divides $|N(H)|$. It follows that $N_{p}=|G| /|N(H)|$ divides $|G| /|H|=q$. In particular, $N_{p}$ is not divisible by $p$.

Consider the group action of $K:=H$ on $X$ as described in Example 5.28. Let $S=\left\{L \in X: \mathcal{O}_{L}=\{L\}\right\}$. By Corollary $4.6,|S|=|X| \bmod p$. Since $p$ does not divide $N_{p}=|X|, S$ is non-empty. Thus there exists $L \in X$ such that $\mathcal{O}_{L}=\{L\}$. It follows that $h L=L h$ for every $h \in H$, that is, $H \subseteq N(L)$. Thus $H$ and $L$ are subgroups of $N(L)$. Also, since $|N(L)|=|G| / N_{p}=p^{n} q^{\prime}$ for some divisor $q^{\prime}$ of $q, H$ and $L$ are indeed Sylow $p$-subgroups of $N(L)$. However, since $L$ is normal in $N(L)$, by the Second Sylow Theorem, there is only one Sylow $p$-subgroup of $N(L)$. Thus $H=L$. This shows that $S$ has only one element. In particular, $1=|X| \bmod p$ as desired.

A group $G$ is called simple if it has no normal subgroup.
Example 5.30 : Let $G$ be a group of order 12. The possible choices for $N_{2}$ are 1 and 3 . The possible choices for $N_{3}$ are 1 and 4 . If $N_{3}=4$ then $G$ must
have 8 elements of order 3. Indeed, any two Sylow 3 -subgroups intersects trivially in view of the Lagrange's Theorem. In case $N_{3}=4$, there can be only one Sylow 2 -group of order 4 . In any case, $G$ is not simple.

Exercise 5.31 : Show a group of order 40 has a normal, Sylow 5 -subgroup.
Example 5.32 : Consider the group $G L_{2}\left(\mathbb{Z}_{p}\right)$, where $\mathbb{Z}_{p}$ is the multiplicative group $\{0,1, \cdots, p-1\}$ with binary operation multiplication modulo $p$ for a prime number $p$. Any element in $G L_{2}\left(\mathbb{Z}_{p}\right)$ is obviously determined by 4 elements in $\mathbb{Z}_{p}$, out of which a column can be chosen in $p^{2}-1$ ways, and then the remaining column should not be a $\mathbb{Z}_{p}$-multiple of the first column chosen in $p^{2}-p$ ways. Thus $\left|G L_{2}\left(\mathbb{Z}_{p}\right)\right|=p(p-1)^{2}(p+1)$. By the Sylow Third Theorem, the number $N_{p}$ of Sylow $p$-subgroups is either 1 or $p+1$. Produce two Sylow $p$-subgroups of $G L_{2}\left(\mathbb{Z}_{p}\right)$ to conclude that $N_{p}=p+1$.

Corollary 5.33. Let $G_{p \cdot q}$ be a group of order $p q$, where $p$ and $q$ are prime numbers such that $q<p$. Then:
(1) $G_{p-q}$ has only one Sylow $p$-subgroup $H_{p}$.
(2) If $p \neq 1 \bmod q$ then $G_{p \cdot q}$ has only one Sylow $q$-subgroup $H_{q}$.
(3) If $G_{p \cdot q}$ has only one Sylow $q$-subgroup $H_{q}$ then $G_{p \cdot q}$ is cyclic.
(4) If $p \neq 1 \bmod q$ then $G_{p \cdot q}$ is cyclic.
(5) $G_{p .2}$ is either abelian or isomorphic to the dihedral group $D_{p}$.

