2012-06-05

Weak Cayley Table Isomorphisms

Long Pham Bao Nguyen
Brigham Young University - Provo

Weak Cayley Table Isomorphisms

Long Bao Nguyen

A dissertation submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Stephen Humphries, Chair
Darrin Doud
Wayne Barrett
Pace Nielsen
William Lang

Department of Mathematics

Brigham Young University

June 2012

ABSTRACT

Weak Cayley Table Isomorphisms

Long Bao Nguyen
Department of Mathematics, BYU
Doctor of Philosophy

We investigate weak Cayley table isomorphisms, a generalization of group isomorphisms. Suppose G and H are groups. A bijective map $\phi : G \to H$ is a *weak Cayley table isomorphism* if it satisfies two conditions:

1) If $x \sim y$, then $\phi(x) \sim \phi(y)$;

2) For all $x, y \in G$, $\phi(xy) \sim \phi(x)\phi(y)$.

If there exists a weak Cayley table isomorphism between two groups, then we say that the two groups have the *same weak Cayley table*.

This dissertation has two main goals. First, we wish to find sufficient conditions under which two groups have the same weak Cayley table. We specifically study Frobenius groups and groups which satisfy the Camina pair condition.

Second, we consider the group of all weak Cayley table isomorphisms between G and itself. We call this group the *weak Cayley table group* of G and denote it by $\mathcal{W}(G)$. Any automorphism of G is an element of $\mathcal{W}(G)$. The inverse map on G is also an element of $\mathcal{W}(G)$. We say that the weak Cayley table group is *trivial* if it is generated by the set of all automorphisms of G and the inverse map. Humphries [11] proved that the symmetric groups S_n, the dihedral groups D_{2n} and the free groups $F_n (n \neq 3)$ all have trivial weak Cayley table groups. We will investigate the weak Cayley table groups of the alternating groups, certain types of Coxeter groups, the projective special linear groups and certain sporadic simple groups.

Keywords: groups, group automorphisms, weak Cayley table, weak Cayley table isomorphisms, weak Cayley table groups, character table.

Acknowledgments

The process of completing both my Master's and Ph.D. has been a long and humbling one. As I was beginning my course work, with three Ph.D. qualifiers still looming and a dissertation topic that was hazy, at best, I wondered how I was going to be able to do it all. These hurdles often seemed insurmountable. That I am able to successfully finish the program I attribute to the invaluable help of many wonderful people, of whom I will mention a few. I am forever indebted to them.

It is very difficult for me to fully and adequately express my heartfelt gratitude to my advisor, Dr. Stephen Humphries. His guidance has been, without a doubt, one of the most important factors in my success. I am grateful for his patience. He has given me time and space to learn and discover my own mathematics while providing direction and purpose to all that I do. None of this would have been possible without him.

I want to thank the rest of my committee: Dr. Doud; Dr. Nielsen, Dr. Lang and Dr. Barrett for all of their support and help in the editing and presentation of this dissertation. I especially want to acknowledge Lonette for all that she has done for me all these years. She has been so helpful and kind. I also want to thank Brigham Young University, in general, and the Mathematics Department, in particular, for providing me with the opportunity and funding to pursue such a great education.

I also wish to express my love and appreciation for my family. My parents have always encouraged me to pursue higher education and have instilled in me a love of hard work and learning; and my brothers and sister have always believed in me. Lastly, I am grateful for my wife, Lillie. Everything that is good in my life is because of her. I am thankful for her patience as I spend long hours in the office and at home. She's been there to encourage and support me through all of my personal highs and lows. She is the love of my life.

The study of mathematics has been as beautiful and wonderful as it has been spiritual. Though it is a deeply personal sentiment, I want to publicly express my gratitude and love for my Savior, Jesus Christ. He has been patient and kind in this process. Many significant

insights in my research have been attended by his spiritual confirmations and certainly motivated by his spiritual revelations.

Contents

Chapter 1. Introduction

This dissertation focuses on weak Cayley table isomorphisms of groups, these being generalizations isomorphisms of groups. We first consider weak Cayley table isomorphisms between two groups G and H and generalize several results in this area. Then we investigate the weak Cayley table group of a group G. In particular, we will study the weak Cayley table group of the alternating groups, the Coxeter groups, certain sporadic groups and the projective special linear groups. The dissertation is composed primarily of three main chapters. We summarize here some of its major results and offer a brief outline of its content.

Given two groups G and H, a *weak Cayley table isomorphism* between them is a bijection $\phi : G \to H$ which satisfies two conditions:

1) If $x \sim y$, then $\phi(x) \sim \phi(y)$;

2) For all $x, y \in G$, $\phi(xy) \sim \phi(x)\phi(y)$.

If there exists a weak Cayley table isomorphism between two groups, then we say that the two groups have the *same weak Cayley table*. In Chapter 2, we also define *Frobenius groups* and *Camina pairs*.

Johnson, Mattarei and Sehgal [15] proved several results which provide sufficient conditions for two groups to have the same weak Cayley table. We generalize their results in section 2 of Chapter 2 and prove several results which deal with Frobenius groups and Camina pairs.

In section 3 of Chapter 2, we begin with the statement of Camina's theorem regarding groups which satisfy the Camina pair condition. Camina's theorem motivates two questions concerning the weak Cayley tables of such groups. We prove several results which partially answer these questions.

Section 4 of Chapter 2 establishes some notation regarding the cohomology of groups. We then prove a simple result which says that a certain map determined by a weak Cayley table map is a trivial element of a cohomology group. We end the section by constructing a

simple way to define a weak Cayley table isomorphism between a group G and itself.

In Chapter 3, we consider the group of all weak Cayley table isomorphisms between G and itself. We call this group the *weak Cayley table group* of G and define what it means for the weak Cayley table group to be *trivial*. Humphries [11] proved that the symmetric groups S_n, the dihedral groups D_{2n} and the free groups $F_n (n \neq 3)$ all have trivial weak Cayley table groups.

Humphries' techniques for S_n do not generalize nicely in proving that the alternating group has trivial weak Cayley table group. We introduce the concept of graph automorphisms in section 2 to prove the alternating group case. The projective special linear groups require additional modification of Humphries' techniques. This we do in sections 3, 4 and 5.

We further generalize Humphries' techniques in sections 6 and 7 of Chapter 3 to prove that two types of Coxeter groups have trivial weak Cayley table groups: the Coxeter groups of type C_n and the Coxeter groups of type B_n.

