## 3.4 Lagrange's Theorem

In this section, we prove the first fundamental theorem for groups that have finite number of elements. To do so, we start with the following example to motivate our definition and the ideas that they lead to.

**Example 3.4.1.** *Consider the set* $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$*. Then* $\mathbb{R}^2$ *is an abelian group with respect to component wise addition. That is, for each* $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$*, the binary operation is defined by* $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$*. Check that if* $H$ *is a non-trivial subgroup of* $\mathbb{R}^2$ *then* $H$ *represents a line passing through* $(0, 0)$*.*

*Hence,* $H_1 = \{(x, y) \in \mathbb{R}^2 : y = 0\}$*,* $H_2 = \{(x, y) \in \mathbb{R}^2 : x = 0\}$ *and* $H_3 = \{(x, y) \in \mathbb{R}^2 : y = 3x\}$ *are subgroups of* $\mathbb{R}^2$*. Note that* $H_1$ *represents the* $X$*-axis,* $H_2$ *represents the* $Y$*-axis and* $H_3$ *represents a line passes through the origin and has slope* $3$*.*

*Fix the element* $(2, 3) \in \mathbb{R}^2$*. Then*

1. $(2, 3) + H_1 = \{(2, 3) + (x, y) : y = 0\} = \{(2 + x, 3) : x \in \mathbb{R}\}$*. This is the equation of a line that passes through the point* $(2, 3)$ *and is parallel to the* $X$*-axis.*

2. *verify that* $(2, 3) + H_2$ *represents a line that passes through the point* $(2, 3)$ *and is parallel to the* $Y$*-axis.*

3. $(2, 3) + H_3 = \{(2 + x, 3 + 3x) : x \in \mathbb{R}\} = \{(x, y) \in \mathbb{R}^2 : y = 3x - 3\}$*. So, this represents a line that has slope* $3$ *and passes through the point* $(2, 3)$*.*

*So, we see that if we fix a subgroup* $H$ *of* $\mathbb{R}^2$ *and take any point* $(x_0, y_0) \in \mathbb{R}^2$*, then the set* $(x_0, y_0) + H$ *gives a line that is a parallel shift of the line represented by* $H$ *and* $(x_0, y_0) + H$ *contains the point* $(x_0, y_0)$*. Hence, it can be easily observed that*

1. $(x_1, y_1)$ *lies on the line* $(x_0, y_0) + H$ *if and only if* $(x_0, y_0) + H = (x_1, y_1) + H$*.*

2. *for any two* $(x_0, y_0), (x_1, y_1) \in \mathbb{R}^2$*, either* $(x_0, y_0) + H = (x_1, y_1) + H$ *or they represent two parallel lines which themselves are parallel to the line represented by* $H$*.*

3. $\bigcup\limits_{x \in \mathbb{R}} \bigcup\limits_{y \in \mathbb{R}} (x, y) + H = \mathbb{R}^2$*.*

*That is, if we define a relation, denoted* $\sim$*, in* $\mathbb{R}^2$ *by* $(x_1, y_1) \sim (x_2, y_2)$*, whenever* $(x_1 - x_2, y_1 - y_2) \in H$*, then the above observations imply that this relation is an equivalence relation. Hence, as* $(x, y)$ *vary over all the points of* $\mathbb{R}^2$*, we get a partition of* $\mathbb{R}^2$*. Moreover, the equivalence class containing the point* $(x_0, y_0)$ *is the set* $(x_0, y_0) + H$*.*

Therefore, we see that given a subgroup $H$ of a group $G$, it may be possible to partition the group $G$ into subsets that are in some sense similar to $H$ itself. Example 3.4.1 also implies that for each $g \in G$, we need to consider the set $g + H$, if $G$ is an additive group or either the set $gH$ or the set $Hg$, if $G$ is a multiplicative group. So, we are led to the following definition.

**Definition 3.4.2** (Left and Right Coset). *Let $G$ be a group and let $H$ be a subgroup of $G$. Then for each $g \in G$ the set*

1. *$gH = \{gh : h \in H\}$ is called the left coset of $H$ in $G$.*

2. *$Hg = \{hg : \; h \in H\}$ is called the right coset of $H$ in $G$.*

**Remark 3.4.3.** *Since the identity element $e \in H$, for each fixed $g \in G$, $g = ge \in gH$. Hence, we often say that $gH$ is the left coset of $H$ containing $g$. Similarly, $g \in Hg$ and hence $Hg$ is said to be the right coset of $H$ containing $g$.*

