Advances in Pure Mathematics, 2021, 11, 816-834
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A Minimal Presentation of a Two-Generator Permutation Group on the Set of Integers

Simon Aloff[1]*, Michael Miniere[1], John T. Saccoman[2]

[1]Middlesex College, Edison, NJ, USA
[2]Seton Hall University, South Orange, NJ, USA
Email: *saloff@middlesexcc.edu

How to cite this paper: Aloff, S., Miniere, M. and Saccoman, J.T. (2021) A Minimal Presentation of a Two-Generator Permutation Group on the Set of Integers. *Advances in Pure Mathematics*, **11**, 816-834.
https://doi.org/10.4236/apm.2021.1110055

Received: September 20, 2021
Accepted: October 26, 2021
Published: October 29, 2021

Abstract

In this paper, we investigate the algebraic structure of certain 2-generator groups of permutations of the integers. The groups fall into two infinite classes: one class terminates with the quaternion group and the other class terminates with the Klein-four group. We show that all the groups are finitely presented and we determine minimal presentations in each case. Finally, we determine the order of each group.

Keywords

Permutation Groups, Combinatorial Group Theory, Presentation of Groups

1. Introduction

We determine finite minimal presentations for certain 2-generator groups of permutations of the integers. Much of the work contained herein appeared in [1]. For further results in this area, we recommend [2] and [3]. For all algebra definitions and terminology not found in this paper, we refer the reader to [4], and for more background on permutation groups, we refer the reader to [5].

First, we introduce some notation that we will follow in this paper. We will denote by $\mathbb{Z}^+$ and $\mathbb{Z}^-$ two separate copies of the integers, *i.e.*, $\mathbb{Z}^+=\{\cdots,-3^+,-2^+,-1^+,0^+,1^+,2^+,3^+,\cdots\}$, $\mathbb{Z}^-=\{\cdots,-3^-,-2^-,-1^-,0^-,1^-,2^-,3^-,\cdots\}$, and let $S=\mathbb{Z}^+\cup\mathbb{Z}^-$. We denote by Σ the group of all one-to-one mappings of S onto itself. We will refer to Σ as the *infinite symmetric group*, and its elements will be called permutations of S. This paper will, for the most part, deal with the combinatorial group theory aspects of the permutation group G generated by σ and τ. In our notation, $\sigma\tau$ denotes τ followed by σ. The permutations $\sigma,\tau\in\Sigma$ that are the focus of this work are defined as follows:

- $\sigma(x^+) = (x-1)^+$
- $\sigma(x^-) = (x+1)^-$
- $\tau(x^-) = x^+$
- $\tau(x^+) = \begin{cases} (x+2)^- & x \equiv 0 \pmod 2 \\ (x-2)^- & x \equiv 1 \pmod 2 \end{cases}$

We illustrate σ and τ in **Figure 1**.

We state a few pertinent definitions.

Definition 1.1 *Let* $\tilde{G}$ *be an arbitrary group.*

1) A group $\tilde{G}$ is finitely generated by elements $g_1, g_2, \cdots, g_j \in \tilde{G}$ if each $x \in \tilde{G}$ has a representation $x = x_1 x_2 \cdots x_n$ with each $x_i \in \{g_1, g_1^{-1}, g_2, g_2^{-1}, \cdots, g_j, g_j^{-1}\}$. For the following definitions, we assume that $\tilde{G}$ has a specified set of generators $g_1, g_2, \cdots, g_j$.

2) A word in $\tilde{G}$ is a sequence $x_1, x_2, \cdots, x_n$ with each $x_i \in \{g_1, g_1^{-1}, g_2, g_2^{-1}, \cdots, g_j, g_j^{-1}\}$. The word $w = x_1, x_2, \cdots, x_n$ represents the element $x_1 x_2 \cdots x_n \in \tilde{G}$, so we will write $w = x_1 x_2 \cdots x_n$. We will allow the empty word (no symbols) which represents the identity in $\tilde{G}$.

3) If $w = x_1 x_2 \cdots x_n$ is a word, then $w^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1}$.

4) A relator is a word that represents the identity. A trivial relator is a word $w = xx^{-1}$ with *x* a word. The set of relators is denoted $R(\tilde{G})$.

5) Two words are equivalent if one can be transformed into the other in a finite number of steps by inserting or deleting a trivial relator at an arbitrary location during each step. This is a valid equivalence relation on the set of words. Hereafter, a word will mean the equivalence class of the word.

6) If x, y are words, then $x^{-1}yx$ is a conjugate of *y*. The conjugate of a relator is itself a relator, and a finite product of relators is also a relator.

7) A relator z can be inserted into a word $\omega_1 = AB$ (with A, B words) to obtain a new word $\omega_2 = AzB$ by multiplying ω_1 on the right by $B^{-1}zB$, *i.e.*, $\omega_1 = AB \to AB(B^{-1}zB) = AzB = \omega_2$.

8) If $\omega_1, \omega_2, \cdots, \omega_n$ are words, then $N(\omega_1, \omega_2, \cdots, \omega_n)$ is the set of words that are the finite products of the conjugates of $\omega_1, \omega_1^{-1}, \omega_2, \omega_2^{-1}, \cdots, \omega_n, \omega_n^{-1}$. If each $\omega_i \in R(\tilde{G})$, then $N(\omega_1, \omega_2, \cdots, \omega_n) \subset R(\tilde{G})$.

9) $\tilde{G}$ is finitely presented if there is a finite set of relators $\{z_1, z_2, \cdots, z_n\}$ such that $R(\tilde{G}) = N(z_1, z_2, \cdots, z_n)$. The presentation $\{z_1, z_2, \cdots, z_n\}$ is minimal if $R(\tilde{G}) \neq N(z_1, z_2, \cdots, z_{i-1}, z_{i+1}, \cdots, z_n)$ for $i = 1, 2, \cdots, n$.

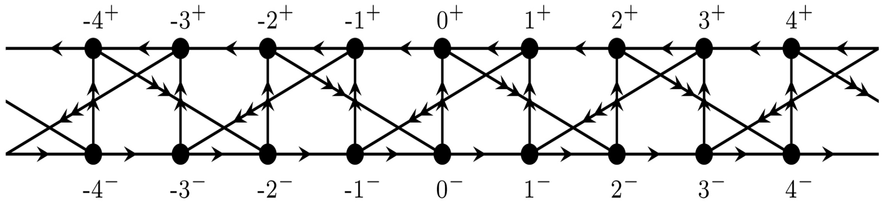

Figure 1. The permutation σ is represented by the single arrow, and τ is represented by the double arrow.

2. Main Results

2.1. Properties of τ and σ

Theorems 2.1 and 2.2 demonstrate how the application of τ and σ to integers impacts the resulting parities.

Theorem 2.1 *The permutations* τ *and* σ *satisfy the following properties*:

1) If $x \equiv 0 \pmod 2$, then

- $\tau^2(x^+) = (x+2)^+$, and $\tau^{-2}(x^+) = (x-2)^+$
- $\tau^2(x^-) = (x+2)^-$, and $\tau^{-2}(x^-) = (x-2)^-$
- $(\tau\sigma)^2(x^+) = (x-2)^+$, and $(\tau\sigma)^{-2}(x^+) = (x+2)^+$
- $(\tau\sigma)^2(x^-) = (x+2)^-$, and $(\tau\sigma)^{-2}(x^-) = (x-2)^-$

2) If $x \equiv 1 \pmod 2$, then

$\tau^2(x^+) = (x-2)^+$, and $\tau^{-2}(x^+) = (x+2)^+$

- $\tau^2(x^-) = (x-2)^-$, and $\tau^{-2}(x^-) = (x+2)^-$
- $(\tau\sigma)^2(x^+) = (x+2)^+$, and $(\tau\sigma)^{-2}(x^-) = (x-2)^+$
- $(\tau\sigma)^2(x^-) = (x-2)^-$, and $(\tau\sigma)^{-2}(x^+) = (x+2)^-$.

Proof: (1.) Suppose $x \equiv 0 \pmod 2$. We prove the first formula:

- $\tau^2(x^+) = \tau((x+2)^-) = (x+2)^+$,
- $\tau^2(x^-) = \tau(x^+) = (x+2)^-$,
- $\tau\sigma\tau\sigma(x^+) = \tau\sigma\tau((x-1)^+) = \tau\sigma((x-3)^-) = \tau((x-2)^-) = (x-2)^+$,
- $\tau\sigma\tau\sigma(x^-) = \tau\sigma\tau((x+1)^-) = \tau\sigma((x+1)^+) = \tau(x^+) = (x+2)^-$.

To determine inverses, note that τ^2 and $(\tau\sigma)^2$ preserve both sign parity (*i.e.*, +, −) and even/odd parity. If $\tau^{-2}(x^+) = y^+$, then $x^+ = \tau^2(y^+) = (y+2)^+$, so $y = x-2$, and thus, $\tau^{-2}(x^+) = (x-2)^+$. The proofs of the other formulas are similar. (2.) Suppose $x \equiv 1 \pmod 2$. We prove the first formula:

- $\tau^2(x^+) = \tau((x-2)^-) = (x-2)^+$,
- $\tau^2(x^-) = \tau(x^+) = (x-2)^-$,
- $\tau\sigma\tau\sigma(x^+) = \tau\sigma\tau((x-1)^+) = \tau\sigma((x+1)^-) = \tau((x+2)^-) = (x+2)^+$,
- $\tau\sigma\tau\sigma(x^-) = \tau\sigma\tau((x+1)^-) = \tau\sigma((x+1)^+) = \tau(x^+) = (x-2)^-$.

The inverse properties follow as in part (1.), and the other formulas follow similarly. ■

The next theorem generalizes Theorem 2.1.

Theorem 2.2 *Let* $a,b,c \in \mathbb{Z}$ *and* $x \in 2\mathbb{Z}$.

1).

- $(\tau\sigma)^a(x^+) = \begin{cases} (x-a)^+, & a \equiv 0 \pmod 2 \\ (x-a-2)^-, & a \equiv 1 \pmod 2 \end{cases}$
- $(\tau\sigma)^a((x+1)^+) = \begin{cases} (x+1+a)^+, & a \equiv 0 \pmod 2 \\ (x+1+a)^-, & a \equiv 1 \pmod 2 \end{cases}$
- $(\tau\sigma)^a(x^-) = \begin{cases} (x+a)^-, & a \equiv 0 \pmod 2 \\ (x+a)^+, & a \equiv 1 \pmod 2 \end{cases}$

- $(\tau\sigma)^a\left((x+1)^-\right)=\begin{cases}(x+1-a)^-, & a\equiv 0(\bmod 2)\\ (x+3-a)^+, & a\equiv 1(\bmod 2)\end{cases}$

2).

