# Symmetric Groups

Evelyn Zhu

May 2022

**Abstract**

In this paper, we explore applications, examples, and representative theories of Symmetric groups in a symmetric group. All elements are all bijections to the set itself, and the group operation is function composition. We begin by discussing the definition of symmetry with a few basic examples and applications. We then introduce and define some real-world applications followed by properties and special elements of symmetric groups. Lastly, we show the subgroup structure of symmetric groups and some of the representative theories.

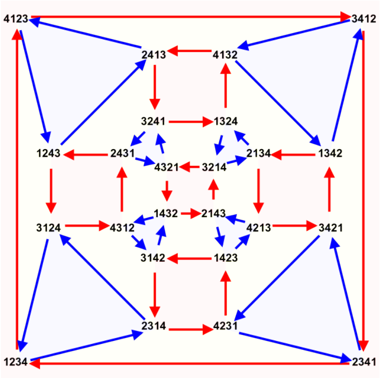


Figure 1: Example of a symmetric group

# 1 Introduction

In this paper, we start with introducing some basic properties, actions and theorems of the group.Then we will define symmetric groups in particular, providing its properties and theorems. Next, we will look into examples of symmetric groups and proofs of them. We then introduce the representative theorem - Cayley's theorem - of symmetric groups with some historical background about Arthur Cayley and the proof of his theorem.

# 2 Introduction to Groups

**Definition 2.1** (Groups)**. A group** is defined by the ordered pair $(G, \circ)$ where $G$ is a set and $\circ$ is a binary operation that maps $G \times G \to G$, satisfying the following conditions:

- *Closure:* The binary operation $\circ$ is said to be closed on set $G$ if for any elements $a, b \in G$ $a \circ b$ is also an element of $G$. Note that closure has been implied in the definition $\circ$ $G \times G \to G$, but by convention we include closure as one of the four criteria of a group.

- *Associativity:* The binary operation $\circ$ is associative such that for any elements $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.

- *Identity:* There exists a unique identity element $e \in G$ such that for all $a \in G$, $e \circ a = a = a \circ e$. The identity is often represented by $e$ or 1.

**Definition 2.2** (Group Inverse)**.** A group is a set $G$ together with a binary operation on $G$, denoted "$\cdot$", that combines any two elements $a$ and $b$ to form an element of $G$, denoted a $\cdot$ $b$.

- **Associativity** For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

- **Identity element** There exist an element $e$ in $G$ such that, for every $a$ in $G$ has $e \cdot a = a$, and $a \cdot e = a$. Such an element is called the **identity element** of group.
- **Inverse element** For each $a$ in $G$, there exists an element $b$ in $G$ such that $a \cdot b = e$ and $b \cdot a = e$, where $e$ is the **identity element**.
  For each $a$, the element $b$ is unique; it is called the **inverse** of $a$ and is commonly denoted $a^{-1}$.

**Definition 2.3** (Subgroups)**.** For a group $G$, a subset $H$ of $G$ is a **subgroup**, denoted $H \leqslant G$, if $H$ is a group under the operation of $G$. (Specifically, check that $H$ is closed under the operation and includes the identity and inverses.) $H = 1$ is the trivial subgroup and all $H \neq G$ are **proper subgroups** of $G$.

Group actions are fundamental for the group study. Every module is a special case of a set acted upon by an (abelian) group. Therefore, in general, a group action sort of encapsulates the state of a system when it is transformed with reversible transformations.

**Definition 2.4** (Group Action)**.** A group action is a representation of the elements of a group as symmetries of a set. Function $f : G \times X \to X$ satisfying the following properties:

(1) $f(e_G, x) = x$ for all x ∈ X

(2) $f(gh, x) = f(g, f(h, x))$ for all g, h ∈ G and x ∈ X. When the action is clear, the function $f(g, x)$ is often written as g $\cdot$ $x$. Therefore, (1) $e_G \cdot x = x$, (2) $g \cdot (h \cdot x) = (gh) \cdot x$.

## 2.1 Injection, Surjection, and Bijection

- A function is *injective* (*one to one*) if each possible element of the co-domain is mapped to only one element. The function $f : X \to Y$ is *injective*, if for all

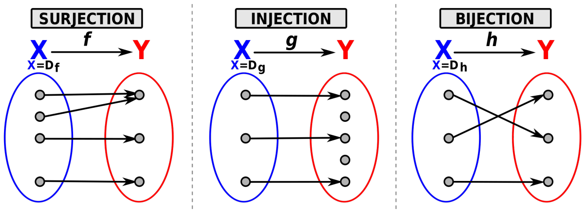


Figure 2: Figure 2: visual example of injection, surjection, and bijection

$x, x^{'} \in X, f(x) = f(x^{'}) \Rightarrow x = x^{'}$.