In general, given a group G, it is computationally difficult to determine whether the weak Cayley table group of G is trivial. But because of the techniques we develop in Chapter 3, we can efficiently determine that certain simple groups have trivial weak Cayley groups through the computer algebra program Magma. We do this for the Mathieu groups M_{11}, M_{12} and M_{22} and the Janko groups J_1 and J_2 in Chapter 4.

We have included in the Appendix some of the code we use in Chapter 4. In addition, we provide another proof for the case $PSL(2, p)$ discussed in section 6.

Chapter 2. Weak Cayley Table Isomorphisms

2.1 Introduction

Johnson, Mattarei and Sehgal [15] generalize the concept of group automorphisms by introducing the concept of a weak Cayley table isomorphism between two groups. We first give their definition of a weak Cayley table of a group.

Definition 2.1.1. *Let $G = \{g_1 = e, g_2, \ldots, g_n\}$ be a finite group. The weak Cayley table of G is a table whose rows and columns are indexed by the elements of G and the (g, h) entry is the conjugacy class of gh.*

We note that the row indexed by e gives the conjugacy classes of G.

Example 2.1.2. *Let $G = S_3$ be the symmetric group on 3 letters. Let $C_0 = \{(1)\}$, $C_1 = \{(132), (123)\}$ and $C_2 = \{(12), (13), (23)\}$ be the conjugacy classes of G. Then the weak Cayley table of G is given in Table 2.1.*

	(1)	(123)	(132)	(12)	(23)	(13)
(1)	C_0	C_1	C_1	C_2	C_2	C_2
(123)	C_1	C_1	C_0	C_2	C_2	C_2
(132)	C_1	C_0	C_1	C_2	C_2	C_2
(12)	C_2	C_2	C_2	C_0	C_1	C_1
(23)	C_2	C_2	C_2	C_1	C_0	C_1
(13)	C_2	C_2	C_2	C_1	C_1	C_0

Table 2.1: The Weak Cayley Table for S_3

Definition 2.1.3. *Let G be a group and $a, b \in G$. We say that a is conjugate to b, denoted by $a \sim b$, if there exists $x \in G$ such that $b = x^{-1}ax$. We also define $a^x = x^{-1}ax$.*

Definition 2.1.4. *Suppose G and H are groups. A weak Cayley table isomorphism is a bijection $\phi : G \to H$ satisfying the following conditions:*

1) If $x \sim y$, then $\phi(x) \sim \phi(y)$;

2) For all $x, y \in G$, $\phi(xy) \sim \phi(x)\phi(y)$.

It's easy to see that if there exists a weak Cayley table isomorphisms $\phi : G \to H$, then G and H have the same weak Cayley table.

Example 2.1.5. *Let $G_1 = \langle a, b | a^9 = b^3 = 1, bab^{-1} = a^4 \rangle$ and $G_2 = \langle a, b, z | a^3 = b^3 = z^3 = 1, az = za, bz = zb, bab^{-1} = az \rangle$. Then G_1 and G_2 both have 27 elements. The centers are $Z(G_1) = \langle a^3 \rangle \cong \mathbb{Z}_3$ and $Z(G_2) = \langle z \rangle \cong \mathbb{Z}_3$.*

The groups G_1 and G_2 have the same weak Cayley table. We exhibit an explicit weak Cayley table isomorphism between G_1 and G_2.

$$
\begin{aligned}
e &\to e; \\
a^3 &\to z; \\
a^6 &\to z^2; \\
\left[a, a^4, a^7\right] &\to \left[az, az^2, a\right]; \\
\left[a^2, a^5, a^8\right] &\to \left[a^2, a^2z, a^2z^2\right]; \\
\left[b, a^3b, a^6b\right] &\to \left[bz, bz^2, b\right]; \\
\left[b^2, a^3b^2, a^6b^2\right] &\to \left[b^2z^2, b^2, b^2z\right]; \\
\left[ab, a^4b, a^7b\right] &\to \left[abz, abz^2, ab\right]; \\
\left[a^2b^2, a^5b^2, a^8b^2\right] &\to \left[a^2b^2, a^2b^2z, a^2b^2z^2\right]; \\
\left[a^2b, a^5b, a^8b\right] &\to \left[a^2bz, a^2bz^2, a^2b\right]; \\
\left[ab^2, a^4b^2, a^7b^2\right] &\to \left[ab^2, ab^2z, ab^2z^2\right].
\end{aligned}
$$

The following result establishes some basic properties of any weak Cayley table isomorphism ϕ.

Lemma 2.1.6. *Let ϕ be a weak Cayley table isomorphism between G and H. Then,*

(1) $\phi(e) = e$ and $\phi(g^{-1}) = \phi(g)^{-1}$, where e denotes the identity element of G.

(2) If N is a normal subgroup of G, then $\phi(N)$ is a normal subgroup of H.

(3) If N is a normal subgroup of G , then the image of the coset gN in G is the coset $\phi(g)\phi(N)$ in H.

4) If N is a normal subgroup of G, then ϕ induces a weak Cayley table isomorphism $\bar{\phi} : G/N \to H/\phi(N)$.

(5) If $\phi : G \to H$ is a weak Cayley table isomorphism, then G and H have the same number of involutions, that is, the same number of elements of order 2.

(6) If G and H have the same weak Cayley table, then they have the same character tables.

Proof. We will prove parts (1), (2), (3) and (5). The proof of parts (4) and (6) can be found in [15]. To prove part (1), we note that the first condition of the definition implies that $\phi(e)$ is central in H. The second condition then gives us that $\phi(e)\phi(e) = \phi(ee) = \phi(e)$ and thus $\phi(e) = e$. To prove the second part of (1) we note that $e = \phi(e) = \phi(gg^{-1}) \sim \phi(g)\phi(g^{-1})$. Thus, $\phi(g)\phi(g^{-1}) = e$ and $\phi(g^{-1}) = \phi(g)^{-1}$. The proof of part (2) is clear since ϕ sends classes in G to classes in H.