- $\sigma^b\tau^c\left(x^+\right)=\begin{cases}(x-b+c)^+, & c\equiv 0(\bmod 2)\\ (x+1+b+c)^-, & c\equiv 1(\bmod 2)\end{cases}$
- $\sigma^b\tau^c\left((x+1)^+\right)=\begin{cases}(x+1-b-c)^+, & c\equiv 0(\bmod 2)\\ (x+b-c)^-, & c\equiv 1(\bmod 2)\end{cases}$
- $\sigma^b\tau^c\left(x^-\right)=\begin{cases}(x+b+c)^-, & c\equiv 0(\bmod 2)\\ (x-b+c-1)^+, & c\equiv 1(\bmod 2)\end{cases}$
- $\sigma^b\tau^c\left((x+1)^-\right)=\begin{cases}(x+1+b-c)^-, & c\equiv 0(\bmod 2)\\ (x-b-c+2)^+, & c\equiv 1(\bmod 2)\end{cases}$

Proof:

1) First, suppose $a\equiv 0(\bmod 2)$, so $a=2k$. By Theorem 2.1,

- $(\tau\sigma)^a\left(x^+\right)=\left[(\tau\sigma)^2\right]^k\left(x^+\right)=(x-2k)^+=(x-a)^+$
- $(\tau\sigma)^a\left(x^-\right)=\left[(\tau\sigma)^2\right]^k\left(x^-\right)=(x+2k)^-=(x+a)^-$
- $(\tau\sigma)^a\left((x+1)^+\right)=\left[(\tau\sigma)^2\right]^k\left((x+1)^+\right)=(x+1+2k)^+=(x+1+a)^+$
- $(\tau\sigma)^a\left((x+1)^-\right)=\left[(\tau\sigma)^2\right]^k\left((x+1)^-\right)=(x+1-2k)^-=(x+1-a)^-$

Now suppose $a\equiv 1(\bmod 2)$, so $a=2k+1$. Then

- $(\tau\sigma)^a\left(x^+\right)=(\tau\sigma)(\tau\sigma)^{2k}\left(x^+\right)=(\tau\sigma)\left((x-2k)^+\right)=(x-2k-3)^-=(x-a-2)^-$
- $(\tau\sigma)^a\left(x^-\right)=(\tau\sigma)(\tau\sigma)^{2k}\left(x^-\right)=(\tau\sigma)\left((x+2k)^-\right)=(x+2k+1)^+=(x+a)^+$
- $$(\tau\sigma)^a\left((x+1)^+\right)=(\tau\sigma)(\tau\sigma)^{2k}\left((x+1)^+\right)=(\tau\sigma)\left((x+1+2k)^+\right)$$ $$=(x+2k+2)^-=(x+1+a)^-$$
- $$(\tau\sigma)^a\left((x+1)^-\right)=(\tau\sigma)(\tau\sigma)^{2k}\left((x+1)^-\right)=(\tau\sigma)\left((x+1-2k)^-\right)$$ $$=(x+2-2k)^+=(x+3-a)^+$$

2) Suppose $c\equiv 0(\bmod 2)$, so $c=2k$. Then

- $\sigma^b\tau^c\left(x^+\right)=\sigma^b\left(\tau^2\right)^k\left(x^+\right)=\sigma^b\left((x+2k)^+\right)=(x+2k-b)^+=(x-b+c)^+$
- $\sigma^b\tau^c\left(x^-\right)=\sigma^b\left(\tau^2\right)^k\left(x^-\right)=\sigma^b\left((x+2k)^-\right)=(x+2k+b)^-=(x+b+c)^-$
- $$\sigma^b\tau^c\left((x+1)^+\right)=\sigma^b\left(\tau^2\right)^k\left((x+1)^+\right)=\sigma^b\left((x+1-2k)^+\right)$$ $$=(x+1-b-2k)^+=(x+1-b-c)^+$$
- $$\sigma^b\tau^c\left((x+1)^-\right)=\sigma^b\left(\tau^2\right)^k\left((x+1)^-\right)=\sigma^b\left((x+1-2k)^-\right)$$ $$=(x+1+b-2k)^-=(x+1+b-c)^-.$$

Also, if $c\equiv 1(\bmod 2)$, so $c=2k+1$, then

- $$\sigma^b\tau^c\left(x^+\right)=\sigma^b\tau\tau^{2k}\left(x^+\right)=\sigma^b\tau\left(\left(x+2k\right)^+\right)=\sigma^b\left(\left(x+2k+2\right)^-\right)$$ $$=\left(x+2k+2+b\right)^-=\left(x+b+c+1\right)^-$$
- $$\sigma^b\tau^c\left(x^-\right)=\sigma^b\tau\tau^{2k}\left(x^-\right)=\sigma^b\tau\left(\left(x+2k\right)^-\right)=\sigma^b\left(\left(x+2k\right)^+\right)$$ $$=\left(x+2k-b\right)^+=\left(x-b+c-1\right)^+$$
- $$\sigma^b\tau^c\left(\left(x+1\right)^+\right)=\sigma^b\tau\tau^{2k}\left(\left(x+1\right)^+\right)=\sigma^b\tau\left(\left(x+1-2k\right)^+\right)$$ $$=\sigma^b\left(\left(x-1-2k\right)^-\right)=\left(x+b-1-2k\right)^-=\left(x+b-c\right)^-$$
- $$\sigma^b\tau^c\left(\left(x+1\right)^-\right)=\sigma^b\tau\tau^{2k}\left(\left(x+1\right)^-\right)=\sigma^b\tau\left(\left(x+1-2k\right)^-\right)$$ $$=\sigma^b\left(\left(x+1-2k\right)^+\right)=\left(x+1-2k-b\right)^+=\left(x-b-c+2\right)^+.$$ ■

We can use Theorem 2.2 to prove a uniqueness of representation theorem for the permutations σ,τ.

Theorem 2.3 *Let* $a,b,c\in\mathbb{Z}$ *and* $a\geq 0$. *Suppose* $(\tau\sigma)^a=\sigma^b\tau^c$. *Then* $a=b=c=0$.

Proof. If $(\tau\sigma)^a=\sigma^b\tau^c$, then their images agree on all values in *S*. In particular, on $0^+,1^+,0^-$ and 1^-. There are two cases:

1) First suppose $a\equiv 0(\bmod 2)$. Then we must have $c\equiv 0(\bmod 2)$ in order to preserve sign parity. We substitute the values $0^+,1^+,0^-$ and 1^- into the equation $(\tau\sigma)^a=\sigma^b\tau^c$ and use Theorem 2.2. This yields

- At 0^+, have $-a=-b+c$.
- At 1^+, have $a+1=-b-c+1$.
- At 0^-, have $a=b+c$.
- At 1^-, have $-a+1=b-c+1$.

These equations imply that $a=b=c=0$.

2) Now suppose that $a\equiv 1(\bmod 2)$, and again substitute the values $0^+,1^+,0^-$ and 1^-, respectively. Now,

- At 0^+, have $-a-2=b+c+1$.
- At 1^+, have $a+1=b-c$.
- At 0^-, have $a=-b+c-1$.
- At 1^-, have $-a+3=-b-c+2$.

These equations imply that $a=b=c=-1$. Since we assumed $a\geq 0$, this is impossible, so the desired result follows. ■

Now we return to the group G generated by the permutations σ,τ,σ^{-1} and τ^{-1}. We will show that G is finitely presented and determine a minimal presentation.

Theorem 2.4 *The following words are in* $R(G)$.

- $\omega_1=\tau^{-1}\sigma^2\tau\sigma^2$
- $\omega_2=\sigma^{-1}\tau^2\sigma\tau^2$
- $\omega_3=\sigma^2\omega_1^{-1}\sigma^{-2}=\tau^{-1}\sigma^{-2}\tau\sigma^{-2}$
- $\omega_4=\sigma^{-2}\tau\omega_1\tau^{-1}\sigma^2=\tau\sigma^2\tau^{-1}\sigma^2$
- $\omega_5=\tau\omega_1^{-1}\tau^{-1}=\tau\sigma^{-2}\tau^{-1}\sigma^{-2}$
- $\omega_6=\sigma\omega_2\sigma^{-1}=\tau^2\sigma\tau^2\sigma^{-1}$

- $\omega_7 = \tau^2\omega_2\tau^{-2} = \tau^2\sigma^{-1}\tau^2\sigma$
- $\omega_8 = \tau^{-2}\sigma\omega_2^{-1}\sigma^{-1}\tau^2 = \tau^{-2}\sigma\tau^{-2}\sigma^{-1}$

Then $N(\omega_1,\omega_2) = R(G)$, and $\{\omega_1,\omega_2\}$ is a finite presentation for *G*.

Proof. We will prove this theorem by demonstrating containment in both directions. To show $N(\omega_1,\omega_2) \subseteq R(G)$, we first show that ω_1 and ω_2 are in $R(G)$. If $x \equiv 0 (\text{mod}\, 2)$, then

- $\omega_1(x^+) = \tau^{-1}\sigma^2\tau\sigma^2(x^+) = \tau^{-1}\sigma^2\tau((x-2)^+) = \tau^{-1}\sigma^2(x^-) = \tau^{-1}((x+2)^-) = x^+$
- $\omega_2(x^+) = \sigma^{-1}\tau^2\sigma\tau^2(x^+) = \sigma^{-1}\tau^2\sigma((x+2)^+) = \sigma^{-1}\tau^2((x+1)^+)$ $= \sigma^{-1}((x-1)^+) = x^+$
- $\omega_1(x^-) = \tau^{-1}\sigma^2\tau\sigma^2(x^-) = \tau^{-1}\sigma^2\tau((x+2)^-) = \tau^{-1}\sigma^2((x+2)^+)$ $= \tau^{-1}(x^+) = x^-$
- $\omega_2(x^-) = \sigma^{-1}\tau^2\sigma\tau^2(x^-) = \sigma^{-1}\tau^2\sigma((x+2)^-) = \sigma^{-1}\tau^2((x+3)^-)$ $= \sigma^{-1}((x+1)^-) = x^-$

If $x \equiv 1 (\text{mod}\, 2)$, then

- $\omega_1(x^+) = \tau^{-1}\sigma^2\tau\sigma^2(x^+) = \tau^{-1}\sigma^2\tau((x-2)^+) = \tau^{-1}\sigma^2((x-4)^-)$ $= \tau^{-1}((x-2)^-) = x^+$
- $\omega_2(x^+) = \sigma^{-1}\tau^2\sigma\tau^2(x^+) = \sigma^{-1}\tau^2\sigma((x-2)^+) = \sigma^{-1}\tau^2((x-3)^+)$ $= \sigma^{-1}((x-1)^+) = x^+$
- $\omega_1(x^-) = \tau^{-1}\sigma^2\tau\sigma^2(x^-) = \tau^{-1}\sigma^2\tau((x+2)^-) = \tau^{-1}\sigma^2((x+2)^+)$ $= \tau^{-1}(x^+) = x^-$
- $\omega_2(x^-) = \sigma^{-1}\tau^2\sigma\tau^2(x^-) = \sigma^{-1}\tau^2\sigma((x-2)^-) = \sigma^{-1}\tau^2((x-1)^-)$ $= \sigma^{-1}((x+1)^-) = x^-$

Since the conjugate of an element in $R(G)$ is also in $R(G)$, it follows that $N(\omega_1,\omega_2) \subseteq R(G)$. In addition, since $\omega_3,\omega_4,\cdots,\omega_8$ are conjugates of $\omega_1,\omega_1^{-1},\omega_2$, or ω_2^{-1}, they are in $R(G)$.

