Chapter 3

Groups and Polya Theory

3.1 Groups

Our aim in this chapter is to look at groups and use it to the study of questions of the type:

1. How many different necklace configurations are possible if we use 6 beads of 3 different colors? Or, for that matter what if we use n beads of m different colors?

2. How many different necklace configurations are possible if we use 12 beads among which 3 are *red*, 5 are *blue* and 4 are *green*? And a generalization of this problem.

3. Counting the number of chemical compounds which can be derived by the substitution of a given set of radicals in a given molecular structure.

It can be easily observed that if we want to look at different color configurations of a necklace formed using 6 beads, we need to understand the symmetries of a hexagon. Such a study is achieved through what in literature is called *groups*. Once we have learnt a bit about groups, we study *group action*. This study helps us in defining an equivalence relation on the set of color configurations for a given necklace. And it turns out that the number of distinct color configurations is same as the number of equivalence classes.

Before coming to the definition and its properties, let us look at the properties of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. We know that the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ satisfy the following:

Binary Operation: for every $a, b \in \mathbb{Z}$ $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$, $a + b$, called the addition of a and b, is an element of $\mathbb{Z}$ $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$;

Addition is Associative: for every $a, b, c \in \mathbb{Z}$ $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$, $(a + b) + c = a + (b + c)$;

Additive Identity: the element zero, denoted $\mathbf{0}$, is an element of $\mathbb{Z}$ $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$ and has the property that for every $a \in \mathbb{Z}$ $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$, $a + \mathbf{0} = a = \mathbf{0} + a$;

Additive Inverse: For every element $a \in \mathbb{Z}\ (\mathbb{Q}, \mathbb{R}, \mathbb{C})$, there exists an element $-a \in \mathbb{Z}\ (\mathbb{Q}, \mathbb{R}, \mathbb{C})$ such that $a + (-a) = \mathbf{0} = -a + a$;

Addition is Commutative: We also have $a + b = b + a$ for every $a, b \in \mathbb{Z}\ (\mathbb{Q}, \mathbb{R}, \mathbb{C})$.

Now, let us look at the sets $\mathbb{Z}^* = \mathbb{Z} - \{\mathbf{0}\}, \mathbb{Q}^* = \mathbb{Q} - \{\mathbf{0}\}, \mathbb{R}^* = \mathbb{R} - \{\mathbf{0}\}$ and $\mathbb{C}^* = \mathbb{C} - \{\mathbf{0}\}$. As in the previous case, we see that similar statements hold true for the sets $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$. Namely,

Binary Operation: for every $a, b \in \mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*),\ a \cdot b$, called the multiplication of a and b, is an element of $\mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*)$;

Multiplication is Associative: for every $a, b, c \in \mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*),\ \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

Multiplicative Identity: the element one, denoted $\mathbf{1}$, is an element of $\mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*)$ and for all $a \in \mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*),\ \ a \cdot \mathbf{1} = a = \mathbf{1} \cdot a$;

Multiplication is Commutative: One also has $a \cdot b = b \cdot a$ for every $a, b \in \mathbb{Z}^*\ (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*)$.

Observe that if we choose $a \in \mathbb{Z}^*$ with $a \neq 1, -1$ then there does not exist an element $b \in \mathbb{Z}^*$ such that $a \cdot b = 1 = b \cdot a$. Whereas, for the sets $\mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ one can always find a b such that $a \cdot b = 1 = b \cdot a$.

Based on the above examples, an abstract notion called *groups* is defined. Formally, one defines a group as follows.

Definition 3.1.1 (Group). *A group G, usually denoted $(G, *)$, is a non-empty set, together with a binary operation, say $*$, such that the elements of G satisfy the following:*

1. *for every $a, b, c \in G$, $\ (a * b) * c = a * (b * c)$ (*Associativity Property*) holds in G;*
2. *there is an element $\mathbf{e} \in G$ such that $a * \mathbf{e} = a = \mathbf{e} * a$, for all $a \in G$ (*Existence of Identity*);*
3. *for every element $a \in G$, there exists an element $b \in G$ such that $a * b = \mathbf{e} = b * a$ (*Existence of Inverse*).*

In addition, if the set G satisfies $a * b = b * a$, for every $a, b \in G$, then G is said to be **an abelian (commutative)** *group.*

Before proceeding with examples of groups that concerns us, we state a few basic results in group theory without proof. The readers are advised to prove it for themselves.

Remark 3.1.2. *Let $(G, *)$ be a group. Then the following hold:*

1. *The identity element of G is unique. Hence, the identity element is denoted by e.*
2. *For each fixed $a \in G$, the element $b \in G$ such that $a * b = e = b * a$ is also unique. Therefore, for each $a \in G$, the element b that satisfies $a * b = e = b * a$ is denoted by a^{-1}.*

3. *Also, for each $a \in G$, $(a^{-1})^{-1} = a$.*

4. *If $a*b = a*c$, for some $a, b, c \in G$ then $b = c$. Similarly, if $b*d = c*d$, for some $b, c, d \in G$ then $b = c$. That is, the cancelation laws in G.*

5. *For each $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

6. *By convention, we assume $a^0 = e$, for all $a \in G$.*

7. *For each $a \in G$, $(a^n)^{-1} = (a^{-1})^n$, for all $n \in \mathbb{Z}$.*

In the remaining part of this chapter, the binary operation may not be explicitly mentioned as it will be clear from the context. Now, let us now look at a few examples that will be used later in this chapter.