We now prove part (3). Let $g, h \in G$ be elements of the same coset of N in G. Then we have that $h^{-1}g \in N$ and $\phi(h^{-1}g) \in \phi(N)$. Since ϕ is a weak Cayley table isomorphism, $\phi(h^{-1}g)$ and $\phi(h^{-1})\phi(g)$ are conjugate in H. By part (1), $\phi(h^{-1})\phi(g) = \phi(h)^{-1}\phi(g)$. Thus $\phi(h^{-1}g)$ is conjugate to $\phi(h)^{-1}\phi(g)$ in H. Since $\phi(N)$ is normal in H by part (2), $\phi(h^{-1}g) \in \phi(N)$ implies that its conjugate $\phi(h)^{-1}\phi(g)$ is also in $\phi(N)$. Thus $\phi(g)\phi(N) = \phi(h)\phi(N)$ as required.

To prove part (5), let $x \in G$ be an involution so that $x^2 = e$. Then

$$\phi(x)^2 \sim \phi(x^2) = \phi(e) = e.$$

Thus $\phi(x)^2 = e$. Thus ϕ sends involutions in G to involutions in H. Suppose now that $\phi(x)$

is an involution in H. We show that x must be an involution in G. We have

$$e = \phi(x)^2 \sim \phi(x^2).$$

Thus, $\phi(x^2) = e$. But since $\phi(e) = e$ and the fact that ϕ is a bijection, we must have that $x^2 = e$. Thus x is an involution. □

Thus, a weak Cayley table isomorphism between two groups is a strictly stronger condition than merely having the same character tables. For example, it is a fact that the dihedral group D_8 and the quaternion group Q_8 have the same character table [14]. However, they do not have the same weak Cayley table since D_8 has five involutions and Q_8 has only one.

Definition 2.1.7. *A pair (G, N), with N a nontrivial, normal and proper subgroup of G, is a Camina pair if conjugacy classes of G in $G \setminus N$ are unions of cosets of N. We also say that G and N satisfy the Camina pair condition and that G is a Camina pair group.*

Example 2.1.8. *Let*

$$D_8 = \langle a, b | a^4 = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

The conjugacy classes of D_8 are $C_1 = \{e\}$, $C_2 = \{a^2\}$, $C_3 = \{a, a^3\}$, $C_4 = \{b, a^2b\}$ and $C_5 = \{ab, a^3b\}$. Let $N = Z(G) = \{e, a^2\}$. Then the conjugacy classes of G in $G \setminus N$ are cosets of N. Thus, (G, N) is a Camina pair.

Definition 2.1.9. *A group G is a Frobenius group if it has a nontrivial subgroup A such that $A \cap A^g = \{e\}$ for every $g \in G \setminus A$. The subgroup A is called the Frobenius complement of G.*

Suppose G is a Frobenius group with Frobenius complement A. Let N be the subset of G consisting of those elements that are not conjugate in G to any nonidentity element of A. Frobenius proved using character theory that N is always a subgroup of G [13]. A character-free proof is still unknown. Note also that since N is a subgroup, it must be a normal subgroup of G. The normal subgroup N is called the *Frobenius kernel* of G. By

definition of N, we have that $N \cap A = \{e\}$. Further, if G is a finite group, it is easy to show that $|N| = |G|/|A|$. Thus, A is the complement of the normal subgroup N in G.

Example 2.1.10. *Let $G = S_3$ and $A = \{(1), (12)\}$. The conjugates of A are $A = \{(1), (12)\}$, $A^{(13)} = \{(1), (23)\}$, and $A^{(23)} = \{(1), (13)\}$. Thus, the Frobenius kernel N is $\{(1), (123), (132)\}$. In this case, G is a Frobenius group with Frobenius kernel N and Frobenius complement A.*

2.2 Generalizing Johnson, Mattarei and Sehgal

We consider two groups G_1 and G_2 with normal subgroups N_1 and N_2, respectively, such that (G_1, N_1) and (G_2, N_2) are Camina pairs and investigate conditions under which G_1 and G_2 have the same weak Cayley table.

We first look at a result of Johnson, Mattarei and Sehgal [15].

Theorem 2.2.1. *(Johnson, Mattarei and Sehgal [15]) Suppose G is a group of odd order which acts on an abelian group N. Suppose further that G_1 and G_2 are nonisomorphic extensions of N by G such that (G_1, N) and (G_2, N) are Camina pairs. Then G_1 and G_2 have the same Cayley table.*

We note that the assumption that G has odd order is necessary for this result since D_8 and Q_8 are extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2 \times \mathbb{Z}_2$ and thus satisfy the other assumptions of the theorem but do not have the same weak Cayley table.

Our first immediate goal is to generalize this result. What if we weaken the requirement that $G_1/N \cong G_2/N$ and replace it instead with G_1/N and G_2/N having only the same weak Cayley table? Here is a result in this direction.

Theorem 2.2.2. *Let $N_i \trianglelefteq G_i$, for $i = 1, 2$ with $|G_i/N_i|$ odd. Suppose that the following conditions hold:*

(1) There exists a weak Cayley table isomorphism $\beta : H_1 = G_1/N_1 \to H_2 = G_2/N_2$;

(2) There exists a map $\alpha : N_1 \to N_2$ such that α sends classes of G_1 in N_1 to classes of G_2 in N_2 and $\alpha(n_1 n_2)$ is conjugate in G_2 to $\alpha(n_1)\alpha(n_2)$ for all $n_1, n_2 \in N_1$;

(3) (G_i, N_i) *is a Camina pair for* $i = 1, 2$.

Then G_1 *and* G_2 *have the same weak Cayley table.*

Proof. Since G_i is an extension of N_i by H_i, for $i = 1, 2$, we write $G_i = N_i \times H_i$ with multiplication defined as

$$(n_1, g_1)(n_2, g_2) = (n_1 n_2^{g_1^{-1}} f_i(g_1, g_2), g_1 g_2),$$

for some function f_i, for $i = 1, 2$. We may assume that $f_i(g, e) = f_i(e, g) = e$ for all $g \in H_i$.

We note that for an arbitrary element (n, g) of either group G_1 and G_2, we have that $(n, g)^{-1} = (m, g^{-1})$ for some $m \in N_i$. In addition, since $(n, g) = (n, e)(e, g)$ for all $n \in N_i, g \in H_i$, we have that $(n, g)(m, g)^{-1} = (n, e)(e, g)(e, g)^{-1}(m, e)^{-1} = (nm^{-1}, e)$.