Now, to show that the reverse inclusion holds, we assume that *g* is a word in *G* having the form $g = AxyB$, where A, B are words in *G*. Then *g* can be transformed to $\tilde{g} = A\tilde{y}\tilde{x}B$ by multiplying *g* on the right by $B^{-1}y^{-1}zyB$ where $x,\tilde{x},y,\tilde{y},z$ are as indicated below:

x	y	$\tilde{y}$	$\tilde{x}$	z
τ	σ^{-2}	σ^2	τ	ω_1
σ^2	τ^{-1}	τ^{-1}	σ^{-2}	ω_1^{-1}
σ	τ^{-2}	τ^2	σ	ω_2
τ^2	σ^{-1}	σ^{-1}	τ^{-2}	ω_2^{-1}

Continued

τ	σ^2	σ^{-2}	τ	ω_3
σ^{-2}	τ^{-1}	τ^{-1}	σ^2	ω_3^{-1}
τ^{-1}	σ^{-2}	σ^2	τ^{-1}	ω_4
σ^2	τ	τ	σ^{-2}	ω_4^{-1}
τ^{-1}	σ^2	σ^{-2}	τ^{-1}	ω_5
σ^{-2}	τ	τ	σ^2	ω_5^{-1}
τ^{-2}	σ	σ	τ^2	ω_6
σ^{-1}	τ^2	τ^{-2}	σ^{-1}	ω_6^{-1}
τ^{-2}	σ^{-1}	τ^{-2}	σ^{-1}	ω_7
σ	τ^2	τ^{-2}	σ	ω_7^{-1}
τ^2	σ	σ	τ^{-2}	ω_8
σ^{-1}	τ^{-2}	τ^2	σ^{-1}	ω_8^{-1}

Hence, $\tilde{g} = gB^{-1}y^{-1}zyB$, implying that $g = \tilde{g}B^{-1}y^{-1}z^{-1}yB$. Since $B^{-1}y^{-1}z^{-1}yB \in N(\omega_1,\omega_2)$, this shows that any word $g \in G$ can be transformed to an element $\tilde{g}$ by moving even powers of σ to the left and even powers of τ to the right. When this process is completed, $\tilde{g}$ has the form $\sigma^{b'}x\tau^{c'}$, where x has the form $\tau^{i_1}\sigma^{j_1}\tau^{i_2}\sigma^{j_2}\cdots\tau^{i_n}\sigma^{j_n}$, with each $i_k, j_k = \pm 1$. If some exponent is −1, say, τ^{-1}, then we can represent this as $\tau^{-1} = \tau\tau^{-2}$. Now, the τ^{-2} can be moved to the right. In this way, we eventually arrive at $\tilde{g} = \sigma^b(\tau\sigma)^a\tau^c, a \geq 0$, and $\tilde{g} = gC$, with $C \in N(\omega_1,\omega_2)$. Now, suppose $g \in R(G)$. Since $C \in N(\omega_1,\omega_2)$, it follows that $C \in R(G)$. Therefore, $\tilde{g} \in R(G)$, so $\sigma^b(\tau\sigma)^a\tau^c$ is the identity, and $(\tau\sigma)^a = \sigma^{-b}\tau^{-c}$ in *G*. By Theorem 2.3, $a = b = c = 0$. This means that $\tilde{g}$ is the empty word, and *g* is the word $C^{-1} \in N(\omega_1,\omega_2)$. Thus, $R(G) \subseteq N(\omega_1,\omega_2)$, and we have $R(G) = N(\omega_1,\omega_2)$. ■

Theorem 2.4 has an immediate corollary.

Corollary 2.5 *Every word* $\omega \in G$ *has an equivalent form* $\omega = \sigma^b(\tau\sigma)^a\tau^c x$, *where* $x \in N(\omega_1,\omega_2)$. *and* $a \geq 0$.

We are now ready to prove our main result.

Theorem 2.6 $\{\omega_1,\omega_2\}$ *is a minimal presentation for G.*

Proof. We must show that $\omega_1 \notin N(\omega_2)$ and $\omega_2 \notin N(\omega_1)$, where $\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2$ and $\omega_2 = \sigma^{-1}\tau^2\sigma\tau^2$. For any word $x = \sigma^{i_1}\tau^{j_1}\cdots\sigma^{i_n}\tau^{j_n}$, define $e_\sigma(x) = i_1 + i_2 + \cdots + i_n$ and $e_\tau(x) = j_1 + j_2 + \cdots + j_n$. If $y = z^{-1}\omega_1 z$, then $e_\sigma(y) = 4$. If $y = z^{-1}\omega_2 z$, then $e_\tau(y) = 4$. If $y = z^{-1}\omega_1^{-1}z$, then $e_\sigma(y) = -4$. If $y = z^{-1}\omega_2^{-1}z$, then $e_\tau(y) = -4$. If *x* is a conjugate of ω_2 or ω_2^{-1}, then $e_\sigma(x) = 0$. If $\omega_1 \in N(\omega_2)$, then $\omega_1 = x_1x_2\cdots x_n$, with each x_i a conjugate of ω_2 or ω_2^{-1}. Therefore, $4 = e_\sigma(\omega_1) = e_\sigma(x_1) + e_\sigma(x_2) + \cdots + e_\sigma(x_n) = 0$, a contradiction. Hence, $\omega_1 \notin N(\omega_2)$. By a similar argument, $\omega_2 \notin N(\omega_1)$. ■

Example 2.7 *Transform* $\omega = \tau^4\sigma^{-1}\tau\sigma^2\tau^3\sigma^3$ *by* $AxyB \to A\tilde{y}\tilde{x}B$ *of Theorem 2.5 and show that* $\omega \in N(\omega_1, \omega_2)$.

The step-by-step process involves multiplying $AxyB$ *on the right by* $C = B^{-1}y^{-1}zyB$ (*where z is a particular value of* ω_i *or* ω_i^{-1}) *to obtain* $A\tilde{y}\tilde{x}B$. *At each stage, we make use of the reductions* $\sigma^a\sigma^b = \sigma^{a+b}$, $\tau^a\tau^b = \tau^{a+b}$, *delete* σ^0, τ^0. *We halt the procedure when the identity, i.e., the empty word, is reached.*

A	x	y	B	$\tilde{y}$	$\tilde{x}$	z	$C = B^{-1}y^{-1}zyB$
$A_1 = \tau^2$	τ^2	σ^{-1}	$\tau\sigma^2\tau^3\sigma^3 = B_1$	σ^{-1}	τ^{-2}	ω_2^{-1}	$C_1 = B_1^{-1}\sigma\omega_2^{-1}\sigma^{-1}B_1$
$A_2 =$ empty	τ^2	σ^{-1}	$\tau^{-1}\sigma^2\tau^3\sigma^3 = B_2$	σ^{-1}	τ^{-2}	ω_2^{-1}	$C_2 = B_2^{-1}\sigma\omega_2^{-1}\sigma^{-1}B_2$
$A_3 = \sigma^{-1}\tau^{-2}$	τ^{-1}	σ^2	$\tau^3\sigma^3 = B_3$	σ^{-2}	τ^{-1}	ω_5	$C_3 = B_3^{-1}\sigma^{-2}\omega_5\sigma^2B_3$
$A_4 = \sigma^{-1}\tau^{-1}$	τ^{-1}	σ^{-2}	$\tau^2\sigma^3 = B_4$	σ^2	τ^{-1}	ω_4	$C_4 = B_4^{-1}\sigma^2\omega_4\sigma^{-2}B_4$
$A_5 = \sigma^{-1}$	τ^{-1}	σ^2	$\tau\sigma^3 = B_5$	σ^{-2}	τ^{-1}	ω_5	$C_5 = B_5^{-1}\sigma^{-2}\omega_5\sigma^2B_5$

So the first step replaces $\tau^2\sigma^{-1}$ with $\sigma^{-1}\tau^{-2}$ and simplifies by reducing exponents. At the final step, we obtain $\omega C_1C_2C_3C_4C_5 = I$ (*i.e.*, the empty word). Hence, $\omega = (C_1C_2C_3C_4C_5)^{-1} = C_5^{-1}C_4^{-1}C_3^{-1}C_2^{-1}C_1^{-1}$. Expressing everything in terms of powers of σ and τ reduces the equation to $\omega = \tau^4\sigma^{-1}\tau\sigma^2\tau^3\sigma^3$, with deletion of σ^0, τ^0. ■

2.2. The Finite Permutation Groups G_{4n}

We define a translation operation on $S = \mathbb{Z}^+ \cup \mathbb{Z}^-$ for each positive integer *n*. We then form equivalence classes denoted by S_{4n}. The permutations σ, τ are well-defined mappings on S_{4n}. The permutation group generated by σ, τ on S_{4n} is denoted by G_{4n}. Theorem 2.2 is generalized in order to determine the relators $R(G_{4n})$ of G_{4n}. We also determine the order of each G_{4n}.

Definition 2.8 *Let n be a positive integer and* $S = \mathbb{Z}^+ \cup \mathbb{Z}^-$. *Define a mapping* $\phi_n : S \to S$ *by*

- $\phi_n(x^+) = (x+n)^+ = \sigma^{-n}(x^+)$
- $\phi_n(x^-) = (x+n)^- = \sigma^n(x^-)$

If $x \in S$, then $x+n$ denotes $\phi_n(x)$.

