# Mälardalen University

PROJECT IN MATHEMATICS

**The Title of the Thesis**

by

*Adrian Swande*

MMA291 — Project in Mathematics

**DIVISION OF MATHEMATICS AND PHYSICS**
MÄLARDALEN UNIVERSITY
SE-721 23 VÄSTERÅS, SWEDEN

MMA291 — Project in Mathematics

*Date of presentation*:
XX June 2026

*Project name*:
The Title of the Thesis

*Author*:
Adrian Swande

*Version*: 1
22nd January 2026

*Supervisor*:
Peder Thompson

*Examiner*:
To be determined

*Comprising*:
7.5 ECTS credits

**Abstract**

Under construction.

# Acknowledgements

Under construction.

# Contents

# Chapter 1

# Introduction

# Chapter 2

# Preliminaries

## 2.1 Groups

**Definition 1** (Group)**.** In mathematics, a *group G* denotes a set of elements $\{a, b, c, \cdots\}$ and an accompanying binary operator $*$, together satisfying the following conditions:

1. *Closure*: For every ordered pair of elements in the group, the binary product thereof (as defined by the binary operator) is also an element of that group; $\forall a, b \in G$ $(a * b = c \in G)$.

2. *Associativity*: The order wherein ordered pairs of elements are evaluated has no consequence on the restulting product; $\forall a, b, c \in G$ $((a * b) * c = a * (b * c))$.

3. *Existence of Identity*: There exists in the group an *identity* element, the omission of which from any expression containing any other element or elements has no consequence on the evaluation of that expression; $\exists e \in G$ $\forall a \in G$ $(e * a = a * e = a)$.

4. *Existence of Inverse*: Each element in the group has its own *inverse*, who's product therewith evalutes to the identity; $\forall a \in G$ $\exists b \in G$ $(a * b = b * a = e)$, where $e$ is the identity.

**Definition 2** (Commutativity)**.** Let $G$ be a group. Then it is *commutative* (or *Abelian*) if $\forall a, b \in \mathbb{G}$ $(a * b = b * a)$.

The integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ together with *addition* constitutes an Abelian group with 0 acting as its identity (since $\forall a \in \mathbb{Z}$ $(0 + a = a + 0 = a)$). The negative numbers exist as the inverses of the positives, and vice versa. We know addition is associative, and since $\mathbb{Z}$ is infinite in each direction, we will never find a pair of elements therein whose sum is not also an element therein. This group can also be expressed as additively *generated* by the element 1, since 1 and its inverse $-1$ together with $+$ can express the whole group. This generative definition is denoted $G = (\langle\{1\}\rangle, +) = (\mathbb{Z}, +)$. The group generated by 2 – to give another example – is the group of all *even* integers.

**Definition 3** (Cyclicity)**.** A group which can be generated by a single element is called a *cyclic* group.

When the operator is given implicitly, a cyclic group with the generator $g$ can be written as $\langle g \rangle$.

**Definition 4** (Subgroup). Let $G$ be a group under a binary operator $*$. Then $H \subset G$ is a *subgroup* of $G$ if $H$ is also a group under $*$.

## 2.2 Permutations

**Definition 5** (Permutation). A *permutation* $\pi$ of the set $A$ is a bijective map $\pi : A \to A$.

We write $\pi^n$ for a permutation $\pi$ to denote $\pi \circ \cdots \circ \pi$ where $\pi$ is composed with itself $n \in \mathbb{N}$ times. $\pi^{-n}$ denotes the composition $\pi^{-1} \circ \cdots \circ \pi^{-1}$ where the inverse $\pi^{-1}$ is composed with itself $n \in \mathbb{N}$ times. The permutation $\pi^0$ always equals the identity.

**Definition 6** (Permutation Group). A *permutation group* on a set $A$ is a group of permutations of $A$ under composition.

**Definition 7** (Support). The *support* $\underline{\pi}$ of a permutation $\pi$ of $A$ is the set $\{a \in A \mid \pi(a) \neq a\}$.

A permutation whoose support is the empty set equals the identity. We say that a permutation $\pi$ of $A$ *fixes* an element $a \in A$ if $a \notin \underline{\pi}$.