We partition $H_1 \setminus \{e\}$ into subsets S_1 and S_2 such that $S_2 = \{g^{-1} : g \in S_1\}$. We can do this since $|H_i|$ is odd by assumption. Now we define the map $\phi : G_1 \to G_2$ as follows.

$$\begin{aligned}
\phi(n, e) &= (\alpha(n), e), \forall n \in N_1, \\
\phi(n, g) &= (\alpha(n), \beta(g)), \forall n \in N_1, g \in S_1, \\
\phi((n, g)^{-1}) &= (\alpha(n), \beta(g))^{-1}, \forall n \in N_1, g \in S_1.
\end{aligned}$$

We first show that ϕ preserves conjugacy classes. Clearly this is true for classes in N_1 by the hypothesis on α. For classes outside of N_1, by the Camina pair assumption, since β is a weak Cayley table isomorphism, classes of G_i are full preimages of conjugacy classes of $H_i = G_i/N_i$, which are preserved by β. Now we show $\phi((n_1, g_1)(n_2, g_2))$ is conjugate in G_2 to $\phi(n_1, g_1)\phi(n_2, g_2)$. We have three cases:

Case 1: $g_1 = g_2 = e$. Here

$$\phi((n_1, e)(n_2, e)) = \phi((n_1 n_2, e)) = (\alpha(n_1 n_2), e).$$

On the other hand,

$$\phi(n_1, e)\phi(n_2, e) = (\alpha(n_1), e)(\alpha(n_2), e) = (\alpha(n_1)\alpha(n_2), e).$$

These elements are conjugate since α is a weak Cayley table isomorphism.

Case 2: $g_1 \neq g_2^{-1}$. Here

$$\begin{aligned}\phi((n_1, g_1)(n_2, g_2)) &= \phi(n_1 n_2^{g_1^{-1}} f_1(g_1, g_2), g_1 g_2) \\ &= (\alpha(n_1 n_2^{g_1^{-1}} f_1(g_1, g_2)), \beta(g_1 g_2)).\end{aligned}$$

On the other hand,

$$\begin{aligned}\phi(n_1, g_1)\phi(n_2, g_2) &= (\alpha(n_1), \beta(g_1))(\alpha(n_2), \beta(g_2)) \\ &= (\alpha(n_1)\alpha(n_2)^{\beta(g_1)^{-1}} f_2(\beta(g_1), \beta(g_2)), \beta(g_1)\beta(g_2)).\end{aligned}$$

These elements are conjugate since β is a weak Cayley table isomorphism on the quotient and (G_2, N_2) is a Camina pair.

Case 3: $g_2 = g_1^{-1} \neq e$. Without loss of generality, assume $g_1 \in S_1$. Write $(n_2, g_2) = (n, g_1)^{-1}$ for some $n \in N_1$. Then

$$\begin{aligned}\phi((n_1, g_1)(n_2, g_2)) &= \phi((n_1, g_1)(n, g_1)^{-1}) \\ &= \phi(n_1 n^{-1}, e) = (\alpha(n_1 n^{-1}), e).\end{aligned}$$

Also,

$$\begin{aligned}\phi(n_1, g_1)\phi(n_2, g_2) &= \phi(n_1, g_1)\phi((n, g_1)^{-1}) \\ &= (\alpha(n_1), \beta(g_1))(\alpha(n), \beta(g_1))^{-1} \\ &= (\alpha(n_1)\alpha(n)^{-1}, e) = (\alpha(n_1)\alpha(n^{-1}), e).\end{aligned}$$

Thus these elements are also conjugate by the assumption on α. Hence, G_1 and G_2 have the same weak Cayley table. □

The following corollary follows directly from the theorem.

Corollary 2.2.3. *Suppose (G_1, N_1) and (G_2, N_2) are Camina pairs with $|G_i/N_i|$ odd and $N_1 \cong N_2$, $G_1/N_1 \cong G_2/N_2$. Suppose also that classes of G_1 in N_1 correspond to classes of G_2 in N_2 after identifying N_1 and N_2. Then G_1 and G_2 have the same weak Cayley table.*

Here is another generalization of Theorem 2.2.1 that will be useful.

Theorem 2.2.4. *(Johnson, Mattarei and Sehgal, [15, Theorem 4.1]) Let G_i be an extension of H_i by the abelian normal subgroup N such that the conjugacy classes of G_1 which lie in N are the same as the conjugacy classes of G_2 in N. Suppose that H_1 and H_2 have the same weak Cayley table via $\alpha : H_1 \to H_2$ with $n^x = n^{\alpha(x)}$ for all $n \in N$, $x \in H_i$. Suppose that (G_1, N) and (G_2, N) are Camina pairs. Finally, having fixed a representation for each G_i as an extension of H_i by N, suppose that for every involution $x \in H_1$, we have $(e, x)^2 = (e, \alpha(x))^2$. Then G_1 and G_2 have the same weak Cayley table.*

2.3 Camina's Theorem

In this section, we state a theorem of Camina and deduce some results. Suppose G is a group with a proper non-trivial normal subgroup N such that (G, N) is a Camina pair. Camina [2] shows that G must satisfy one of three conditions.

Theorem 2.3.1. *(Camina [2]) Let G be a group with a non-trivial proper normal subgroup N satisfying the Camina pair condition. Then G satisfies one of the following conditions:*

(1) G is a Frobenius group with kernel N,

(2) N is a p-group for some prime p, or

(3) G/N is a p-group for some prime p.

Now suppose (G_i, N_i) for $i = 1, 2$ are Camina pairs. From the conclusions of Camina's theorem, we will attempt to answer the following two questions:

(1) If we suppose further that G_1 and G_2 are Frobenius groups, what further assumptions do we need to guarantee that they have the same weak Cayley table?

(2) If instead G_1/N_1 and G_2/N_2 are p-groups, what are some sufficient conditions to guarantee that the two groups have the same weak Cayley table?

To answer the first question, we have this result due to Johnson, Mattarei and Sehgal in [15] but without proof. We fill in the proof below.

Corollary 2.3.2. *Let G_1, G_2 be Frobenius groups with kernels $N_1 \cong N_2$ and $H_1 = G_1/N_1 \cong G_2/N_2 = H_2$. Assume also that classes of G_1 in N_1 coincide with classes of G_2 in N_2. Then G_1, G_2 have the same weak Cayley table.*

Proof. If $|G_i/N_i|$ is odd, the assumptions of the theorem satisfy the first two conditions Theorem 2.2.2. Since G_1, G_2 are both Frobenius groups with kernels N_1 and N_2, respectively, we have that (G_1, N_1) and (G_2, N_2) are Camina pairs. Thus all of the assumptions of Theorem 2.2.2 are satisfied and the conclusion follows.