Theorem 2.9 *If n is even, then* $\sigma(x+n) = \sigma(x)+n$, *and* $\tau(x+n) = \tau(x)+n$

Proof. If $x = x^+$, then $\sigma(x^+ + n) = \sigma((x+n)^+) = (x+n-1)^+ = \sigma(x^+)+n$, and

$$\tau(x^+ + n) = \tau((x+n)^+) = \begin{cases} (x+n+2)^-, & \text{if } x \equiv 0 \pmod 2 \\ (x+n-2)^-, & \text{if } x \equiv 1 \pmod 2 \end{cases}$$

$=$

$$\begin{cases} \tau(x^+)+n, & \text{if } x \equiv 0 \pmod 2 \\ \tau(x^+)+n, & \text{if } x \equiv 1 \pmod 2 \end{cases}$$

If $x = x^-$, then $\sigma(x^- + n) = \sigma((x+n)^-) = (x+n+1)^- = \sigma(x^-) + n$, and $\tau(x^- + n) = \tau((x+n)^-) = (x+n)^+ = \tau(x^-) + n$. ■

Definition 2.10 *Let n be a positive integer. Define a relation* $\tilde{n}$ *on S by*

- $x^+ \tilde{n} y^+$ if $x \equiv y \pmod{2n}$
- $x^- \tilde{n} y^-$ if $x \equiv y \pmod{2n}$

Theorem 2.11 $\tilde{n}$ *is an equivalence relation on S.*

Proof. Trivial, since $x \equiv y \pmod{2n}$ is an equivalence relation on $\mathbb{Z}$. ■

Remark: For simplicity of notation, we write ˜ instead of $\tilde{n}$ when *n* is a fixed positive integer.

Definition 2.12 S_{4n} *is the set of equivalence classes of S under* ˜.

Example 2.13 *Let* $[\,]$ *denote an equivalence class in* S_{4n}. *Then*

- $S_4 = \{[0^+],[1^+],[0^-],[1^-]\}$
- $S_8 = \{[0^+],[1^+],[2^+],[3^+],[0^-],[1^-],[2^-],[3^-]\}$

Theorem 2.14 *Let* $x, y \in S$. *If* $x \,\tilde{}\, y$, *then* $\sigma(x) \,\tilde{}\, \sigma(y)$ *and* $\tau(x) \,\tilde{}\, \tau(y)$. *Therefore,* σ, τ *induce permutations of* S_{4n}.

Proof. Suppose $x^+ \,\tilde{}\, y^+$. Then $x \equiv y \pmod{2n}$, so $x^+ = y^+ + 2kn$ for some $k \in \mathbb{Z}$. By Theorem 2.9, $\sigma(x^+) = \sigma(y^+ + 2kn) = \sigma(y^+) + 2kn$, and $\tau(x^+) = \tau(y^+ + 2kn) = \tau(y^+) + 2kn$. Therefore, $\sigma(x^+) \,\tilde{}\, \sigma(y^+)$ and $\tau(x^+) \,\tilde{}\, \tau(y^+)$; an identical argument applies to $x^- \,\tilde{}\, y^-$. Therefore, σ, τ induce maps of S_{4n} to S_{4n}. Since $\sigma, \tau : S \to S$ are onto, the induced maps on S_{4n} are onto.

RTS: the induced maps are 1-1. Suppose $\sigma([x^+]) = \sigma([y^+])$. Then $\sigma(x^+)\sigma(y^+)$, implying, for some $k \in \mathbb{Z}$, $\sigma(x^+) = \sigma(y^+) + 2kn = \sigma(y^+ + 2kn)$ by Theorem 2.2. Since σ is 1-1, $x^+ = y^+ + 2kn$, and $[x^+] = [y^+]$. Identical arguments apply to $\sigma([x^-]) = \sigma([y^-]), \tau([x^+]) = \tau([y^+])$, and $\tau([x^-]) = \tau([y^-])$. ■

Definition 2.15 G_{4n} *is the group of permutations of* S_{4n} *generated by the permutations of* σ *and* τ.

Corollary 2.5 still applies, so that each word w in G_{4n} has an equivalent word representation $w = \sigma^b (\tau\sigma)^a \tau^c x$ with $a \ge 0$ and $x \in N(\omega_1, \omega_2)$. However, Theorem 2.3 no longer applies, so we require a modification.

Theorem 2.16 *Let* $\sigma, \tau : S_{4n} \to S_{4n}$ *as defined above. Let* a, b, c *be integers. Then* $(\tau\sigma)^a = \sigma^b \tau^c$ *if*

1) $a \equiv b \equiv c \equiv 0 \pmod 2$, $2b \equiv 0 \pmod{2n}$, $2c \equiv 0 \pmod{2n}$, $a \equiv b + c \pmod{2n}$, or

2) $a \equiv b \equiv c \equiv 1 \pmod 2$, $2(b+1) \equiv 0 \pmod{2n}$, $2(c+1) \equiv 0 \pmod{2n}$, $a \equiv b + c + 1$ (mod 2n).

Proof. First suppose $a \equiv 0 \pmod 2$ and $(\tau\sigma)^a = \sigma^b \tau^c$. The formula for $(\tau\sigma)^a$ in Theorem 2.2 imply that $c \equiv 0 \pmod 2$. Let $x \equiv 0 \pmod 2$. Equating $(\tau\sigma)^a$ and $\sigma^b \tau^c$ on the classes $[x^+], [(x+1)^+], [x^-], [(x+1)^-]$.

1) $[(x-a)^+] = [(x-b+c)^+]$

2) $[(x+1+a)^+] = [(x+1-b-c)^+]$

3) $\left[(x+a)^{-}\right]=\left[(x+b+c)^{-}\right]$

4) $\left[(x+1-a)^{-}\right]=\left[(x+1+b-c)^{-}\right]$

5) Equations (1)-(4) imply, by Definition 2.10, that $-a\equiv -b+c \pmod{2n}$

6) $a+1\equiv -b-c+1 \pmod{2n}$

7) $a\equiv b+c \pmod{2n}$

8) $-a+1\equiv b-c+1 \pmod{2n}$. Now, (5) and (7) imply that $2c\equiv 0 \pmod{2n}$. Additionally, (5) and (6) imply that $2b\equiv 0 \pmod{2n}$. Finally, (7) implies $a\equiv b+c \pmod{2n}$. Hence, $a\equiv 0 \pmod 2$, and Equations (1)-(4) imply

9) $a\equiv b\equiv c\equiv 0 \pmod 2$

10) $2b\equiv 0 \pmod{2n}$

11) $2c\equiv 0 \pmod{2n}$

12) $a\equiv b+c \pmod{2n}$

Conversely, suppose 9 - 12 hold. Then, working mod 2*n*, $-a\equiv -(b+c)\equiv -b-c+2c\equiv -b+c$, while $a+1\equiv b+c+1\equiv b+c+1-2b-2c\equiv -b-c+1$, with $a\equiv b+c$, and thus, $-a+1\equiv -(b+c)+1\equiv -b-c+1+2b\equiv b-c+1$, so Equations (5)-(8) hold. This Implies (1)-(4), which implies $(\tau\sigma)^a=\sigma^b\tau^c$.

Now suppose $a\equiv 1 \pmod 2$ and $(\tau\sigma)^a=\sigma^b\tau^c$. Again, by Theorem 2.2, we must have $c\equiv 1 \pmod 2$ and the equations

1') $-a-2\equiv (b+c+1) \pmod{2n}$

2') $a+1\equiv (b-c) \pmod{2n}$

3') $a\equiv (-b+c-1) \pmod{2n}$

4') $-a+3\equiv (-b-c+2) \pmod{2n}$; substituting $a\equiv c\equiv 1 \pmod 2$ into (2') yields $2\equiv (b-1) \pmod 2$, so

5') $a\equiv b\equiv c\equiv 1 \pmod 2$; (1') and (2') yields

6') $2(b+1)\equiv 0 \pmod{2n}$; (1') and (3') yields

7') $2(c+1)\equiv 0 \pmod{2n}$; (4') yields

8') $a\equiv (b+c+1) \pmod{2n}$

Conversely, if (5')-(8') hold, then, working mod 2*n*,

- $-a-2\equiv -b-c-1-2+2(b+1)+2(c+1)\equiv b+c+1$
- $a+1\equiv b+c+1+1-2(c+1)\equiv b-c$
- $a\equiv b+c+1-2(b+1)\equiv -b+c-1$
- $-a+3\equiv -b-c-1+3\equiv -b-c+2$

Hence, (1')-(4') hold, which implies $(\tau\sigma)^a=\sigma^b\tau^c$. ■

Corollary 2.17 *$\sigma^b(\tau\sigma)^a\tau^c$ is the identity in G_{4n} if and only if*

1) $a\equiv b\equiv c\equiv 0 \pmod 2$, $2b\equiv 0 \pmod{2n}$, $2c\equiv 0 \pmod{2n}$, $a+b+c\equiv 0 \pmod{2n}$, or

2) $a\equiv b\equiv c\equiv 1 \pmod 2$, $2(b-1)\equiv 0 \pmod{2n}$, $2(c-1)\equiv 0 \pmod{2n}$, $a+b+c\equiv 1 \pmod{2n}$

Proof. $\sigma^b(\tau\sigma)^a\tau^c$ is the identity if and only if $(\tau\sigma)^a=\sigma^{-b}\tau^{-c}$. Now, replace b,c with $-b,-c$ in Theorem 2.14. ■

Corollary 2.18 *If a word ω represents the identity in G_{4n}, i.e., $\omega\in R(G_{4n})$, then $\omega=\sigma^b(\tau\sigma)^a\tau^c x$ where $x\in N(\omega_1,\omega_2)$ and a,b,c satisfy*

(1) *or* (2) *of Corollary* 2.17.

Proof. By Corollary 2.5, there is a word $y \in N(\omega_1, \omega_2)$ such that $\omega y = \sigma^b (\tau\sigma)^a \tau^c$. Hence, $\omega = \sigma^b (\tau\sigma)^a \tau^c y^{-1}$. Since ω and y^{-1} represent the identity in G_{4n}, $\sigma^b (\tau\sigma)^a \tau^c$ represents the identity, and Cor. 2.17 applies. ■

We can improve Corollary 2.18 as follows:

Theorem 2.19 *A word* $\omega \in R(G_{4n})$ *if* $\omega = g\sigma^b (\tau\sigma)^a \tau^c g^{-1} \omega'$, *where* $\omega' \in N(\omega_1, \omega_2)$, $g = \sigma$ *or* 1 (*i.e.*, *empty word*), *and a*, *b*, *c satisfy* (*henceforth* (*)): $a \equiv b \equiv c \equiv 0 (\operatorname{mod} 2)$, $2b \equiv 0 (\operatorname{mod} 2n)$, $2c \equiv 0 (\operatorname{mod} 2n)$, $a + b + c \equiv 0 (\operatorname{mod} 2n)$.