**Definition 8** (Orbit). The *orbit* $\overset{a}{\pi}$ of an element $a \in A$ under a permutation $\pi$ of $A$ is the set $\{b \in A \mid \phi(a) = b, \phi \in \langle \pi \rangle\}$. The orbit $\overset{a}{G}$ – where $G$ is a permutation group on $A$ – is the union $\bigcup_{\pi \in G} \overset{a}{\pi}$ of the orbits of $a$ under each permutation in the group – or put differently: $\overset{a}{G} = \{\pi(a) \mid \pi \in G\}$.

Herefrom follows that $b \in \overset{a}{\pi} \Leftrightarrow a \in \overset{b}{\pi}$ and $b \in \overset{a}{G} \Leftrightarrow a \in \overset{b}{G}$.

**Definition 9** (Cycle). A *cycle* is a permutation $\pi$ such that $\forall a, b \in \underline{\pi} \; \exists \phi \in \langle \pi \rangle \, (\phi(a) = b)$.

Since the support of the identity is the empty set, the identity also a cycle.

**Definition 10** (Transposition). a *transposition* is a cycle $\pi$ where $|\underline{\pi}| = 2$.

**Theorem 1.** *Let $\pi$ be a permutation of a set $A$. Then there exists a family $(\pi_i)_{i \in I}$ of cycles on $A$ with pairwise disjoint supports such that $\forall a \in A \; \exists i \in I \, \big(a \in \underline{\pi}_i \wedge \pi_i(a) = \pi(a) \wedge \pi_j(a) = a \wedge i \neq j\big)$.*

*Proof.* Take any element $a \in A$. Define the first cycle $\pi_1$ with $\forall n \in \mathbb{Z} \, \Big(\pi_1^n(a) = \pi(a) \wedge b \notin \overset{a}{\pi_1}\Big) \Rightarrow \pi_1(b)$ Then $\underline{\pi}_1 = \overset{a}{\pi}$. Let $a_{k+1} \in A \setminus \bigcup_{i \in \{1, \cdots, k\}} \underline{\pi}_i$ where $k \in \mathbb{N}$ and each $\pi_i$ is defined in the same way as $\pi_1$ for each $a_i$. Then $\underline{\pi}_{k+1}$

$\square$

6

In *cycle notation*, the fact above is used to express permutations in a convenient way. Here, each cycle in the expressed permutation is written as a parenthesized list of elements. For example, the permutation $(a, b, c)(d, e)$ maps $a \mapsto b$, $b \mapsto c$ and $c \mapsto a$, as well as $d \mapsto e$ and $e \mapsto d$. Note that this permutation is the same as the permutation $(c, a, b)(e, d)$, but not the same as $(a, c, b)(d, e)$.

In this text, permutations containing symbols or numbers with multiple digits will be written with dividing commas, whilst permutations containing exclusively the numbers 0 through 9 will be written therewithout – for example $(1234) = (1, 2, 3, 4)$.

**Lemma 1.** *Let $\alpha$ and $\beta$ be permutations of A. Then $\alpha$ and $\beta$ do not commute if and only if there is an element $c \in \underline{\alpha} \cap \underline{\beta}$ where the cycles of $\alpha$ and $\beta$ wherein $c$ is contained are neither equal nor each other's inverses.*

*Proof.* Let $\alpha$ and $\beta$ be permutations of $A$ and $\underline{\alpha} \cap \underline{\beta} = \emptyset$. Then $\forall b \in A \; (\alpha(b) = b \vee \beta(b) = b)$. Thus for each $b \in A$ both $(\alpha \circ \beta)(b)$ and $(\beta \circ \alpha)(b)$ evaluate to the same expression, which will be either $\alpha(b)$, $\beta(b)$ or $b$. A permutation always commutes with itself, so if $\alpha_c = \beta_c$ for some $c \in \underline{\alpha} \cap \underline{\beta}$ – where $\alpha_c$ and $\beta_c$ are the cycles of $\alpha$ and $\beta$ wherein $c$ occurs – then $\alpha_c \circ \beta_c = \beta_c \circ \alpha$. If each cycle in $\alpha$ and $\beta$ commute, so do they. If $\alpha_c = \beta_c^{-1}$, then the cycles neutralize each other $\alpha_c \circ \beta_c = \beta_c \circ \alpha_c = e$. Now suppose there is an element $c \in \underline{\alpha} \cap \underline{\beta}$ such that $\alpha_c \neq \beta_c$ and $\alpha_c \neq \beta_c^{-1}$. Then from $\beta(c) \notin \underline{\alpha}$ follows $(\alpha \circ \beta)(c) = \beta(c)$ and thereof $(\beta \circ \alpha)(c) \neq \beta(c)$. If $\beta(c) \in \underline{\alpha}$, then $(\alpha \circ \beta)(c) \neq \beta(c)$

$\square$

# Chapter 3

# The Conjugates and Commutators of Permutations

Herein, all lowercase geek letters are implied to be elements in a permutation group $G$ on $A$. Elements of $A$ are represented by lowercase latin characters. Further, the operator $\circ$ will henceforth be implicit, and thus omitted from expressions. As an example, take $\pi \circ \phi = \pi\phi$.