If $|G_i/N_i|$ is even, then by 12.6.19 of Scott [18], N_1 and N_2 are abelian subgroups. Moreover, by Theorem 6.3 of Isaacs [12], H_1 and H_2 each has a unique involution. Suppose x_i is the unique involution in H_i. Since G_i are Frobenius groups, $C_{G_i}(x_i) \subseteq H_i$ and we have that each x_i must act by inversion on N_i. Thus all the assumptions of Theorem 2.2.4 are satisfied and the conclusion follows. □

Chillag and Macdonald [3] showed that if (G, N) is a Camina pair, then requiring that G be a Frobenius group is equivalent to requiring that G is a split extension of N. Thus, we have this corollary, part of whose proof follows their argument.

Corollary 2.3.3. *Suppose N and H are finite groups. Suppose that G_1 and G_2 are split extensions of N by H such that (G_i, N) for $i = 1, 2$ are Camina pairs. If the conjugacy classes in N of G_1 and G_2 coincide, then G_1 and G_2 have the same weak Cayley table.*

Proof. Let G be any split extension of N by H satisfying the assumptions of the corollary. We can write $G = HN$, with $N \cap H = \{1\}$ and $N \triangleleft G$. Fix $h \neq e$, $h \in H$. Let $e \neq n \in N$. Since (G, N) is a Camina pair, h is conjugate to hn. Suppose $h^m = hn$, where $m = m_1 m_2, m_1 \in H, m_2 \in N$. Then

$$n = h^{-1}h^{m_1 m_2} = h^{-1}m_2^{-1}hm_2(h^{-1}m_1^{-1}hm_1)^{m_2}. \tag{2.1}$$

Since N normal in G, $h^{-1}m_2^{-1}hm_2 \in N$. Also, $n, m_2 \in N$ and 2.1 implies that $h^{-1}m_1^{-1}hm_1 \in N$. But $h^{-1}m_1^{-1}hm_1$ is also in H. We have $h^{-1}m_1^{-1}hm_1 \in N \cap H = \{1\}$. Thus, from 2.1, we have $nm_2^{-1} = h^{-1}m_2^{-1}h$. Since $n \neq e$, we have $m_2 \neq e$. Now let $n' = h^{-1}m_2'^{-1}hm_2$ for some $m_2' \in N$. Clearly, if $n \neq n'$, then $m_2 \neq m_2'$. Thus as n varies over $N \setminus \{1\}$, we have that conjugating by h for all $h \in H \setminus \{1\}$ on $N \setminus \{1\}$ is fixed-point free. Thus G is Frobenius with kernel N and complement H. This shows that G_1 and G_2 are both Frobenius groups with kernel N and complement H. The result follows from the previous corollary. □

To answer the second question above, that is, assuming further that G_i/N_i for $i = 1, 2$ are p-groups, we have the following result.

Theorem 2.3.4. *Suppose (G_1, N_1) and (G_2, N_2) are Camina pairs with $N_1 \cong N_2$ such that $|G_i/N_i|$ is an abelian p-group for $i = 1, 2$ and that the classes of G_1 in N_1 coincide with classes of G_2 in N_2 after identifying N_1 and N_2. Suppose further that G_i is neither a p-group nor a Frobenius group with kernel N_i, $i = 1, 2$. Then G_1 and G_2 have the same weak Cayley table.*

Proof. Let H_i be the Sylow p-subgroup of G_i, $i = 1, 2$. It's easy to see that $G_i = N_i H_i$. We first prove that $(H_i, H_i \cap N_i)$ is a Camina pair. We do this by showing $|C_{H_i}(g)| =$

$|C_{H_i/H_i\cap N_i}(g(H_i \cap N_i))|$. We have

$$\begin{aligned} |C_{H_i}(g)| &\leq |C_{G_i}(g)| \\ &= |C_{G_i/N_i}(gN_i)| \\ &= |C_{H_i/H_i\cap N_i}(g(H_i \cap N_i))| \\ &\leq |C_{H_i}(g)|, \end{aligned}$$

where the last inequality is given by Corollary 2.24 of Isaacs [13]. Thus, $(H_i, H_i \cap N_i)$ is a Camina pair.

We now prove that (H_i, H_i') is also a Camina pair where H_i' is the commutator subgroup of H_i. We do this by showing that $H_i \cap N_i = H_i'$. By the second isomorphism theorem, $N_iH_i/N_i \cong H_i/N_i \cap H_i$. But since $N_iH_i/N_i = G_i/N_i$ is an abelian group, we have that $H_i' \leq N_i \cap H_i$.

Lemma 2.1 of Macdonald [17] is useful at this point. We first define some notation. We write $G^1 = G$, $G^2 = [G, G]$ and in general, $G^k = [G^{k-1}, G]$ for $k > 2$. This series of subgroups of G is called the *lower central series* of G.

Lemma 2.3.5. *[17, Lemma 2.1] If (G, N) is a Camina pair and G has nilpotence class c then $N = G^r$ for some r satisfying $1 < r \leq c$.*

Since H_i is a finite p-group and $(H_i, H_i \cap N_i)$ is a Camina pair, by Lemma 2.3.5, we have $H_i \cap N_i = H_i^r$. Thus, $H_i \cap N_i \leq H_i'$ and so $H_i \cap N_i = H_i'$. We have that (H_i, H_i') is a Camina pair as required.

We now appeal to the main result of Dark [5] and Theorem 3 of Chillag, Mann and Scoppola [4].

Theorem 2.3.6. *(Dark [5]) If G is a finite p-group such that (G, N) is a Camina pair for some subgroup N and $G' = N$, then $G^4 = 1$.*

Theorem 2.3.7. *(Chillag, Mann, Scoppola [4]) Let (G, N) be a Camina pair with G/N a*

p-group and let $P \in Syl_p(G)$. Assume that the nilpotence class of P is at most 4. Then G is a Frobenius group with complement Q_8 and N is a subgroup of index 4 in G.

Thus, by Theorem 2.3.6, H_i has nilpotence class of at most 3. By Theorem 2.3.7 above, G_i is a Frobenius group with complement Q_8 and N_i is a subgroup of index 4. Let K_i be the kernel of G_i. Since N_i is normal in G, by [18, Theorem 12.6.8], either $N_i \leq K_i$ or $K_i \leq N_i$. Since N_i has index 4 and K_i has index 8, we have that $K_i \leq N_i$ with $|N_i : K_i| = 2$.