- A function is *surjective* (*onto*) if each element of the co-domain is mapped to by at least one element of the domain. The function $f : X \to Y$ is *surjective*, if for all $y \in Y$, there is $x \in X$ such that $f(x) = y$.
- A function is *bijective* if it is both *injective* and *surjective*. It is also called a *bijection* or a *one-to-one correspondence*. The function $f : X \to Y$ is *bijective*, if for all $y \in Y$, there is a unique $x \in X$ such that $f(x) = y$.

## 2.2 Homomorphisms and Isomorphisms

The Greek roots "homo" and "morph" mean "same shape". In Abstract Algebra, *homomorphism* is a special correspondence between elemenst of two groups. Whereas *Isomorphism* is a function that captures a one-to-one relationship between two groups. If there exists an *isomorphism* between two groups, then the groups are called *isomorphic*. An isomorphism is a special type of *homomorphism*.

**Definition 2.5.** A **homomorphism** is a function $\phi : G \to H$ between two groups satisfying $\phi(\mathrm{ab}) = \phi(\mathrm{a})\phi(\mathrm{b})$, for all a,b $\in G$.

A group **isomorphism** isomorphism is a group homomorphism which is a bijection.

**Example 2.6** (Logarithm and exponential)**.** Let $\mathbb{R}^x$ be the multiplicative group of positive real numbers, and let $\mathbb{R}$ be the additive group of real numbers. The logarithm function log : $\mathbb{R}^x \rightarrow$ satisfies that $\log(xy) = \log(x) + \log(y)$ for all $x, y \in \mathbb{R}^+$, so log is a group *homomorphism*. The exponential function exp : $\mathbb{R} \rightarrow \mathbb{R}^x$ satisfies $exp(x + y) = (expx) + (expy)$ for all $x, y \in \mathbb{R}$ so exponential function is also a *homomorphism*.Logarithm and exponential function are inverse of each other. Since log is a *homomorphism* that has an inverse ($exp$) that is also a *homomorphism*, both log and (exp) are isomorphisms between $\mathbb{R}^x$ and $\mathbb{R}$.

# 3 Introduction to Symmetric Groups

**Definition 3.1** (Symmetric group)**.**

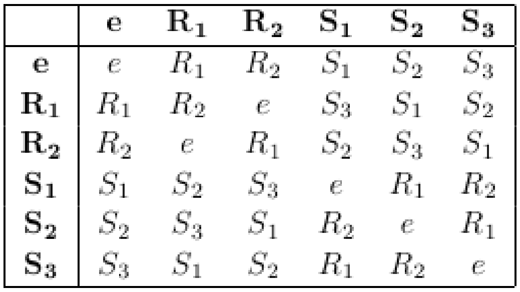
- The elements of the group are permutations on the given set (i.e., bijective maps from the set to itself).
- The product of two elements is their composite as permutations, i.e., function composition.
- The identity element of the group is the identity function from the set to itself.
- The inverse of an element in the group is its inverse as a function.

**Example 3.2.** The standard example of a group action is when $G$ equals the symmetric group $S_n$ (or a subgroup of $S_n$) and $X = 1, 2, \ldots, n$. Then G acts on X by the formula $g \cdot x = g(x)$.The properties are clear: $e \cdot x = e(x) = xe \times x = e(x) = x$ when e is the identity of $S_n$, and g $\cdot (h \cdot x) = g \cdot h(x) = g(h(x) = (g \circ h)(x)$.
For example, $D_n$ is generated y an n-cycle $\sigma$ and a 2-cycle $\tau$ satisfying the condition $\sigma^n = \tau^2 = 1, \tau\sigma^{n-1}$. For example, n=3, take $\sigma = (123)$ and $\tau = (23)$. Then $D_3 =$ id, (12), (13), (23), (123), (132). [**?**]

# 4 Theorems

## 4.1 Cayley’s theorem

Arthur Cayley was a famous British Mathematician in the 19th century. His most important work was in developing the algebra of matrices and work in non-euclidean and *n*-dimensional geometry. As early as 1849 Cayley had written a paper linking his ideas on permutations with Cauchy’s. He gives the *’Cayley tables’* of some special permutation groups but, much more significantly for the introduction of the abstract group concept, he realised that matrices and quaternions(complex number applied in mechanics to calculate the 3-D rotations) were groups. [3]



| | $\mathbf{e}$ | $\mathbf{R_1}$ | $\mathbf{R_2}$ | $\mathbf{S_1}$ | $\mathbf{S_2}$ | $\mathbf{S_3}$ |
|---|---|---|---|---|---|---|
| $\mathbf{e}$ | $e$ | $R_1$ | $R_2$ | $S_1$ | $S_2$ | $S_3$ |
| $\mathbf{R}_1$ | $R_1$ | $R_2$ | $e$ | $S_3$ | $S_1$ | $S_2$ |
| $\mathbf{R_2}$ | $R_2$ | $e$ | $R_1$ | $S_2$ | $S_3$ | $S_1$ |
| $\mathbf{S_1}$ | $S_1$ | $S_2$ | $S_3$ | $e$ | $R_1$ | $R_2$ |
| $\mathbf{S_2}$ | $S_2$ | $S_3$ | $S_1$ | $R_2$ | $e$ | $R_1$ |
| $\mathbf{S_3}$ | $S_3$ | $S_1$ | $S_2$ | $R_1$ | $R_2$ | $e$ |

Figure 3: Figure 3: Cayley’s table

**2.2.1. Cayley’s Table**

The cayley table describes the structure of a finite group by arranging all the possible products of all the group’s elements in a square table reminiscent of an addition or multiplication table.