Proof. (1) By the Third Sylow Theorem, $N_{p}$ divides $q$ and $N_{p}=1 \bmod p$. Thus $N_{p} \leq q<p$, and hence $N_{p}=1$.
(2) Again, by the Third Sylow Theorem, $N_{q}$ divides $p$ and $N_{q}=1 \bmod q$. Either $N_{q}$ is $p$ or 1 . If $p \neq 1 \bmod q$ then $N_{q}$ must be 1 .
(3) Suppose $G_{p \cdot q}$ has only one Sylow $q$-subgroup $H_{q}$. By Remark 5.27, $H_{p}$ and $H_{q}$ are normal in $G_{p \cdot q}$. Clearly, $H_{p}$ and $H_{q}$ are cyclic of order $p$ and $q$ respectively. By the Lagrange's Theorem, $H_{p} \cap H_{q}$ is trivial. Let $x$ and $y$ denote the generators of $H_{p}$ and $H_{q}$ respectively. Since $H_{p}$ is normal in $G_{p \cdot q},(x y)(y x)^{-1}=x\left(y x^{-1} y^{-1}\right) \in H_{p}$. Also, since $H_{q}$ is normal in $G_{p \cdot q}$, $(x y)(y x)^{-1}=\left(x y x^{-1}\right) y^{-1} \in H_{q}$. Since $H_{p} \cap H_{q}=\{e\}, x y=y x$. It is easy to see that the order of $x y$ is $p q$. In particular, $G_{p \cdot q}$ is a cyclic group generated by $x y$.
(4) This follows from (2) and (3).
(5) Let $x$ and $y$ denote the generators of $H_{p}$ and $H_{2}$ respectively. Thus $x^{p}=e$ and $y^{2}=e$. Since $H_{p}$ is normal, $y x y=y x y^{-1} \in H_{p}$. Thus $y x y=x^{j}$ for some $0 \leq j<p$. But then $x=y^{2} x y^{2}=y x^{j} y=x^{j^{2}}$, and hence $j^{2}=1$ $\bmod p$. The only possible choices of $j$ are $\pm 1$. If $j=1$ then $G_{p \cdot 2}$ is abelian. If $i=-1$ then the relations $x^{p}=e, y^{2}=e, y x y=x^{-1}$ determines the dihedral group $D_{p}$.

Remark 5.34 : Every group of order 15 is cyclic.

Exercise 5.35 : Consider the group $G_{7.3}$. Verify the following:
(1) $G_{7.3}$ has unique Sylow 7 -subgroup, and $G_{7.3}$ has $k$ Sylow 3-subgroups $H_{3, j}(j=1, \cdots, k)$, where possible values of $k$ are 1 and 7 .
(2) Suppose $H_{7}$ is generated by $x$ and $H_{3,1}$ is generated by $y$. There exists positive integer $i<7$ such that $y x=x^{i} y$. Further, $i$ satisfies $i^{3}=1 \bmod 7$, that is, $i=1,2,4$.
(3) Let $G_{i}$ denote the group generated by $x, y$ satisfying $x^{7}=e, y^{3}=e$, and $y x=x^{i} y$. Then $G_{1}$ is abelian and isomorphic to $H_{7} \times H_{3,1}$.
(4) Define $\phi: G_{2} \rightarrow G_{4}$ by $\phi(x)=x$ and $\phi(y)=y^{2}$. Show that $\phi$ extends to an isomorphism.
Conclude that there are two isomorphism classes of groups of order 21.
Corollary 5.36. Let $p, q$ be primes. Then every group $G$ of order $p^{2} q$ is not simple.

Proof. Let $H_{p}, H_{q}$ denote Sylow $p$-subgroup and Sylow $q$-subgroup of $G$ respectively.

Suppose $q \neq 1 \bmod p$. By the Third Sylow Theorem, $H_{p}$ is the only Sylow $p$-subgroup, and hence normal in $G$.

Suppose $p^{2} \neq 1 \bmod q$. Then $p \neq 1 \bmod q$. By similar reasoning, $H_{q}$ is a normal Sylow $q$-subgroup of $G$.

Suppose $q=1 \bmod p$ and $p^{2}=1 \bmod q$. This implies $q>p$. But then $q$ must divide $p+1$ and $p$ divides $q-1$. This is possible iff $p=2$ and $q=3$. The desired conclusion follows from Example 5.30.

Exercise 5.37 : Let $G$ be a group of order 56 and let $N_{p}$ denote the number of Sylow $p$-subgroups of $G$. Verify the following:
(1) Either $N_{7}=1$ or $N_{7}=8$.
(2) If $N_{7}=8$ then $G$ contains 48 elements of order 7 .
(3) Either $N_{7}=1$ or $N_{2}=1$.
(4) $G$ is not simple.