**Definition 11** (Conjugate). The *conjugate* $\searrow_\beta^\alpha$ of $\beta$ by $\alpha$ is the composition $\alpha^{-1}\beta\alpha$.

**Definition 12** (Commutator). The *commutator* $\times_\beta^\alpha$ of $\alpha$ and $\beta$ is the composition $\beta^{-1}\alpha^{-1}\beta\alpha$.

These two constructions – though they can seem arbitrary at first – have interesting and useful properties when working within groups – specifically when the supports of their two permutations share elements.

In the trivial case where they share no element, the permutations commute, so the conjugate of $\alpha$ and $\beta$ is $\beta$, and the commutator thereof is the identity; $\alpha \cap \beta = \emptyset$ implies that $\alpha^{-1}\beta\alpha = \beta$ and $\beta^{-1}\alpha^{-1}\beta\alpha = e$.

**Lemma 2.** *Let $\underline{\alpha} \cap \underline{\beta} = \{c\}$. Then the cycle of $\searrow_\beta^\alpha$ wherein $c$ occurs has the form* $\left(\alpha^{-1}(c), \beta(c), \beta^2(c), \cdots, \beta^{-1}(c)\right)$.

*Proof.* For each $b \in \underline{\alpha} \setminus \{\alpha^{-1}(c)\}$, $\alpha(b) \notin \underline{\beta}$. Since $\beta\alpha(b) = \alpha(b)$, the conjugate can be rewritten for $b$: $\left(\alpha^{-1}\beta\alpha\right)(b) = \left(\alpha^{-1}\alpha\right)(b) = b$. In the case of $\alpha^{-1}(c)$, $\left(\alpha^{-1}\beta\alpha\alpha^{-1}\right)(c) = \left(\alpha^{-1}\beta\right)(c) = \beta(c)$, since $\beta(c) \notin \underline{\alpha} \Rightarrow \left(\alpha^{-1}\beta\right)(c) = \beta(c)$. For each $d \in \underline{\beta} \setminus \{\beta^{-1}(c), c\}$, $d, \beta(d) \notin \underline{\alpha}$, so $\left(\alpha^{-1}\beta\alpha\right)(d) = \beta(d)$. Lastly, $\beta^{-1}(c)$ maps to $\left(\alpha^{-1}\beta\alpha\beta^{-1}\right)(c) = \left(\alpha^{-1}\beta\beta^{-1}\right)(c) = \alpha^{-1}(c)$. This gives the function

$$
\searrow_\beta^\alpha (x) = \begin{cases}
x & : x \in \underline{\alpha} \setminus \{\alpha^{-1}(c)\} \\
\beta(c) & : x = \alpha^{-1}(c) \\
\beta(x) & : x \in \underline{\beta} \setminus \{\beta^{-1}(c), c\} \\
\alpha^{-1}(c) & : x = \overline{\beta}^{-1}(c)
\end{cases}
\tag{3.1}
$$

which, in cycle notation, is written $\left(\alpha^{-1}(c), \beta(c), \beta^2(c), \cdots, \beta^{-1}(c)\right) \cdots$. $\qquad\square$

Note that if $\beta$ is a transposition, then $\beta = (c, \beta(c))$ and $\beta(c) = \beta^{-1}(c)$. Thus

$$\searrow_\beta^\alpha (x) = \begin{cases} x & : x \in \underline{\alpha} \setminus \{\alpha^{-1}(c)\} \\ \beta(c) & : x = \alpha^{-1}(c) \\ \beta(x) & : x \in \emptyset \\ \alpha^{-1}(c) & : x = \beta^{-1}(c) \end{cases}$$

$$= \begin{cases} x & : x \in \underline{\alpha} \setminus \{\alpha^{-1}(c)\} \\ \beta(c) & : x = \alpha^{-1}(c) \\ \alpha^{-1}(c) & : x = \beta(c) \end{cases}$$

$$= \left(\alpha^{-1}(c), \beta(c)\right).$$

**Lemma 3.** *Let $\underline{\alpha} \cap \underline{\beta} = \{c\}$. Then $\times_\beta^{\nearrow\alpha} = (c, \beta^{-1}(c), \alpha^{-1}(c))$.*