Proof. Suppose $\omega \in R(G_{4n})$. By Corollary 2.18, $\omega = \sigma^b (\tau\sigma)^a \tau^c x$ where $x \in N(\omega_1, \omega_2)$, and a, b, c satisfy (1) or (2) of Corollary 2.17. Suppose they satisfy (2). Making use of $\tau^2 \sigma = \sigma \tau^{-2}$, which follows from the relator $\omega_6 = \tau^2 \sigma \tau^2 \sigma^{-1}$, and $\tau^{-2} \sigma = \sigma \tau^2$, which follows from the relator $\omega_8 = \tau^{-2} \sigma \tau^{-2} \sigma^{-1}$, we can move even powers of τ to the right to obtain

$$\begin{aligned} \omega &= \sigma^b (\tau\sigma)^a \tau^c x = \sigma\sigma^{b-1} (\tau\sigma)^a \tau\tau^{c-1} \sigma\sigma^{-1} x \\ &= \sigma\sigma^{b-1} (\tau\sigma)^a \tau\sigma\tau^{1-c} \sigma^{-1} x y = \sigma\sigma^{b'} (\tau\sigma)^{a'} \tau^{c'} \sigma^{-1} \omega' \end{aligned}$$

where $y \in N(\omega_1, \omega_2)$, $a' = a + 1$, $b' = b - 1$, $c' = 1 - c$, $\omega' = xy \in N(\omega_1, \omega_2)$. Then

$a' \equiv b' \equiv c' \equiv 0 (\operatorname{mod} 2)$, $2b' \equiv 0 (\operatorname{mod} 2n)$, $2c' \equiv 0 (\operatorname{mod} 2n)$, and $a' + b' + c' = a + 1 + b - 1 + 1 - c = a + b + c - 2(c - 1) - 1 \equiv 0 (\operatorname{mod} 2n)$.

If (1) holds, we can take $g = 1$ and $\omega' = x$. ■

Next we determine the relators $R(G_{4n})$ and minimal presentations for G_{4n}. We first consider $n = 1$, then *n* odd and greater than 1, then *n* even.

Theorem 2.20 $R(G_4) = N(\sigma^2, (\tau\sigma)^2, \tau^2)$ *and* $\{\sigma^2, (\tau\sigma)^2, \tau^2\}$ *is a minimal presentation for* G_4.

Proof. The diagram for S_4 (see **Figure 2**) shows that $\sigma^2, (\tau\sigma)^2$, and τ^2 all belong to $R(G_4)$. Therefore, $N(\sigma^2, (\tau\sigma)^2, \tau^2) \subset R(G_4)$. Conversely, suppose $\omega \in R(G_4)$. By Theorem 2.19, $\omega = g\sigma^b (\tau\sigma)^a \tau^c g^{-1} \omega'$ with a, b, c even and $\omega' \in N(\omega_1, \omega_2)$, and $g = \sigma$ or 1. But $\omega_1 = \tau^{-1} \sigma^2 \tau \sigma^2$ and $\omega_2 = \sigma^{-1} \tau^2 \sigma \tau^2$ belong to $N(\sigma^2, (\tau\sigma)^2, \tau^2)$, so $R(G_4) \subset N(\sigma^2, (\tau\sigma)^2, \tau^2)$.

Now we show that $\{\sigma^2, (\tau\sigma)^2, \tau^2\}$ is a minimal presentation for G_4. First, we show that $(\tau\sigma)^2$ cannot be expressed as a product of conjugates of $\sigma^2, \sigma^{-2}, \tau^2, \tau^{-2}$. Suppose it could, so (a) $(\tau\sigma)^2 = c_1 c_2 \cdots c_k$, where each c_i is a conjugate of $\sigma^2, \sigma^{-2}, \tau^2, \tau^{-2}$. Now (a) is an equation valid in the free group on the symbols σ, τ. It must hold if σ, τ take values in any group *G*. Let *G* be the permutation group on $\{1, 2, 3\}$ and $\sigma = (12)$, $\tau = (23)$. Then $\sigma^2 = \tau^2 = id$,

$$\begin{array}{c} S_4 \\ [0^+] \rightleftharpoons [1^+] \\ \Uparrow\Downarrow \qquad \Uparrow\Downarrow \\ [0^-] \rightleftharpoons [1^-] \end{array}$$

Figure 2. The diagram shows σ, τ on S_4.

and $\tau\sigma=(132)$, $(\tau\sigma)^2=(123)$ as permutations in *G*. In *G*, (a) becomes $(123)=id$, which is a contradiction. Therefore, $(\tau\sigma)^2$ cannot have (a) as a representation in the free group of σ,τ.

For the other two cases, take (b) $\sigma^2=c_1c_2\cdots c_k$, with c_i conjugate in $\tau^2,(\tau\sigma)^2$. Choose $\sigma=(132),\tau=(23),(\tau\sigma)=(12)$. Then (b) yields $(123)=id$, a contradiction. Finally, take (c) $\tau^2=c_1c_2\cdots c_k$, c_i conjugate in $\sigma^2,(\tau\sigma)^2$. Choose $\sigma=(12),\tau=(132),(\tau\sigma)=(23)$. Then (c) yields $(123)=id$, a contradiction. Therefore, $\left\{\sigma^2,(\tau\sigma)^2,\tau^2\right\}$ is a minimal presentation for G_4. ■

Theorem 2.21 *If n is odd and* $n>1$, *then* $R(G_{4n})=N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1,\omega_2\right)$ *and* $\left\{\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1,\omega_2\right\}$ *is a minimal presentation.*

Proof. Clearly, $\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n}$ all satisfy the hypothesis of Theorem 2.19, so they clearly belong to $R(G_{4n})$. Since ω_1,ω_2 also belong to $R(G_{4n})$, we have $N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1,\omega_2\right)\subset R(G_{4n})$.

Conversely, suppose $\omega\in R(G_{4n})$. By Theorem 2.19, $\omega=g\sigma^b(\tau\sigma)^a\tau^c g^{-1}\omega'$, with a,b,c satisfying (*), and $\omega'\in N(\omega_1,\omega_2)$ with $g=\sigma$ or 1. Then a,b,c are multiples of 2*n*, so $\omega\in N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1,\omega_2\right)$.

Let $F(\sigma,\tau)$ be a free group on the symbols σ,τ. To show $\left\{\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1,\omega_2\right\}$ is a minimal presentation, we argue as follows:

Let $\omega=\sigma^{i_1}\tau^{j_1}\cdots\sigma^{i_k}\tau^{j_k}$. Define $e_\sigma(\omega)=i_1+i_2+\cdots+i_k$, $e_\tau(\omega)=j_1+j_2+\cdots+j_k$ Then e_σ,e_τ are well-defined for $\omega\in F(\sigma,\tau)$. Since $\omega_1=\tau^{-1}\sigma^2\tau\sigma^2$, $\omega_2=\sigma^{-1}\tau^2\sigma\tau^2$, we have $e_\sigma(\omega_1)=4$, $e_\sigma(\omega_2)=0$. Also, $e_\sigma\left(\sigma^{2n}\right)=e_\sigma\left((\tau\sigma)^{2n}\right)=2n$, and $e_\sigma\left(\tau^{2n}\right)=0$. If $\omega_1\in N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_2\right)$, applying e_σ to the representation for ω_1 yields $4\equiv 0(\bmod 2n)$. Since $n\ge 3$, this is a contradiction. Therefore, $\omega_1\notin N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_2\right)$. Using e_τ and employing a similar argument, we obtain $\omega_2\notin N\left(\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n},\omega_1\right)$.

Now suppose $(\tau\sigma)^{2n}\in N\left(\sigma^{2n},\tau^{2n},\omega_1,\omega_2\right)$ so that $(\tau\sigma)^{2n}=c_1c_2\cdots c_k$, where each c_i is a conjugate in $N\left(\sigma^{2n},\tau^{2n},\omega_1,\omega_2\right)$. Since this equation holds in $F(\sigma,\tau)$, it most hold in any group *G* in which σ,τ are assigned values. Let *G* be the permutation group on $\{1,2,\cdots,2n+1\}$ and set $\sigma=(12)(34)\cdots(2n-1,2n)$, $\tau=(23)(45)\cdots(2n,2n+1)$. Then $\sigma^2=\tau^2=id$, so $c_1c_2\cdots c_k=id$ in *G*, but $\tau\sigma=(1,3,5,\cdots,(2n-1),(2n+1),2n,(2n-2),\cdots,2)$, which has order $2n+1$, so that $(\tau\sigma)^{2n}\ne id$ in *G*. Therefore, $(\tau\sigma)^{2n}\notin N\left(\sigma^{2n},\tau^{2n},\omega_1,\omega_2\right)$.

To show that $\sigma^{2n}\notin N\left(\tau^{2n},(\tau\sigma)^{2n},\omega_1,\omega_2\right)$, let *G* be as above, with $\sigma=(1,2,3,\cdots,2n,2n+1)$, $\tau=(1,2)(3,2n+1)(4,2n)(5,2n-1)\cdots(n+1,n+3)$. Then $\tau\sigma=(2,2n+1)(3,2n)\cdots(n+1,n+2)$, while $\tau\sigma^2=(1,2n+1)(2,2n)(3,2n-1)\cdots(n,n+2)$. Thus, $\sigma^{2n}\ne id$, but $\tau^{2n}=(\tau\sigma)^{2n}=id$, $\omega_2=\sigma^{-1}\tau^2\sigma\tau^2=id$, $\omega_1=\tau^{-1}\sigma^2\tau\sigma^2=id$. Therefore, $\sigma^{2n}\notin N\left(\tau^{2n},(\tau\sigma)^{2n},\omega_1,\omega_2\right)$.