Exercise 5.38 : Show that a finite group with every normal and abelian Sylow subgroup is necessarily abelian.

## 6. Structure Theorem for Finite Abelian Groups

We will always assume that an abelian group $G$ carries addition as the binary operation. We say that $G$ is the direct sum $H_{1} \oplus H_{1} \oplus \cdots H_{k}$ of subgroups $H_{1}, H_{2}, \cdots, H_{k}$ of $G$ if $G=H_{1}+H_{2}+\cdots+H_{k}$ and $H_{i} \cap H_{j}=\{0\}$ for all $i \neq j$.

The most basic example of finite abelian groups is the cyclic group $C_{n}$ of order $n$. It turns out that this forms a building block in the representation theorem for abelian groups.

Exercise 6.1 : Let $m, n \in \mathbb{N}$ be coprime. Show that there exist $x, y \in C_{m n}$ of order $m$ and $n$ respectively such that $C_{m n}=\langle x\rangle \oplus\langle y\rangle$, where
$<a\rangle$ denotes the cyclic group generated by $a \in C_{m n}$. Conclude that $C_{m n}$ is isomorphic to $C_{m} \oplus C_{n}$.

Remark 6.2 : Any cyclic group is isomorphic to the direct sum of finitely many cyclic groups of prime-power order. In fact, if $m=\prod_{j=1}^{l} p_{j}^{k_{j}}$, where $p_{j}$ are distinct primes and $k_{j}$ are positive integers then $C_{m}$ is isomorphic to the direct sum $\oplus_{j=1}^{l} C_{p_{j}}$.

To understand finite abelian groups, in view of the last remark, it suffices to understand the structure of non-cyclic abelian groups.

For an $n \times n$ matrix $A$, the $i$ th row is denoted by $A_{i}$.
Exercise 6.3: For $n \geq 2$, let $a_{1}, \cdots, a_{n}$ be integers with gcd 1. For $n \geq 2$, consider the statement $P_{n}$ : Then there exists $A \in S L_{n}(\mathbb{Z})$ such that $A_{1}=$ [ $a_{1} \cdots a_{n}$ ]. Prove $P_{n}$ by induction on $n$ by verifying:
(1) $P_{2}$ holds true.
(2) Assume $P_{n-1}$. Let $d$ be the gcd of $a_{1}, \cdots, a_{n-1}$. Then there exists $B \in S L_{n-1}(\mathbb{Z})$ such that $B_{1}=\left[b_{1} \cdots b_{n-1}\right]$, where $b_{i}=a_{i} d^{-1}$.
(3) Let $B$ be as ensured by (2). Choose $s, t \in \mathbb{Z}$ such that $s a_{n}+t d=1$. Let $A$ be such that $A_{1}=\left[a_{1} \cdots a_{n}\right], A_{i}=\left[B_{i} 0\right](i=2, \cdots, n-1)$, and $A_{n}=\left[c_{1} \cdots c_{n-1} t\right]$, where $c_{i}=(-)^{n} s b_{i}$. Verify that $A \in S L_{n}(\mathbb{Z})$.

Lemma 6.4. Let $G$ be an abelian group such that $x_{1}, \cdots, x_{n} \in G$ are generators of $G$. If $X=\left[x_{1} \cdots x_{n}\right]^{t}$ and $A \in S L_{n}(\mathbb{Z})$ then the entries of $A X$ are generators of $G$. In particular, if $y_{1}=a_{1} x_{1}+\cdots+a_{n} x_{n}$, then there exist $y_{2}, \cdots, y_{n}$ such that $y_{1}, \cdots, y_{n} \in G$ are generators of $G$.
Proof. Note that if $A \in S L_{n}(\mathbb{Z})$ then $A^{-1} \in S L_{n}(\mathbb{Z})$. If $x \in G$ then there exists $k_{1}, \cdots, k_{n} \in \mathbb{Z}$ such that $x=k_{1} x_{1}+\cdots k_{n} x_{n}$. Now if $A X=Y$ then $x=k_{1}\left(A^{-1} X\right)_{1}+\cdots+k_{n}\left(A^{-1} X\right)_{n}$ is a $\mathbb{Z}$-linear combination of $y_{1}, \cdots, y_{n}$. This completes the proof of the first part. To see the remaining part, let $A \in S L_{n}(\mathbb{Z})$ with first row $\left[a_{1} \cdots a_{n}\right]$ as ensured by the last exercise, and take $y_{i}=\left(A^{-1} X\right)_{i}$ for $i=2, \cdots, n$.