**Theorem 4.1** (Cayley’s theorem)**.** *In group theory, Cayley states that every Group G is isomorphic to a subgroup of a symmetric group. Specifically, G is isomorphic to a subgroup of the symmetric group whose elements are the permutations of the underlying set of G. [4]*

*Proof.* Given $g \in G$, we define a map $\lambda_g$ $:G \to G$ by $\lambda$ $g(x) = gx$ for all $x \in G$. This is a well-defined mapping. Indeed, if $x = y$ then $gx = gy$ so that $\lambda$ $g(x) = \lambda$ $g(y)$. Next, we show that $\lambda_g$ is one-to-one. To see this, suppose that $\lambda_g(x) = \lambda_g(y)$. Then $gx = gy$ and by the left-cancellation property $x = y$.To see that $\lambda_g$ is onto, let $y \in G$. Then $g^{-1}y \in G$ and $\lambda_g(g^1y) = y$. Hence, $\lambda_g \in Sym(G)$. Next, We define $\Lambda : G \to Sym(G)$ by $\Lambda(g) = \lambda_g$. This is a well-defined mapping. For if $g_1 = g_2$ then $g_1x = g_2x$ for all $x \in G$, that is, $\lambda_{g1}(x) = \lambda_{g2}(x)$ for all $x \in G$ and hence $\lambda_{g1} = \lambda_{g2}$, i.e. $\lambda(g_1) = \lambda(g_2)$.

Now, given $g_1$, $g_2 \in G$ we have $\lambda_{g1}g_2(x) = (g_1g_2)x = g_1(g_2x) = \lambda_{g1}(g_2x) = \lambda_g1$ $\lambda_{g_2}(x)$ for all $x \in G$. Thus, $\Lambda(g_1g_2) = \lambda_{g1g2} = \lambda_g1$ $\lambda_g2 = \Lambda(g_1)$ $\Lambda(g_2)$, and so $\Lambda$ is a *homomorphism*. Finally, we show that $\Lambda$ is one-to-one. Indeed, if $\Lambda(g1) = \Lambda(g2)$ then $\lambda_{g1}(x) = \lambda_{g2}(x)$ for all $x \in G$. In particular, $\lambda_{g1}(e) = \lambda_{g2}(e)$. That is, $g_1e = g_2e$ or $g_1 = g_2$. Therefore, $G \approx \Lambda(G)$. □

Cayley's theorem was historically important. Cayley's theorem was initially strange but retroactively instinctive idea. It promotes symmetries of an object to the status of an object in their own, is an early example of the formal style typical of later algebra, and it helps prepare the ground psychologically for working in an abstract or axiomatized mode that was new in the 19th century.

## 5 Discussion and Application

Other than mathematical fields, group theory and symmetric groups can also be used in creating digital holograms(Image rendering, or reconstruction of object data is performed numerically from digitized interferograms, i.e. CCD camera). The problem of creating digital holograms depends on three components, namely: the image, the transform, and the hologram. Each one of these components has its own symmetry properties, which can be helpful to reduce the computational complexity. The use of group theory and image symmetry properties allow the reduction of the computational complexity in the creation of digital holograms. Therefore, the characteristics of symmetric group can also be applied in real life. [5]

## 6 Acknowledgement

I would like to thank the MIT PRIMES Circle for providing me the opportunity to deeply explore complex math topics. In particular, I would like to thank Marisa Gaetz and Mary Stelow for hosting organizing this event and making everything possible. Most of all, I would like to present my appreciation to my dearest mentor Kaili Liu for teaching, helping, and supporting me through this semester. Lastly, I want to thank my dearest friend Yiyang Feng for being my mental support. Without them, I could never achieve such accomplishments.

## References

[1] Patrick Corn and Jimin Khim. Group actions. https://brilliant.org/wiki/group-actions/.

[2] Symmetry Group is Group. https://proofwiki.org/wiki/Symmetry_Group_is_Group.

[3] J. O'Connor and E. F. Robertson. Biography of Arthur Cayley. https://mathshistory.st-andrews.ac.uk/Biographies/Cayley/.

[4] Marcel B. Finan. Cayley's Theorem. https://faculty.atu.edu/mfinan/4033/notes.htm.

[5] Application of Mathematical Symmetrical Group Theory in the Creation Process of Digital Holograms. https://www.hindawi.com/journals/mpe/2017/5612743/.