Finally, we show that $\tau^{2n}\notin N\left(\sigma^{2n},\tau^{2n},\omega_1,\omega_2\right)$. Let *G* be as above, with $\tau=(1,2,3,\cdots,2n,2n+1)$, $\sigma=(1,2)(3,2n+1)(4,2n)(5,2n-1)\cdots(n+1,n+3)$. Then $\tau\sigma=(1,3)(4,2n+1)(5,2n)\cdots(n+2,n+3)$, $\sigma\tau^2=(1,2n+1)(2,2n)(3,2n-1)\cdots(n,n+2)$. Thus, $\sigma^{2n}=(\tau\sigma)^{2n}=id$,

$\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2 = id$, $\omega_2 = \sigma^{-1}\tau^2\sigma\tau^2 = id$, but $\tau^{2n} \neq id$. Therefore, $\tau^{2n} \notin N\left(\sigma^{2n}, (\tau\sigma)^{2n}, \omega_1, \omega_2\right)$. This proves that $\left\{\sigma^{2n}, (\tau\sigma)^{2n}, \tau^{2n}, \omega_1, \omega_2\right\}$ is a minimal presentation for $R(G_{4n})$, the relators in G_{4n}. ■

Theorem 2.22 *If n is even, then*

$$R(G_{4n}) = N\left((\tau\sigma)^{2n}, \sigma^n(\tau\sigma)^n, (\tau\sigma)^n\tau^n, \omega_1, \omega_2\right).$$

Proof. First note that $\tau^{2n}, \sigma^{2n} \in N\left((\tau\sigma)^{2n}, \sigma^n(\tau\sigma)^n, (\tau\sigma)^n\tau^n, \omega_1, \omega_2\right)$, since $\tau^{2n} = (\tau\sigma)^{-2n}\left[(\tau\sigma)^n\left[(\tau\sigma)^n\tau^n\right](\tau\sigma)^{-n}\right](\tau\sigma)^n\tau^n$ and $\sigma^{2n} = \sigma^n(\tau\sigma)^n\left[(\tau\sigma)^{-n}\left[\sigma^n(\tau\sigma)^n\right](\tau\sigma)^n\right](\tau\sigma)^{-2n}$. Therefore it is sufficient to show that $R(G_{4n}) = \tilde{N} = N\left(\sigma^{2n}, \tau^{2n}, (\tau\sigma)^{2n}, \sigma^n(\tau\sigma)^n, (\tau\sigma)^n\tau^n, \omega_1, \omega_2\right)$. By Theorem 2.19, $\omega \in R(G_{4n})$ if $\omega = g\sigma^b(\tau\sigma)^a\tau^c g^{-1}\omega'$, with $\omega' \in N(\omega_1, \omega_2)$, $g = \sigma$ or 1, and $a \equiv b \equiv c \equiv 0 \pmod 2$, $2b \equiv 2c \equiv 0 \pmod{2n}$, $a + b + c \equiv 0 \pmod{2n}$. The conditions on a, b, c are equivalent to $a \equiv b \equiv c \equiv 0 \pmod 2$, $a \equiv b \equiv c \equiv 0 \pmod n$, $a + b + c \equiv 0 \pmod{2n}$. Each of the elements $\sigma^{2n}, \tau^{2n}, (\tau\sigma)^{2n}, \sigma^n(\tau\sigma)^n, (\tau\sigma)^n\tau^n, \omega_1, \omega_2$ has the required form ω of Theorem 2.19. Therefore, $\tilde{N} \subset R(G_{4n})$.

Conversely, suppose $\omega \in R(G_{4n})$ with $\omega = g\sigma^b(\tau\sigma)^a\tau^c g^{-1}\omega'$ as above. It remains to show that $\sigma^b(\tau\sigma)^a\tau^c \in \tilde{N}$, which would imply that $\omega \in \tilde{N}$. There are four cases.

1) $\underline{b \equiv 0 \pmod{2n} \text{ and } c \equiv 0 \pmod{2n}}$

Then $a \equiv 0 \pmod{2n}$, so $a = 2na', b = 2nb', c = 2nc'$, and

$$\sigma^b(\tau\sigma)^a\tau^c = \left(\sigma^{2n}\right)^{b'}\left[(\tau\sigma)^{2n}\right]^{a'}\left(\tau^{2n}\right)^{c'} \in \tilde{N}.$$

2) $\underline{b \equiv 0 \pmod{2n} \text{ and } c \not\equiv 0 \pmod{2n}}$

Since $a + b + c \equiv 0 \pmod{2n}$, we must have $a \not\equiv 0 \pmod{2n}$. Then $a = 2na' + n, b = 2nb', c = 2nc' + n$, so

$$\sigma^b(\tau\sigma)^a\tau^c = \left(\sigma^{2n}\right)^{b'}\left[(\tau\sigma)^{2n}\right]^{a'}\left[(\tau\sigma)^n\tau^n\right]\left(\tau^{2n}\right)^{c'} \in \tilde{N}.$$

3) $\underline{c \equiv 0 \pmod{2n} \text{ and } b \not\equiv 0 \pmod{2n}}$

Then $a \not\equiv 0 \pmod{2n}$, so $a = 2na' + n, b = 2nb' + n, c = 2nc'$, and

$$\sigma^b(\tau\sigma)^a\tau^c = \left(\sigma^{2n}\right)^{b'}\left[\sigma^n(\tau\sigma)^n\right]\left[(\tau\sigma)^{2n}\right]^{a'}\left(\tau^{2n}\right)^{c'} \in \tilde{N}.$$

4) $\underline{b \not\equiv 0 \pmod{2n} \text{ and } c \not\equiv 0 \pmod{2n}}$

Then $a \equiv 0 \pmod{2n}$, so $a = 2na', b = 2nb' + n, c = 2nc' + n$, and

$$\sigma^b(\tau\sigma)^a\tau^c = \left(\sigma^{2n}\right)^{b'}\left[\sigma^n(\tau\sigma)^n\right]\left[(\tau\sigma)^{2n}\right]^{a'-1}\left[(\tau\sigma)^n\tau^n\right]\left(\tau^{2n}\right)^{c'} \in \tilde{N}.$$

Therefore, $R(G_{4n}) \subset \tilde{N}$. ■

We can improve Theorem 2.22 with the following result.

Theorem 2.23 *Let n be an even positive integer. Let G be any group containing elements* x, y *such that* $x^n(yx)^n = (yx)^n y^n = y^{-1}x^2yx^2 = 1$. *Then* $(yx)^{2n} = 1$.

Proof. First note that $y^{-1}x^m yx^m = 1$ for all even $m > 0$. This is true for $m = 2$ by hypothesis, and the general result follows inductively from $y^{-1}x^{m+2}yx^{m+2} = y^{-1}x^m y\left(y^{-1}x^2yx^2\right)x^m = y^{-1}x^m yx^m = 1$. Also, $x^n(yx)^n = 1$

implies $x^n = (yx)^{-n}$, and $(yx)^n y^n = 1$ implies $y^n = (yx)^{-n}$, so $x^n = y^n$ and $(yx)^{2n} = y^{-2n}$. Therefore, it suffices to show that $y^{2n} = 1$. But $x^n = y^n$ and $y^{-1}x^n yx^n = 1$ imply that $y^{2n} = y^{-1}y^n yy^n = y^{-1}x^n yx^n = 1$. ■

Corollary 2.24 *If n is even, then* $R(G_{4n}) = N\left(\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1, \omega_2\right)$.

Proof. Since $\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2$, Theorem 2.23 implies that $(\tau\sigma)^{2n} \in N\left(\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1, \omega_2\right)$. Therefore, $R(G_{4n}) = N\left(\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1, \omega_2\right)$. ■ Now we determine minimal presentation for $R(G_{4n})$ when *n* is even. We start with $n = 2$.

Theorem 2.25 $\left\{\sigma^2 (\tau\sigma)^2, (\tau\sigma)^2 \tau^2, \omega_1\right\}$ *is a minimal presentation for* G_8.

Proof.

1) Since $\sigma^2 = \tau^2$ follows from $\sigma^2 (\tau\sigma)^2 = (\tau\sigma)^2 \tau^2 = 1$, this implies that $\omega_2 = \sigma^{-1}\tau^2\sigma\tau^2 \in N\left(\sigma^2 (\tau\sigma)^2, (\tau\sigma)^2 \tau^2, \omega_1\right)$.

2) We have $\sigma^2 (\tau\sigma)^2 \notin N\left((\tau\sigma)^2 \tau^2, \omega_1\right)$ since $e_\tau\left(\sigma^2 (\tau\sigma)^2\right) = 2$, whereas $e_\tau\left((\tau\sigma)^2 \tau^2\right) = 4$ and $e_\tau(\omega_1) = 0$ are both divisible by 4.

3) We have $(\tau\sigma)^2 \tau^2 \notin N\left(\sigma^2 (\tau\sigma)^2, \omega_1\right)$ since $e_\sigma\left((\tau\sigma)^2 \tau^2\right) = 2$, whereas $e_\sigma\left(\sigma^2 (\tau\sigma)^2\right) = 4$ and $e_\sigma(\omega_1) = e_\sigma\left(\tau^{-1}\sigma^2\tau\sigma^2\right) = 4$ are both divisible by 4.

4) To show that $\omega_1 \notin N\left(\sigma^2 (\tau\sigma)^2, (\tau\sigma)^2 \tau^2\right)$, let *G* be the permutation group on $\{1,2,3\}$ and set $\sigma = \tau = \{1,2,3\}$. Then $(\tau\sigma)^2 \tau^2 = \sigma^2 (\tau\sigma)^2 = \sigma^6 = 1$, but $\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2 = \sigma^4 = \sigma \neq 1$, so $\omega_1 \notin N\left(\sigma^2 (\tau\sigma)^2, (\tau\sigma)^2 \tau^2\right)$. ■

Theorem 2.26 *If n is even,* $n > 2$, *then* $\left\{\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1, \omega_2\right\}$ *is a minimal presentation for* G_{4n}.

Proof. Corollary 2.24 states that it is a presentation. To demonstrate its minimality, we consider two cases:

1) $\underline{n \not\equiv 0 (\mathrm{mod}\, 4)}$: In this case, $n = 2m$ with $m > 1$, *m* odd.

(a) $\sigma^n (\tau\sigma)^n \notin N\left((\tau\sigma)^n \tau^n, \omega_1, \omega_2\right)$

because $e_\tau\left(\sigma^n (\tau\sigma)^n\right) = n \not\equiv 0 (\mathrm{mod}\, 4)$, whereas

$$e_\tau\left((\tau\sigma)^n \tau^n\right) = 2n \equiv 0 (\mathrm{mod}\, 4), e_\tau(\omega_1) = e_\tau\left(\tau^{-1}\sigma^2\tau\sigma^2\right) = 0 \equiv 0 (\mathrm{mod}\, 4),$$

and

$$e_\tau(\omega_2) = e_\tau\left(\sigma^{-1}\tau^2\sigma\tau^2\right) = 4 \equiv 0 (\mathrm{mod}\, 4)$$

(b) $(\tau\sigma)^n \tau^n \notin N\left(\sigma^n (\tau\sigma)^n, \omega_1, \omega_2\right)$, because $e_\sigma\left((\tau\sigma)^n \tau^n\right) = n \not\equiv 0 (\mathrm{mod}\, 4)$, but $\sigma^n (\tau\sigma)^n, \omega_1, \omega_2$ all have e_σ values divisible by 4.

(c) $\omega_1 \notin N\left(\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_2\right)$ because $e_\sigma(\omega_1) = 4 \not\equiv 0 (\mathrm{mod}\, m)$, but the other elements have e_σ values divisible by *m*.

(d) $\omega_2 \notin N\left(\sigma^n (\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1\right)$ because $e_\tau(\omega_2) = 4 \not\equiv 0 (\mathrm{mod}\, m)$, but the other elements have e_τ values divisible by *m*.