*Proof.* Using (3.1) from the previous lemma,

$$\times_\beta^{\nearrow\alpha} (x) = \beta^{-1} \searrow_\beta^\alpha (x) = \begin{cases} \beta^{-1}(x) & : x \in \underline{\alpha} \setminus \{\alpha^{-1}(c)\} \\ \beta^{-1}\beta(c) & : x = \alpha^{-1}(c) \\ \beta^{-1}\beta(x) & : x \in \underline{\beta} \setminus \{\beta^{-1}(c), c\} \\ \beta^{-1}\alpha^{-1}(c) & : x = \beta^{-1}(c) \end{cases}$$

$$= \begin{cases} x & : x \in \underline{\alpha} \setminus \{\alpha^{-1}(c), c\} \\ \beta^{-1}(x) & : x = c \\ c & : x = \alpha^{-1}(c) \\ x & : x \in \underline{\beta} \setminus \{\beta^{-1}(c), c\} \\ \alpha^{-1}(c) & : x = \beta^{-1}(c) \end{cases}$$

$$= \begin{cases} x & : x \in (\underline{\alpha} \cup \underline{\beta}) \setminus \{\alpha^{-1}(c), \beta^{-1}(c), c\} \\ c & : x = \alpha^{-1}(c) \\ \alpha^{-1}(c) & : x = \beta^{-1}(c) \\ \beta^{-1}(c) & : x = c \end{cases}$$

$$= \left(c, \beta^{-1}(c), \alpha^{-1}(c)\right).$$

$\square$

**Lemma 4.** *Let $\alpha$ and $\beta$ where $\underline{\alpha} \cap \underline{\beta} = \{c_1, \cdots, c_n\}, n \geq 2$ and $\alpha^k(c_1) = \beta^k(c_1)$ for all $k \in \{0, \cdots, n-1\}$. Then $\searrow_\beta^\alpha = ()$.*

*Proof.* Let $b \in \underline{\alpha} \setminus \{\alpha^{-1}(c_1), c_1, \cdots, c_{n-1}\}$, then the conjugation fixes $b$. Note that if $\alpha$ and $\beta$ only share two elements, then $c_1 = c_{n-1}$. $c_{n-1}$ maps to $\beta(c_n)$ and $\forall i \in \{1, \cdots, n-2\}$ $(c_i \mapsto c_{i+1})$ given that $n \geq 3$. Each $g \in \underline{\beta} \setminus \{\beta^{-1}(c_1), c_1, \cdots, c_n\}$ map to $\beta(g)$. Lastly, $\alpha^{-1}(c_1) \mapsto c_1$ and

9

$\beta^{-1}(c_1) \mapsto \alpha^{-1}(c_1)$. This yields the function

$$\searrow_\beta^\alpha (x) = \begin{cases} x & : x \in \underline{\alpha} \setminus \left\{\alpha^{-1}(c_1), c_1, \cdots, c_{n-1}\right\} \\ c_1 & : x = \alpha^{-1}(c_1) \\ c_{i+1} & : i \in \{1, \cdots, n-2\} \wedge n \geq 3 \\ \beta(c_n) & : x = c_{n-1} \\ \beta(x) & : x \in \underline{\beta} \setminus \left\{\beta^{-1}(c_1), c_1, \cdots, c_n\right\} \\ \alpha^{-1}(c_1) & : x = \overline{\beta}^{-1}(c_1) \end{cases} \tag{3.2}$$

$$= \left(\alpha^{-1}(c_1), c_1, \cdots, c_{n-1}, \beta(c_n), \cdots, \beta^{-1}(c_1)\right). \tag{3.3}$$

$\square$

**Lemma 5.** *Let $\alpha$ and $\beta$ where $\underline{\alpha} \cap \underline{\beta} = \{c_1, \cdots, c_n\}$, $n \geq 2$ and $\alpha^{k-1}(c_1) = \beta^{k-1}(c_1)$ for all $k \in \{1, \cdots, n\}$. Then $\diagdown\!\diagup_\beta^\alpha = \left(\alpha^{-1}(c), \beta^{-1}(c)\right)(c_{n-1}, c_n)$.*