**Example 3.4.4.** *Consider the group $D_4$ and let $H = \{e, f\}$ and $K = \{e, r^2\}$ be two subgroups of $D_4$. Then observe the following:*

$$\begin{aligned} H = \{e, f\} = Hf, \quad Hr = \{r, fr\} = H\,fr, & \\ H\,r^2 = \{r^2, fr^2\} = H\,fr^2 \quad \text{and} \quad H\,r^3 = \{r^3, fr^3\} = H\,fr^3. & \qquad (3.1) \\ H = \{e, f\} = fH, \quad rH = \{r, rf\} = rf\,H, & \\ r^2\,H = \{r^2, r^2 f\} = r^2 f\,H \quad \text{and} \quad r^3\,H = \{r^3, r^3 f\} = r^3 f\,H. & \qquad (3.2) \\ K = \{e, r^2\} = Kr^2 = r^2 K, \quad Kr = \{r, r^3\} = rK = Kr^3 = r^3 K & \\ Kf = \{f, r^2 f\} = fK = K\,r^2 f = r^2 f\,K \quad \text{and} & \\ K\,fr = \{fr, fr^3\} = fr\,K = K\,fr^3 = fr^3\,K. & \qquad (3.3) \end{aligned}$$

*From (3.1) and (3.2), we note that in general $Hg \neq gH$, for each $g \in D_4$, whereas from (3.3), we see that $Kg = gK$, for each $g \in D_4$. So, there should be a way to distinguish between these two subgroups of $D_4$. This leads to study of normal subgroups and beyond. The interested reader can look at any standard book in abstract algebra to go further in this direction.*

Now, let us come back to the partition of a group using its subgroup. The proof of the theorem is left as an exercise for the readers.

**Theorem 3.4.5.** *Let $H$ be a subgroup of a group $G$. Suppose $a, b \in G$. Then the following results hold for left cosets of $H$ in $G$:*

1. *$aH = H$ if and only if $a \in H$,*

2. *$aH$ is a subgroup of $G$ if and only if $a \in H$,*

3. *either $aH = bH$ or $aH \cap bH = \emptyset$,*

4. *$aH = bH$ if and only if $a^{-1}b \in H$.*

*Similarly one obtains the following results for right cosets of $H$ in $G$.*

1. *$Ha = H$ if and only if $a \in H$,*

2. *$Ha$ is a subgroup of $G$ if and only if $a \in H$,*

3. *either $Ha = Hb$ or $Ha \cap Hb = \emptyset$,*

4. *$Ha = Hb$ if and only if $ab^{-1} \in H$.*

*Furthermore, $aH = Ha$ if and only if $H = aHa^{-1} = \{aha^{-1} : h \in H\}$.*

To proceed further, we need the following definition.

**Definition 3.4.6** (Order of a Group)**.** *The number of elements in $G$, denoted $|G|$, is called the order of $G$. If $|G| < \infty$, then $G$ is called a group of finite order.*

We are now ready to prove the main result of this section, namely the Lagrange's Theorem.

**Theorem 3.4.7.** *Let $H$ be a subgroup of a finite group $G$. Then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of $H$ in $G$ equals $\dfrac{|G|}{|H|}$.*

**Proof.** We give the proof for left cosets. A similar proof holds for right cosets. Since $G$ is a finite group, the number of left cosets of $H$ in $G$ is finite. Let $g_1H, g_2H, \ldots, g_mH$ be the collection of all left cosets of $H$ in $G$. Then by Theorem 3.4.5, two cosets are either equal or they are disjoint. That is, $G$ is a disjoint union of the sets $g_1H, g_2H, \ldots, g_mH$.

Also, it can be easily verified that $|aH| = |bH|$, for each $a, b \in G$. Hence, $|g_iH| = |H|$, for all $i = 1, 2, \ldots, m$. Thus, $|G| = \left|\bigcup\limits_{i=1}^{m} g_iH\right| = \sum\limits_{i=1}^{m} |g_iH| = m|H|$ (the disjoint union gives the second equality). Thus, $|H|$ divides $|G|$ and the number of left cosets equals $m = \dfrac{|G|}{|H|}$. ■

**Remark 3.4.8.** *The number $m$ in Theorem 3.4.7 is called* the index *of $H$ in $G$, and is denoted by $[G:\ H]$ or $i_G(H)$.*

*Theorem 3.4.7 is a statement about any subgroup of a finite group. It may so happen that the group $G$ and its subgroup $H$ may have infinite number of elements but the number of left (right) cosets of $H$ in $G$ may be finite. One still talks of index of $H$ in $G$ in such cases. For example, consider $H = 10\mathbb{Z}$ as a subgroup of the additive group $\mathbb{Z}$. Then $[\mathbb{Z} :\ H] = 10$. In general, for a fixed positive integer $m$, consider the subgroup $m\mathbb{Z}$ of the additive group $\mathbb{Z}$. Then it can be easily verified that $[\mathbb{Z} :\ m\mathbb{Z}] = m$.*