2) $\underline{n \equiv 0 (\mathrm{mod}\, 4)}$: In this case, $n = 4k$.

(a) $(\tau\sigma)^n \tau^n \notin N\left(\sigma^n (\tau\sigma)^n, \omega_1, \omega_2\right)$. Let *G* be the permutation group on $\left\{1, 2, \cdots, 2n, \tilde{1}, \tilde{2}, \cdots, \widetilde{2n}\right\}$. Let

$\sigma = \left(1,\tilde{3},5,\tilde{7},\cdots,\widetilde{2n-1}\right)\left(\tilde{1},3,\tilde{5},7,\cdots,(2n-1)\right)\left(2n,\widetilde{2n-2},\cdots,\tilde{2}\right)\left(\widetilde{2n},(2n-2),\cdots,2\right)$,

and $\tau = (1,2,3,\cdots,2n)\left(\widetilde{2n},\widetilde{2n-1},\cdots,\tilde{2},\tilde{1}\right)$. Then $\sigma^n = 1, \tau^n \neq 1$. Also, $(\tau\sigma)^2 = 1$, so $(\tau\sigma)^n = 1$. Therefore $\sigma^n (\tau\sigma)^n = 1$, but $(\tau\sigma)^n \tau^n = \tau^n \neq 1$. Let

$$x' = \begin{cases} \tilde{y}, & \text{if } x = y \\ y, & \text{if } x = \tilde{y} \end{cases}$$

Let $a+b$ denote addition (mod 2*n*).

If *x* is odd, $x \xrightarrow{\sigma^2} x+4 \xrightarrow{\tau} (x+4)\pm 1 \xrightarrow{\sigma^2} x \pm 1 \xrightarrow{\tau^{-1}} x$

If *x* is even, $x \xrightarrow{\sigma^2} x-4 \xrightarrow{\tau} (x-4)\pm 1 \xrightarrow{\sigma^2} x \pm 1 \xrightarrow{\tau^{-1}} x$

so $\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2 = 1$ in *G*.

For example, if $n = 4$, then *G* is the permutation group on $\{1,2,3,\cdots,8,\tilde{1},\tilde{2},\cdots,\tilde{8}\}$.

$\sigma = \left(1,\tilde{3},5,\tilde{7}\right)\left(\tilde{1},3,\tilde{5},7\right)\left(8,\tilde{6},4,\tilde{2}\right)\left(\tilde{8},6,\tilde{4},2\right)$

$\sigma^2 = (1,5)\left(\tilde{3},\tilde{7}\right)\left(\tilde{1},\tilde{5}\right)(3,7)(8,4)\left(\tilde{6},\tilde{2}\right)\left(\tilde{8},\tilde{4}\right)(6,2)$

$\tau = (1,2,3,\cdots,8)\left(\tilde{8},\tilde{7},\cdots,\tilde{1}\right)$

$\tau^{-1} = (8,7,\cdots,1)\left(\tilde{1},\tilde{2},\cdots,\tilde{8}\right)$

$\tau\sigma^2 = (1,6,3,8,5,2,7,4)\left(\tilde{1},\tilde{4},\tilde{7},\tilde{2},\tilde{5},\tilde{8},\tilde{3},\tilde{6}\right)$

$\tau^{-1}\sigma^2 = (1,4,7,2,5,8,3,6)\left(\tilde{1},\tilde{6},\tilde{3},\tilde{8},\tilde{5},\tilde{2},\tilde{7},\tilde{4}\right)$

so $\tau^{-1}\sigma^2\tau\sigma^2 = 1$

For $\omega_2 = \sigma^{-1}\tau^2\sigma\tau^2$, we have:

If *x* is odd, $x \xrightarrow{\tau^2} x \pm 2 \xrightarrow{\sigma} \left[(x\pm 2)+2\right]' \xrightarrow{\tau^2} (x+2)' \xrightarrow{\sigma^{-1}} x$

If *x* is even, $x \xrightarrow{\tau^2} x \pm 2 \xrightarrow{\sigma} \left[(x\pm 2)-2\right]' \xrightarrow{\tau^2} (x-2)' \xrightarrow{\sigma^{-1}} x$

Therefore, $\omega_2 = 1$ in *G*.

Since $\sigma^n(\tau\sigma)^n, \omega_1, \omega_2$ are equal to the identity in *G*, but $(\tau\sigma)^n \tau^n \neq 1$, it follows that $(\tau\sigma)^n \tau^n \notin N\left(\sigma^n(\tau\sigma)^n, \omega_1, \omega_2\right)$.

(b) $\sigma^n(\tau\sigma)^n \notin N\left((\tau\sigma)^n \tau^n, \omega_1, \omega_2\right)$.

Using σ and τ from part (a), we note that $(\sigma\tau)^2 = 1$. Therefore, if we exchange the definitions of σ and τ, we obtain $\sigma^n(\tau\sigma)^n \neq 1$, but $(\tau\sigma)^n \tau^n = \omega_1 = \omega_2 = 1$ in *G*, which proves (b).

(c) $\omega_1 \notin N\left(\sigma^n(\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_2\right)$.

Recall that $n = 4k$. Let *G* be the permutation group on $\{1,2,\cdots,8k\}$.

If $k=1$, let $\sigma = (1,2,3,4)(5,6,7,8), \tau = (1,5)(2,6)$

Then $\tau\sigma = (1,6,7,8)(2,3,4,5)$, so $\sigma^4 = \tau^4 = (\tau\sigma)^4 = 1$, but (using $\tau^{-1} = \tau$) $\omega_1(1) = \tau\sigma^2\tau\sigma^2(1) = \tau\sigma^2\tau(3) = \tau\sigma^2(3) = \tau(1) = 5$.

If $k > 1$, let $\sigma = (1,2,\cdots,4k)(4k+1,4k+2,\cdots,8)$) and $\tau = (1,4k+1)(2,4k+2)\cdots(4k,4k+4k)$

Then $\sigma^n = \tau^n = \omega_2 = 1$.

Also,

$\tau\sigma = (1,4k+2,3,4k+4,\cdots,4k-1,4k+4k)(2,4k+3,4,4k+5,\cdots,4k,4k+1)$, so $(\tau\sigma)^n = 1$

But $\omega_1(1) = \tau\sigma^2\tau\sigma^2(1) = \tau\sigma^2\tau(3) = \tau\sigma^2(4k+3) = \tau(4k+5) = 5$.

Therefore $\omega_1 \notin N\left(\sigma^n(\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_2\right)$.

(d) $\omega_2 \notin N\left(\sigma^n(\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1\right)$. Let G be defined as in part (c). If we exchange σ, τ from part (c), we obtain $\omega_2 \notin N\left(\sigma^n(\tau\sigma)^n, (\tau\sigma)^n \tau^n, \omega_1\right)$. ■

In summary, minimal presentations for $R(G_{4n})$ are:

(a) $\left\{\sigma^2, \tau^2, (\tau\sigma)^2\right\}$ for $n=1$;

(b) $\left\{\sigma^2(\tau\sigma)^2, (\tau\sigma)^2\tau^2, \omega_1\right\}$ for $n=2$;

(c) $\left\{\sigma^{2n}, \tau^{2n}, (\tau\sigma)^{2n}, \omega_1, \omega_2\right\}$ for n odd, $n>1$;

(d) $\left\{\sigma^n(\tau\sigma)^n, (\tau\sigma)^n\tau^n, \omega_1, \omega_2\right\}$ for n even, $n>2$.

Definition 2.27 *The* order *of a group is the number of elements in the group.*

We require two lemmas to prove a theorem about the order of G_{4n}:

Lemma 2.28 *The following identities hold in* G_{4n}:

1) $(\tau\sigma)^{-1}\sigma^2 = \sigma^{-2}(\tau\sigma)^{-1}$

2) $(\tau\sigma)^{-1}\sigma^{-2} = \sigma^2(\tau\sigma)^{-1}$

3) $\tau(\tau\sigma)^a\tau^c = \sigma^2(\tau\sigma)^{-1}\tau^{-1}(\tau\sigma)^{a-1}\tau^c, a, c \in \mathbb{Z}$

4) $\tau^{-1}(\tau\sigma)^a\tau^c = \sigma^2(\tau\sigma)^{-1}\tau(\tau\sigma)^{a-1}\tau^c, a, c \in \mathbb{Z}$

Proof (of Lemma 2.28):

1) $\omega_1 = \tau^{-1}\sigma^2\tau\sigma^2 \in R(G_{4n})$, so

$\tau^{-1}\sigma^2 = \sigma^{-2}\tau^{-1} \to (\tau\sigma)^{-1}\sigma^2 = \sigma^{-1}\tau^{-1}\sigma^2 = \sigma^{-2}\sigma^{-1}\tau^{-1} = \sigma^{-2}(\tau\sigma)^{-1}$.

2) $\omega_3 = \tau^{-1}\sigma^{-2}\tau\sigma^{-2} \in R(G_{4n})$, so

$\tau^{-1}\sigma^{-2} = \sigma^2\tau^{-1} \to (\tau\sigma)^{-1}\sigma^{-2} = \sigma^{-1}\tau^{-1}\sigma^{-2} = \sigma^2\sigma^{-1}\tau^{-1} = \sigma^2(\tau\sigma)^{-1}$.

3) $\tau(\tau\sigma)^a\tau^c = \tau^2\sigma(\tau\sigma)^{a-1}\tau^c = \sigma\tau^{-2}(\tau\sigma)^{a-1}\tau^c$ (since $\omega_2 = \sigma^{-1}\tau^2\sigma\tau^2 \in R(G_{4n})$)

$=\left[\sigma^2(\tau\sigma)^{-1}\tau\right]\tau^{-2}(\tau\sigma)^{a-1}\tau^c = \sigma^2(\tau\sigma)^{-1}\tau^{-1}(\tau\sigma)^{a-1}\tau^c$.