*Proof.*

$$\delta(x) = \beta^{-1}\gamma(x) = \begin{cases} x & : x \in (\underline{\alpha} \cup \underline{\beta}) \setminus \left\{\alpha^{-1}(c), \beta^{-1}(c), c_{n-1}, c_n\right\} \\ \beta^{-1}(c) & : x = \alpha^{-1}(c) \\ \alpha^{-1}(c) & : x = \beta^{-1}(c) \\ c_n & : x = c_{n-1} \\ c_{n-1} & : x = c_n \end{cases} \tag{3.4}$$

$\square$

# Chapter 4

# The $2 \times 3$ **Game**

The "$2 \times 3$ game" is a simple puzzle with six tiles in a grid of numbers and a set of allowed moves which permute them. The goal of the game is to sort the grid into a "solved" state from some scrambled state.

$$\begin{array}{|ccc|}\hline 5 & 4 & 2 \\ 3 & 6 & 1 \\\hline\end{array} \xrightarrow{\text{Move}_1} \cdots \xrightarrow{\text{Move}_n} \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 4 & 5 & 6 \\\hline\end{array}$$

Formally, the game can be and will be hereafter modelled as follows. Let $G := (\langle \mathfrak{M} \rangle, \circ)$ be a group compositionally generated by the set of moves $\mathfrak{M} := \{(123), (456), (14)\}$, named $U = (123)$ for *upper row*, $L = (456)$ for *lower row* and $S = (14)$ for *side flip*. A *problem* is a permutation $p \in G$, and a *solution* thereto is a vector $\mathbf{s} \in \mathfrak{M}^*$ such that

$$\bigcirc_{i=n}^{1} \mathbf{s}_i = \mathbf{s}_n \circ \mathbf{s}_{n-1} \circ \cdots \circ \mathbf{s}_1 = p$$

where $n$ denotes the length of $\mathbf{s}$. Note that $\mathbf{s}$ may include the implicitly given inverses of the group generators. Hereafter, $\bigcirc_{i=n}^{1} \mathbf{s}_i$ will be written as $\acute{\mathbf{s}}$.
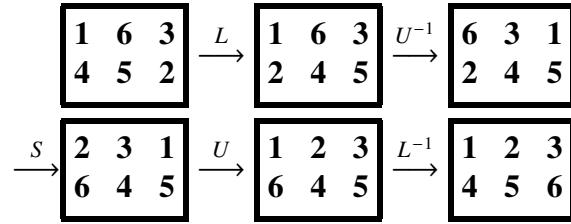
The size of the group $|G|$ is 720, which shows that $G = S_6$, since $|S_6| = 720$. This fact can also be proven in the following way. Each transposition beteen the upper and lower row can be found with the nested conjugate

$$T_1(x, y) = \left(L^{-y+3+1}\right)^{-1} \left(\left(U^{-x+1}\right)^{-1} (S) \left(U^{-x+1}\right)\right) \left(L^{-y+3+1}\right)$$
$$= L^{y-4} U^{x-1} S U^{-x+1} L^{-y+4}$$
$$= L^{y-1} U^{x-1} S U^{-x+1} L^{-y+1},$$

where $x \in \{1, 2, 3\}$ and $y \in \{4, 5, 6\}$. As an example, let $p = (26)$. Then

$$
\begin{aligned}
T_1(2, 6) &= L^{6-1}U^{2-1}SU^{-2+1}L^{-6+1} \\
&= L^5 U^1 S U^{-1} L^{-5} \\
&= (456)^5 (123)^1 (14)(123)^{-1}(456)^{-5} \\
&= (465)(123)(14)(132)(456) \\
&= (465)(24)(456) \\
&= (2, 6).
\end{aligned}
$$

This gives – after some reductions – the solution $\mathbf{s} = \left(L, U^{-1}, S, U, L^{-1}\right)$ visualized below.