Example 3.1.3. Symmetric group on n letters: *Let N denote the set $\{1, 2, \ldots, n\}$. A function $f : N \longrightarrow N$ is called a permutation on n elements if f is both one-to-one and onto. Let $\mathcal{S}_n = \{f : N \longrightarrow N \mid f \text{ is one to one and onto}\}$. That is, $\mathcal{S}_n$ is the set of all permutations of the set $\{1, 2, \ldots, n\}$. Then the following can be verified:*

1. *Suppose $f, g \in \mathcal{S}_n$. Then $f : N \longrightarrow N$ and $g : N \longrightarrow N$ are two one-to-one and onto functions. Therefore, one uses the composition of functions to define the composite function $f \circ g : N \longrightarrow N$ by $(f \circ g)(x) = f\big(g(x)\big)$. Then it can be easily verified that $f \circ g$ is also one-to-one and onto. Hence $f \circ g \in \mathcal{S}_n$. That is, "composition of function", denoted $\circ$, defines a binary operation in $\mathcal{S}_n$.*

2. *It is well known that the composition of functions is an associative operation and thus $(f \circ g) \circ h = f \circ (g \circ h)$.*

3. *The function $\mathbf{e} : N \longrightarrow N$ defined by $\mathbf{e}(i) = i$, for all $i = 1, 2, \ldots, n$ is the identity function. That is, check that $f \circ \mathbf{e} = f = \mathbf{e} \circ f$, for all $f \in \mathcal{S}_n$.*

4. *Now let $f \in \mathcal{S}_n$. As $f : N \longrightarrow N$ is a one-to-one and onto function, $f^{-1} : N \longrightarrow N$ defined by $f^{-1}(i) = j$, whenever $f(j) = i$, for all $i = 1, 2, \ldots, n$, is a well defined function and is also one-to-one and onto. That is, for each $f \in \mathcal{S}_n$, $f^{-1} \in \mathcal{S}_n$ and $f \circ f^{-1} = \mathbf{e} = f^{-1} \circ f$.*

Thus $(\mathcal{S}_n, \circ)$ is a group. This group is called the Symmetric/Permutation *group on n letters. If $\sigma \in \mathcal{S}_n$ then one represents this by writing $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$. This representation of an element of $\mathcal{S}_n$ is called a* TWO ROW NOTATION. *Observe that as σ is one-to-one and onto function from N to N, it can be checked that $N = \{\sigma(1), \sigma(2), \ldots, \sigma(n)\}$. Hence, there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$ (all elements of N except $\sigma(1)$) and so on. Thus, the total number of elements in $\mathcal{S}_n$ is $n! = n(n-1) \cdots 2 \cdot 1$.*

Before discussing other examples, let us try to understand the group $\mathcal{S}_n$. As seen above, any element $\sigma \in \mathcal{S}_n$ can be represented using a two-row notation. There is another notation for permutations that is often very useful. This notation is called the *cycle notation.* Let us try to understand this notation.

Definition 3.1.4. *Let $\sigma \in \mathcal{S}_n$ and let $S = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ be distinct. If σ satisfies*

$$\sigma(i_\ell) = i_{\ell+1}, \;\; \textit{for all } \ell = 1, 2, \ldots, k-1, \;\; \sigma(i_k) = i_1 \quad \textit{and } \sigma(r) = r \;\; \textit{for } r \notin S$$

*then σ is called a k-*cycle *and is denoted by $\sigma = (i_1, i_2, \ldots i_k)$ or $(i_2, i_3, \ldots, i_k, i_1)$ and so on.*

Example 3.1.5. *1. The permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$ in cycle notation can be written as* (1234), (2341), (3412), *or* (4123) *as* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 1$ *and* $\sigma(5) = 5$.

2. *The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$ in cycle notation equals* $(123)(65)$ *as* $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$, $\sigma(4) = 4$, $\sigma(5) = 6$ *and* $\sigma(6) = 5$. *That is, this element is formed with the help of two cycles* (123) *and* (56).

3. *Consider two permutations $\sigma = (143)(27)$ and $\tau = (1357)(246)$. Then, there composition, denoted $\sigma \circ \tau$, is obtained as follows:*
$(\sigma \circ \tau)(1) = \sigma\big(\tau(1)\big) = \sigma(3) = 1$, $(\sigma \circ \tau)(2) = \sigma\big(\tau(2)\big) = \sigma(4) = 3$, $(\sigma \circ \tau)(3) = \sigma\big(\tau(3)\big) = \sigma(5) = 5$, $(\sigma \circ \tau)(4) = \sigma\big(\tau(4)\big) = \sigma(6) = 6$, $(\sigma \circ \tau)(5) = 2$, $(\sigma \circ \tau)(6) = 7$ *and* $(\sigma \circ \tau)(7) = 4$.
Hence
$$\sigma \circ \tau = (143)(27)(1357)(246) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 6 & 2 & 7 & 4 \end{pmatrix} = (235)(467).$$

4. *Similarly, verify that* $(1456)(152) = (16)(245)$.

Definition 3.1.6. *Two cycles $\sigma = (i_1, i_2, \ldots, i_t)$ and $\tau = (j_1, j_2, \ldots, j_s)$ are said to be* disjoint *if*

$$\{i_1, i_2, \ldots, i_t\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset.$$

The proof of the following theorem can be obtained from any standard book on abstract algebra.

Theorem 3.1.7. *Let $\sigma \in \mathcal{S}_n$. Then σ can be written as a product of disjoint cycles.*

Remark 3.1.8. *Observe that the representation of a permutation as a product of disjoint cycles, none of which is the identity, is unique up to the order of the disjoint cycles. The representation of an element $\sigma \in \mathcal{S}_n$ as product of disjoint cycles is called the* cyclic decomposition *of σ.*