Then N_i is Frobenius with kernel K_i. Thus, after identifying N_1 with N_2, we have $K_1 \cong K_2$. And since Q_8 is a complement of both G_1 and G_2, by Corollary 2.3.2 above, G_1 and G_2 have the same weak Cayley table. □

2.4 Weak Cayley Table Isomorphisms and Derivations

We begin with some notation from Dummit and Foote [8, Chapter 17.2]. Let G be a finite group. Let A be an abelian group, written additively, on which G acts as automorphisms. In this case, we say that A is a *G-module*. Define $C^0(G, A) = A$ and for $n \geq 1$ define $C^n(G, A)$ to be the collection of all maps from $G^n = G \times \cdots \times G$ to A. The elements of $C^n(G, A)$ are called *n-cochains*. Each set $C^n(G, A)$ is an additive abelian group given by the usual pointwise addition of functions.

Definition 2.4.1. *For $n \geq 0$, define the n^{th} coboundary homomorphism from $C^n(G, A)$ to $C^{n+1}(G, A)$ by*

$$B_n(f)(g_1, ..., g_{n+1}) =$$
$$g_1 \cdot f(g_2, ..., g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, ..., g_{i-1}, g_i g_{i+1}, g_{i+2}, ..., g_{n+1}) + (-1)^{n+1} f(g_1, ..., g_n),$$

where the product $g_i g_{i+1}$ occupies the i^{th} position in G^n.

It is immediate from the above definition that the B_n are group homomorphisms and $B_n \circ d_{n-1} = 0$ for $n \geq 1$.

Definition 2.4.2. *(1) Let $Z^n(G, A) = ker(B_n)$ for $n \geq 0$. The elements of $Z^n(G, A)$ are called n-cocycles.*

(2) Let $B^n(G,A) = Image(d_{n-1})$ *for* $n \geq 1$ *and* $B^0(G,A) = 1$. *The elements of* $B^n(G,A)$ *are called n-coboundaries.*

The elements of $Z^1(G,A)$, the 1-cocyles, are also called *derivations*. It is easy to check $f : G \to A$ is a derivation if and only if $f(gh) = f(g) + g \cdot f(h)$ for all $g, h \in G$. The elements of $B^1(G,A)$, the 1-coboundaries, are also called *principal derivations*. In this case, f is a 1-coboundary if there exists an $a \in A$ such that $f(g) = g \cdot a - a$ for all $g \in G$.

Since $B_n \circ d_{n-1} = 0$ for $n \geq 1$ we have that $Image(d_{n-1}) \subset ker(B_n)$. Thus $B^n(G,A)$ is a subgroup of $Z^n(G,A)$.

Definition 2.4.3. *For any G-module A, the quotient group* $Z^n(G,A)/B^n(G,A)$ *is called the* n^{th} *cohomology group of G with coefficients in A and is denoted* $H^n(G,A)$, $n \geq 0$.

It is a fact (see Brown [1, Chapter IV]) that A-conjugacy classes of splittings of the split extension $0 \to A \to A \rtimes G \to G \to 1$ are in 1-1 correspondence with the elements of $H^1(G,A) = Z^1(G,A)/B^1(G,A)$, in other words, the classes of derivations modulo principal derivations.

We now apply the notation above to the following context. Suppose G is a finite group. Define $\mathcal{W}(G)$ to be the group of weak Cayley table isomorphisms from G to G. Fix an abelian subgroup N of G. Let $A(G)$ denote the abelian group of all functions $G \to N$. Let $W_N(G)$ be the group of all $\phi \in \mathcal{W}(G)$ such that there exists a function $\delta(\phi) : G \to N$ such that

$$\phi(g) = g\delta(\phi)(g), \text{ for all } g \in G.$$

Assume also that $\delta(\phi) : G \to N$ is constant on the N cosets of G. We note that δ defines a function from $W_N(G)$ to $A(G), \phi \mapsto \delta(\phi)$.

Example 2.4.4. *For* $G = G_{27,3}$ *(in Magma notation), the non-abelian group of order* 27 *and exponent* 3 *and with* $N = Z(G)$, $W_N(G)$ *has* 54 *elements where* $N = Z(G)$.

Lemma 2.4.5. *Let G be a group with an abelian subgroup* $N \leq G$. *For* $\phi_1, \phi_2 \in W_N(G)$ *and* $g \in G$, *we have*

$$\delta(\phi_2\phi_1)(g) = \delta(\phi_1)(g) \cdot \delta(\phi_2)(g).$$

Proof. On the one hand, $(\phi_2\phi_1)(g) = g\delta(\phi_2\phi_1)(g)$. On the other hand, we have

$$\begin{aligned}(\phi_2\phi_1)(g) &= \phi_2(\phi_1(g)) = \phi_2(g\delta(\phi_1)(g)) \\ &= g\delta(\phi_1)(g) \cdot \delta(\phi_2)(g\delta(\phi_1)(g)) = g\delta(\phi_1)(g) \cdot \delta(\phi_2)(g),\end{aligned}$$

where the last equality follows from the fact that $\delta(\phi)$ is constant on the N cosets of G. Cancelling the g on both sides gives the identity. □

Now we define an action of $W_N(G)$ on $A(G)$. For $\phi \in W_N(G)$ and $\mu \in A(G)$ define $\phi \cdot \mu \in A(G)$ by

$$(\phi \cdot \mu)(g) = \mu(\phi(g)) \text{ for all } g \in G.$$

We show that this is indeed an action. To do this, we show that $(\phi_2\phi_1)\cdot(\mu) = \phi_2\cdot(\phi_1\cdot(\mu))$. Fixing $g \in G$, we have

$$\begin{aligned}(\phi_2\phi_1) \cdot (\mu)(g) &= \mu((\phi_2\phi_1)(g)) = \mu(g\delta(\phi_2\phi_1)(g)) \\ &= \mu(g\delta(\phi_1)(g) \cdot \delta(\phi_2)(g)).\end{aligned}$$

But we also have

$$\begin{aligned}\phi_2 \cdot (\phi_1 \cdot (\mu))(g) &= \phi_1 \cdot \mu(\phi_2(g)) = \mu(\phi_1\phi_2(g)) \\ &= \mu(g\delta(\phi_1\phi_2)(g)) = \mu(g\delta(\phi_1)(g) \cdot \delta(\phi_2)(g)),\end{aligned}$$

as required.