4) $\tau^{-1}(\tau\sigma)^a\tau^c = \sigma(\tau\sigma)^{a-1}\tau^c = \sigma^2(\tau\sigma)^{-1}\tau(\tau\sigma)^{a-1}\tau^c$. ■

Lemma 2.29 *Every element* $x \in G_{4n}$ *has representation* $x = \sigma^b(\tau\sigma)^a\tau^c$ *with* b *even.*

Proof (of Lemma 2.29): By Corollary 2.5, every $x \in G_{4n}$ has a representation $x = \sigma^b(\tau\sigma)^a\tau^c$, with $a \ge 0$. If b is even, the proof is complete. Let b be odd and set $b = B+1$, B even. Then

$x = \sigma^B\sigma(\tau\sigma)^a\tau^c = \sigma^B\sigma^2(\tau\sigma)^{-1}\tau\left[(\tau\sigma)^a\tau^c\right] = \sigma^B\sigma^2(\tau\sigma)^{-1}\sigma^2(\tau\sigma)^{-1}\tau^{-1}(\tau\sigma)^{a-1}\tau^c$

(by part (3) of Lemma 2.28) $= \sigma^B\sigma^2(\tau\sigma)^{-1}\sigma^2(\tau\sigma)^{-1}\sigma^2(\tau\sigma)^{-1}\tau(\tau\sigma)^{a-2}\tau^c$ (by part (4) of Lemma 2.28)

Continuing to apply parts (3) and (4) we obtain

$$x = \begin{cases} \sigma^B\left[\sigma^2(\tau\sigma)^{-1}\right]^{a+1}\tau^{-1}\tau^c, & a \text{ odd} \\ \sigma^B\left[\sigma^2(\tau\sigma)^{-1}\right]^{a+1}\tau\tau^c, & a \text{ even} \end{cases}$$

By parts (1) and (2) of Lemma 2.28, all powers of σ^2 can be commuted to the left of $(\tau\sigma)^{-1}$ while preserving even parity. Hence, $x = \sigma^{B'}(\tau\sigma)^{-(a+1)}\tau^{c\pm1}$

with B' even. ■

Theorem 2.30 *The order of* G_{4n} *is*:

1) $4n^3$ if n is odd

2) n^3 if n is even.

Proof.

1) Suppose n is odd. By Lemma 2.29, $x=\sigma^b(\tau\sigma)^a\tau^c$, with b even. By Theorems 2.20 and 2.21, $\sigma^{2n},(\tau\sigma)^{2n},\tau^{2n}$ all belong to $R(G_{4n})$. Therefore we can take $x=\sigma^{\bar{b}}(\tau\sigma)^{\bar{a}}\tau^{\bar{c}}$, with $0\le\bar{a},\bar{b},\bar{c}<2n$, and $\bar{b}$ even. There are $(2n)(n)(2n)=4n^3$ possibilities for $\bar{a},\bar{b},\bar{c}$. If $\sigma^{\bar{b}_1}(\tau\sigma)^{\bar{a}_1}\tau^{\bar{c}_1}=\sigma^{\bar{b}_2}(\tau\sigma)^{\bar{a}_2}\tau^{\bar{c}_2}$, then $(\tau\sigma)^{-\bar{a}_2}\sigma^{\bar{b}_1-\bar{b}_2}(\tau\sigma)^{\bar{a}_1}\tau^{\bar{c}_1-\bar{c}_2}=1$. Since $\bar{b}_1-\bar{b}_2$ is even, we can use the commutation rules to obtain $\sigma^{\pm(\bar{b}_1-\bar{b}_2)}(\tau\sigma)^{\bar{a}_1-\bar{a}_2}\tau^{\bar{c}_1-\bar{c}_2}=1$.

Also, Corollary 2.17 implies that $\bar{a}_1-\bar{a}_2$ and $\bar{c}_1-\bar{c}_2$ are both even, and

- $\bar{b}_1-\bar{b}_2\equiv 0(\operatorname{mod} n)$
- $\bar{c}_1-\bar{c}_2\equiv 0(\operatorname{mod} n)$
- $\bar{a}_1-\bar{a}_2\equiv 0(\operatorname{mod} n)$.

Since $\bar{b}_1-\bar{b}_2\equiv\bar{c}_1-\bar{c}_2\equiv\bar{a}_1-\bar{a}_2\equiv 2(\operatorname{mod} n)$, and n is odd, this implies

- $\bar{b}_1-\bar{b}_2\equiv 0(\operatorname{mod} 2n)$
- $\bar{c}_1-\bar{c}_2\equiv 0(\operatorname{mod} 2n)$
- $\bar{a}_1-\bar{a}_2\equiv 0(\operatorname{mod} 2n)$,

which implies $\bar{b}_1=\bar{b}_2,\bar{c}_1=\bar{c}_2,\bar{a}_1=\bar{a}_2$ because of the conditions on $\bar{a}_i,\bar{b}_i,\bar{c}_i$. Therefore the representation $\sigma^{\bar{b}}(\tau\sigma)^{\bar{a}}\tau^{\bar{c}}$ is unique, and G_{4n} contains $4n^3$ elements when n is odd.

2) Now assume n even. Again, let $x=\sigma^b(\tau\sigma)^a\tau^c$, with b even.

By Theorem 2.19, $\sigma^n(\tau\sigma)^n,(\tau\sigma)^n\tau^n,(\tau\sigma)^{2n}$ belong to $R(G_{4n})$. Using $\sigma^n=(\tau\sigma)^{-n}$, we can transform x so that $0\le b<n$ and b is even. Using $(\tau\sigma)^n=\tau^{-n}$, we can transform x so that $0\le a<n$. Finally, using $(\tau\sigma)^{2n}=1$, we can transform x into:

(*) $x=\sigma^b(\tau\sigma)^a\tau^c$ with $0\le b<n, 0\le a<n, 0\le c<2n$, b even.

The total number of choices for a,b,c is $n\left(\frac{n}{2}\right)(2n)=n^3$. The choices yield distinct elements of G_{4n}, for if $\sigma^{\bar{b}_1}(\tau\sigma)^{\bar{a}_1}\tau^{\bar{c}_1}=\sigma^{\bar{b}_2}(\tau\sigma)^{\bar{a}_2}\tau^{\bar{c}_2}$, then $(\tau\sigma)^{-\bar{a}_2}\sigma^{\bar{b}_1-\bar{b}_2}(\tau\sigma)^{\bar{a}_1}\tau^{\bar{c}_1-\bar{c}_2}=1$, and by commuting even powers of σ with $(\tau\sigma)^{\pm 1}$, we obtain $\sigma^{\pm(\bar{b}_1-\bar{b}_2)}(\tau\sigma)^{\bar{a}_1-\bar{a}_2}\tau^{\bar{c}_1-\bar{c}_2}=1$. By Condition (1) of Corollary 2.17, we obtain

- $\bar{b}_1-\bar{b}_2\equiv 0(\operatorname{mod} n)$
- $\bar{c}_1-\bar{c}_2\equiv 0(\operatorname{mod} n)$
- $\bar{a}_1-\bar{a}_2\equiv 0(\operatorname{mod} n)$.

Since $0\le|\bar{a}_1-\bar{a}_2|,|\bar{b}_1-\bar{b}_2|<n$, we must have $\bar{b}_1=\bar{b}_2$ and $\bar{a}_1=\bar{a}_2$. However, by Condition (1) of Corollary 2.17, $\bar{c}_1-\bar{c}_2\equiv 0(\operatorname{mod} 2n)$, so $\bar{c}_1=\bar{c}_2$, since $0\le|\bar{c}_1-\bar{c}_2|<2n$. Therefore, all the elements $x=\sigma^b(\tau\sigma)^a\tau^c$ in (*) are distinct and the order of G_{4n} is n^3. ■

Finally, we determine isomorphic group structures for G_4 and G_8.

Theorem 2.31

1) G_4 is isomorphic to the Klein-4 group $\mathbb{V}$.

2) G_8 is isomorphic to the multiplicative quaternion group $\mathbb{Q}$.

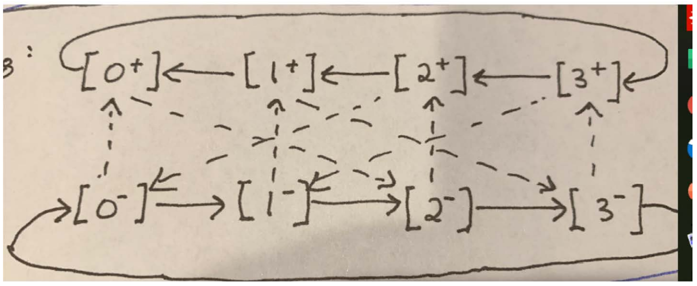

Figure 3. The diagram shows σ, τ on S_8.

Proof.

1) The diagram for G_4 is:

(σ is single line, τ is double line).

$$\begin{array}{ccc} [0^+] & \rightleftharpoons & [1^+] \\ \Uparrow\Downarrow & & \Uparrow\Downarrow \\ [0^-] & \rightleftharpoons & [1^-] \end{array}$$

By Theorem 2.30, G_4 has order 4, so $G_4 = \{1, \sigma, \tau, \sigma\tau = \tau\sigma\}$. Since $\sigma^2 = \tau^2 = (\sigma\tau)^2 = 1$, G_4 is Abelian, but not cyclic, it is $\mathbb{V}$. ■

2) Quaternions $\mathbb{Q} = \{1, i, j, k, -1, -i, -j, -k\}$, with

- $ij = k$
- $ji = -k$
- $i^2 = j^2 = k^2 = -1$
- $jk = i$
- $kj = -i$
- $ki = j$
- $ik = -j$

each has a unique representation of the form $i^a j^b$, with $0 \le a \le 3$, $0 \le j \le 1$. Also, $ji = -k = i^2 ij = i^3 j$. The diagram for G_8 is shown in Figure 3.

Clearly, $\sigma^2 = \tau^2$, and each $x \in G_8$ has a representation $x = \sigma^a \tau^b$, with $0 \le a \le 3$, $0 \le b \le 1$. Also, $\tau\sigma = \sigma^3 \tau$. Therefore, $\phi: \mathbb{Q} \to G_8$ is an isomorphism defined by $\phi(i^a j^b) = \sigma^a \tau^b$ for $0 \le a \le 3$, $0 \le b \le 1$. ■

Acknowledgements

The authors acknowledge the assistance of Dr. Nathan Kahl in the preparation of this paper. This paper is in memory of our late coauthor and friend, Dr. Michael Miniere.

Conflicts of Interest

The authors declare no conflict of interest in regards to the publication of this paper.

References

[1] Miniere, M. (1997) Stevens Institute of Technology. Ph.D. Dissertation, Hoboken,

New Jersey.

[2] Berry, K. and Tretkoff, M. (1994) The Monodromy Group of a Transcendental Function. *Contemporary Mathematics*, *American Mathematical Society*, **169**, 107-122. https://doi.org/10.1090/conm/169/01653

[3] Katsura, T. (2008) Permutation Presentations of Modules over Finite Groups. *Journal of Algebra*, **319**, 3653-3665. https://doi.org/10.1016/j.jalgebra.2008.01.023

[4] Hungerford, T.W. (1974) Algebra. Springer-Verlag, New York.

[5] Fraleigh, J.B. (1976) A First Course in Abstract Algebra. Addison-Wesley Publishing Company, Inc., Reading Mass.