$$
\begin{array}{c}
\boxed{\begin{array}{ccc} 1 & 6 & 3 \\ 4 & 5 & 2 \end{array}} \xrightarrow{L} \boxed{\begin{array}{ccc} 1 & 6 & 3 \\ 2 & 4 & 5 \end{array}} \xrightarrow{U^{-1}} \boxed{\begin{array}{ccc} 6 & 3 & 1 \\ 2 & 4 & 5 \end{array}} \\[2em]
\xrightarrow{S} \boxed{\begin{array}{ccc} 2 & 3 & 1 \\ 6 & 4 & 5 \end{array}} \xrightarrow{U} \boxed{\begin{array}{ccc} 1 & 2 & 3 \\ 6 & 4 & 5 \end{array}} \xrightarrow{L^{-1}} \boxed{\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \end{array}}
\end{array}
$$
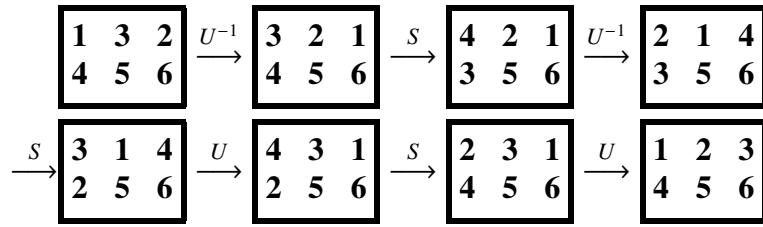
Each transposition beteen elements on the same row can be found with the nested conjugate

$$
\begin{aligned}
T_2(x, y, R) &= \left( (R^{-x+1})^{-1}(S)(R^{-x+1}) \right)^{-1} \left( (R^{-y+1})^{-1}(S)(R^{-y+1}) \right) \left( (R^{-x+1})^{-1}(S)(R^{-x+1}) \right) \\
&= (R^{x-1}SR^{-x+1})^{-1}(R^{y-1}SR^{-y+1})(R^{x-1}SR^{-x+1}) \\
&= (R^{-(-x+1)}S^{-1}R^{-(x-1)})(R^{y-1}SR^{-y+1})(R^{x-1}SR^{-x+1}) \\
&= (R^{x-1}SR^{-x+1})(R^{y-1}SR^{-y+1})(R^{x-1}SR^{-x+1}) \\
&= R^{x-1}SR^{-x+1}R^{y-1}SR^{-y+1}R^{x-1}SR^{-x+1} \\
&= R^{x-1}SR^{-x+y}SR^{x-y}SR^{-x+1}
\end{aligned}
$$

where $x, y \in R$ and $R \in \mathfrak{M} \setminus \{S\}$. As an example, let $p = (23)$. Since 2 and 3 belong to the upper row, $R$ is set to $U$:

$$
\begin{aligned}
T_2(2, 3, U) &= U^{2-1}SU^{-2+3}SU^{2-3}SU^{-2+1} \\
&= U^1 S U^1 S U^{-1} S U^{-1} \\
&= (123)(14)(123)(14)(123)^{-1}(14)(123)^{-1} \\
&= (123)(14)(123)(14)(132)(14)(132) \\
&= (123)(14)(24)(14)(132) \\
&= (123)(12)(132) \\
&= (23).
\end{aligned}
$$

This gives the solution $\mathbf{s} = \left(U^{-1}, S, U^{-1}, S, U, S, U\right)$ visualized below.

$$\begin{array}{ccc} 1 & 3 & 2 \\ 4 & 5 & 6 \end{array} \xrightarrow{U^{-1}} \begin{array}{ccc} 3 & 2 & 1 \\ 4 & 5 & 6 \end{array} \xrightarrow{S} \begin{array}{ccc} 4 & 2 & 1 \\ 3 & 5 & 6 \end{array} \xrightarrow{U^{-1}} \begin{array}{ccc} 2 & 1 & 4 \\ 3 & 5 & 6 \end{array}$$

$$\xrightarrow{S} \begin{array}{ccc} 3 & 1 & 4 \\ 2 & 5 & 6 \end{array} \xrightarrow{U} \begin{array}{ccc} 4 & 3 & 1 \\ 2 & 5 & 6 \end{array} \xrightarrow{S} \begin{array}{ccc} 2 & 3 & 1 \\ 4 & 5 & 6 \end{array} \xrightarrow{U} \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \end{array}$$

Since a transposition of any two elements herein can be composed using the generators in $\mathfrak{M}$ – in other words, since the group $G$ includes every transposition of the elements 1 through 6 – it follows that the group must include every permutation on the six elements, and thereby equal $S_6$.