The last lemma may be interpreted as:
Proposition 6.5. Let $G$ be a finitely generated abelian group. Let $\mathcal{F}=\{F$ : $F$ is a set of generators of $G\}$. Let $n=\min _{F \in \mathcal{F}}|F|$. Let $\mathcal{F}_{n}=\left\{\left[g_{1} \cdots g_{n}\right]^{T}\right.$ : $\left.\left\{g_{1}, \cdots, g_{n}\right\} \in \mathcal{F}\right\}$. Then the group $S L_{n}(\mathbb{Z})$ acts on $\mathcal{F}_{n}$ via $A * F=A F$.

Theorem 6.6. If $G$ is a finitely generated abelian group then $G$ is the direct sum of cyclic groups.

Proof. Let $\left\{x_{1}, \cdots, x_{n}\right\} \in \mathcal{F}_{n}$ be such that $x_{n}$ has the minimal order $k$, where $\mathcal{F}_{n}$ is as defined in the last remark. We prove by induction that $G=\mathbb{Z} x_{1} \oplus \cdots \oplus \mathbb{Z} x_{n}$. The case $n=1$ is trivial. Let $H$ be the proper subgroup of $G$ generated by $x_{1}, \cdots, x_{n-1}$. By the induction hypothesis, $H=$ $\mathbb{Z} x_{1} \oplus \cdots \oplus \mathbb{Z} x_{n-1}$. Thus it suffices to check that $G=H \oplus \mathbb{Z} x_{n}$.

Clearly, $G=H+\mathbb{Z} x_{n}$. Suppose $H \cap \mathbb{Z} x_{n} \neq\{0\}$. Then there there exist $a_{1}, \cdots, a_{n} \in \mathbb{Z}$ such that $a_{1} x_{1}+\cdots+a_{n-1} x_{n-1}=a_{n} x_{n} \neq 0$., In particular, $a_{n}<k$. If gcd of $a_{1}, \cdots, a_{n}$ is $d$ then $y_{1}=\frac{a_{1}}{d} x_{1}+\cdots+\frac{a_{n-1}}{d} x_{n-1}-\frac{a_{n}}{d} x_{n}$ satisfies $d y_{1}=0$. Also, by the preceding proposition, there exist $y_{2}, \cdots, y_{n} \in$ $G$ such that $\left\{y_{2}, \cdots, y_{n}, y_{1}\right\} \in \mathcal{F}_{n}$. But then the order $l$ of $y_{1}$ must be less than or equal to the order $k$ of $x_{n}$, that is $l \leq k$. Also, since $d y_{1}=0, l$ divides $d \leq a_{n}<k$. This is not possible.
Remark 6.7 : Any finite abelian group is isomorphic to the direct sum of finitely many cyclic groups of prime-power order. In particular, the abelian group of order 16, up to isomorphism, are

$$
C_{16}, C_{2} \oplus C_{8}, C_{4} \oplus C_{4}, C_{2} \oplus C_{2} \oplus C_{4}, C_{2} \oplus C_{2} \oplus C_{2} \oplus C_{2}
$$

(see Remark 6.2).
Exercise 6.8 : List all abelian groups of order 216 up to isomorphism.
Acknowledgment. I am thankful to all the students of MTH 751 for their active participation and several valuable inputs.

## References

[1] M. Artin, Algebra, Eastern Economy Edition, 1996.
[2] J. Clay, The Punctured Plane is Isomorphic to the Unit Circle, Journal of Number Theory, 1, 500-501, 1969.
[3] K. Conrad, Group Actions, available online.
[4] S. Kumaresan, Group Actions; Sylow Theorems: Expository Articles (Level 1), private communication.
[5] S. Kumaresan, Basis Theorem for Finitely Generated Abelian Groups: Expository Articles (Level 2), private communication.
[6] P. Morandi, Group Actions, available online.