The proof of Lemma 2.4.5 also shows us that

$$\delta(\phi_2\phi_1) = \delta(\phi_1) \cdot \phi_1(\delta(\phi_2)),$$

that is, $\delta : W_N(G) \to A(G)$ is a derivation. Thus, the natural question is whether δ is a principal derivation, in other words, whether it is a trivial element of the cohomology group. The answer is "yes". Here is the precise statement and proof.

Proposition 2.4.6. *Suppose G is a finite group and N is an abelian subgroup of G. Then $\delta : W_N(G) \to A(G)$ defined above is a principal derivation.*

Proof. We show that there exists $\mu \in A(G)$ such that

$$\delta(\phi)(g) = \mu(\phi(g))\mu(g)^{-1}, \text{ for all } \phi \in W_N(G).$$

Pick a set T of representatives for left cosets of N in G, say $T = \{h_1 = e, h_2, ..., h_m\}$. For each $g \in G$, write $g = h_i n$, for some $h_i \in T$ and $n \in N$. Define $\mu : G \to N$ by

$$\mu(g) = \mu(h_i n) = n.$$

Let $\phi \in W_N(G)$, so that $\phi(g) = g\delta(\phi)(g)$. We show that $\delta(\phi)(g) = \mu(\phi(g))\mu(g)^{-1}$, or equivalently,

$$\phi(g) = g\mu(\phi(g))\mu(g)^{-1}.$$

We have

$$\begin{aligned} g\mu(\phi(g))\mu(g)^{-1} &= g\mu(g\delta(\phi)(g))\mu(g)^{-1} = g\mu(h_i n\delta(\phi)(g))\mu(g)^{-1} \\ &= gn\delta(\phi)(g)\mu(g)^{-1} = gn\delta(\phi)(g)\mu(h_i n)^{-1} \\ &= gn\delta(\phi)(g)n^{-1} = g\delta(\phi)(g) = \phi(g), \end{aligned}$$

as required. □

The above discussion also gives rise to the following question: Given a finite group G with a subgroup N, can we always find a map $\delta \in A(G)$ such that $\phi(g) = g\delta(g)$ is a weak Cayley table isomorphism between G and G?

We indicate one situation where this is possible.

Proposition 2.4.7. *Let G be a finite group such that $(G, Z(G))$ is a Camina pair. Suppose $\delta : G \to Z(G)$ is a function satisfying*

(1) $\delta(g) = e$ for all $g \in Z(G)$;

(2) δ is constant on $Z(G)$ cosets of G;

(3) For all $g, h \notin Z(G)$ and $gh \in Z(G)$, then $\delta(g)\delta(h) = e$.

Then $\phi : G \to G$ defined by $\phi(g) = g\delta(g)$ is a weak Cayley table isomorphism.

Proof. Because $(G, Z(G))$ is a Camina pair, ϕ clearly sends classes to classes. We show that for $g, h \in G$, $\phi(gh) \sim \phi(g)\phi(h)$. There are four cases:

Case 1: $g, h \in Z(G)$. We have $\phi(gh) = gh = \phi(g)\phi(h)$.

Case 2: $g \in Z(G), h \notin Z(G)$. Since $gh \notin Z(G)$, $\phi(gh) = gh\delta(gh)$. Also $\phi(g)\phi(h) = gh\delta(h)$. But $gh\delta(h) \sim gh\delta(gh)$ since $(G, Z(G))$ is a Camina pair, and so we are done.

Case 3: $g, h \notin Z(G)$ and $gh \notin Z(G)$. On the one hand, $\phi(gh) = gh\delta(gh)$. On the other hand, $\phi(g)\phi(h) = g\delta(g)h\delta(h) = gh\delta(g)\delta(h)$, where the last equality follows because $\delta(g), \delta(h) \in Z(G)$. Thus $\phi(gh) \sim \phi(g)\phi(h)$ since $(G, Z(G))$ is a Camina pair.

Case 4: $g, h \notin Z(G)$ and $gh \in Z(G)$. In this case, $\phi(gh) = gh$ since $gh \in Z(G)$. And $\phi(g)\phi(h) = g\delta(g)h\delta(h) = gh\delta(g)\delta(h)$. But by assumption $\delta(g)\delta(h) = e$. Thus $\phi(gh) = \phi(g)\phi(h)$. □

Example 2.4.8. *For $G = G_{27,3}$, let $Z(G) = \langle z \rangle$ and write $G = Z(G) \cup g_1 Z(G) \cup g_1^{-1} Z(G) \cup \cdots \cup g_4 Z(G) \cup g_4^{-1} Z(G)$. Let $\epsilon_1, \ldots, \epsilon_4 \in \{\pm 1\}$. Now define*

$$\delta(z) = e, \forall z \in Z(G);$$

$$\delta(g_i z^j) = z^{\epsilon_i}, \forall i = 1, \ldots, 4;$$

$$\delta(g_i^{-1} z^j) = z^{-\epsilon_i}, \forall i = 1, \ldots, 4.$$

Then δ satisfies Proposition 2.4.7.

Chapter 3. Weak Cayley Table Groups

3.1 Introduction

The set of all weak Cayley table isomorphisms $\phi : G \to G$ forms a group which we denote by $\mathcal{W}(G)$.

Example 3.1.1. *Any automorphism $\phi : G \to G$ is a weak Cayley table isomorphism and thus is an element of $\mathcal{W}(G)$.*

Example 3.1.2. *An anti-automorphism is a bijective map $\phi : G \to G$ such that $\phi(gh) = \phi(h)\phi(g)$ for all $g, h \in G$. Any anti-automorphism is a weak Cayley table isomorphism.*

Example 3.1.3. *The inverse map $\mathcal{I} : G \to G$, defined by*

$$\mathcal{I}(x) = x^{-1},$$

is an anti-automorphism and hence a weak Cayley table isomorphism.

Fact 3.1.4. *Let ϕ be an anti-automorphism. Then ϕ can be written in the form $\phi = \mathcal{I}\psi$, where $\mathcal{I}$ is the inverse map above and ψ is some automorphism of G.*

Definition 3.1.5. *A weak Cayley table isomorphism is trivial if it is either an automorphism or an anti-automorphism. Further, we say that $\mathcal{W}(G)$ is trivial if it consists of only trivial weak Cayley table isomorphisms.*

Let $\mathcal{W}_0(G)$ denote the subgroup of $\mathcal{W}(G)$ of trivial weak Cayley table isomorphisms, that is, $\mathcal{W}_0(G) = \langle Aut(G), \mathcal{I} \rangle$, where $\mathcal{I}$ is the inverse map.

Thus the group $\mathcal{W}(G)$ is trivial if $\mathcal{W}(G) = \mathcal{W}_0(G)$, where $\mathcal{W}_0(G) = \langle Aut(G), \mathcal{I} \rangle$.

We now give two examples of groups for which there exist nontrivial weak Cayley table isomorphisms.

Example 3.1.6. *Let $G = A_4$, the alternating group of degree 4. Since $Aut(A_4) \cong S_4$, we have that $|\mathcal{W}_0(G)| = 48$. But a Magma calculation shows that $|\mathcal{W}(G)| = 288$. Thus there exists nontrivial weak Cayley table isomorphisms for this group.*

Example 3.1.7. *Let $G = \langle a, b \,|\, a^5 = b^4 = 1, bab^{-1} = a^2 \rangle$, which is a group of order 20. Using Magma, we have $|Aut(G)| = 20$ and so $|\mathcal{W}_0(G)| = |\langle Aut, \mathcal{I} \rangle| = 40$. But $|\mathcal{W}(G)| = 57,600$.*

Humphries [11] proved the following important result.

Theorem 3.1.8. *For $n \geq 1$, the group $\mathcal{W}(S_n)$ is trivial.*

Humphries' proof used the following lemma.

Lemma 3.1.9. *Suppose that G is a group containing a nontrivial conjugacy class C such that $G = \langle C \rangle$. Suppose also that for every $\alpha \in \mathcal{W}(G)$, there is an $\phi \in \mathcal{W}_0(G)$ such that the following four statements are true:*

(1) $\phi\alpha(x) = x$ for all $x \in C$;

(2) $\phi\alpha(x) = x$ for all $x \in C^2$;

(3) $\phi\alpha(x) = x$ for all $x \in C^3$;

(4) for all $x, y \in G$ with $x \sim y, x \neq y$, there is a $c \in C \cup C^2$ such that $cx \nsim cy$.

Then $\mathcal{W}(G)$ is trivial.

Proof. We replace $\phi\alpha$ by ϕ in the proof below. Let λ be the length function for G relative to the generating set C. Let $x \in G$ be a shortest word such that $y = \phi(x) \neq x$, is such a word exists. Then $\lambda(x) > 2$ by assumptions (1) and (2), and we can write $x = x'c$ where $c \in C$ and $\lambda(x') < \lambda(x)$. Then we have $\phi(x') = x'$ and so

$$y = \phi(x'c) \sim \phi(x')\phi(c) = x'c = x.$$

Thus by hypothesis (4), there is a $d \in C \cup C^2$ such that $dy \nsim dx$. However, using hypothesis (3) we also have

$$yd \sim \phi(xd) = \phi(x'cd) \sim \phi(x')\phi(cd) = x'cd = xd.$$

This contradiction gives the result. □

Humphries applied this lemma to $G = S_n$ and C the class of transpositions (i, j) in S_n to show that $\mathcal{W}(S_n)$ is trivial. We wish to generalize his methods to show that $\mathcal{W}(A_n)$ is trivial. We do this in the next section.

3.2 The Alternating Groups A_n

In generalizing Humphries' methods, we first observe that his lemma, Lemma 3.1.9, can be slightly modified as follows: Suppose we can pick c in (4) to be in C instead of $C \cup C^2$, then from the proof, we can drop hypothesis (3) thus simplifying our calculations.

We further note that his method for showing hypothesis (1) does not carry over to the groups A_n. This observation leads us to use a different technique to prove hypothesis (1), namely analyzing graph automorphisms.

Theorem 3.2.1. *For $n \geq 5$, the group $\mathcal{W}(A_n)$ is trivial.*

Proof. We first show that for C the class of (i, j, k), hypothesis (1) of Lemma 3.1.9 is satisfied.

Proposition 3.2.2. *Let C be the class of all 3-cycles. Suppose that $\phi : A_n \to A_n$, $n \geq 5$, is a weak Cayley table isomorphism. Then up to composing with a trivial weak Cayley table isomorphism, we have that $\phi(x) = x$ for all $x \in C$.*

Proof. We show that $\phi(C) = C$. We use a counting argument. For $5 \leq n \leq 8$, we can check by Magma that C is the unique smallest class with its size. We next show that for $n \geq 9$, C is the unique smallest size class in A_n. Since weak Cayley table isomorphisms sends classes to classes of the same size, we then have that $\phi(C) = C$.

The class C has $2\binom{n}{3} = \dfrac{n(n-1)(n-2)}{3}$ elements. Suppose $g \in A_n$ contains a k-cycle,

where $k > 3$. Then there exists at least

$$(k-1)!\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k}$$

elements in the class of g. Thus, to show that the class of g is larger than the class of C, we show that

$$\frac{n(n-1)\cdots(n-k+1)}{k} > \frac{n(n-1)(n-2)}{3},$$

or equivalently,

$$\frac{(n-3)(n-4)\cdots(n-k+1)}{k} > \frac{1}{3}.$$

We will show, in fact, that

$$\frac{(n-3)(n-4)\cdots(n-k+1)}{k} > 1. \tag{3.1}$$

Thus, it suffices to show that the numerator of the left term of Equation 3.1 is larger than k. If $k = 4$, then this is clearly true. For $k > 4$, the numerator has at least two terms. Since $n \geq 9$, we have

$$(n-3)(n-4)\cdots(n-k+1) > (n-3)(n-4) > (n-3)2 > n \geq k,$$

as required.

This shows that the class of g is bigger than then class of C if g has a k-cycle where $k > 3$. Now if g has at least two 3-cycles in its decomposition then its size is at least $2\binom{n}{3}\binom{n-3}{3} > 2\binom{n}{3}$. Similarly, if g has a 3-cycle and at least one 2-cycle. Finally, suppose g has all 2-cycles. If g has m 2-cycles where $m \geq 2$, then its class size is

$$\frac{n(n-1)\cdots(n-(2m-1))}{2\cdot 4\cdots(2m)}.$$

Thus, it suffices to show that

$$\frac{(n-3)(n-4)\cdots(n-(2m-1))}{2\cdot 4\cdots(2m)} > \frac{1}{3}.$$

We will show that

$$\frac{(n-3)(n-4)\cdots(n-(2m-1))}{2\cdot 4\cdots(2m)} > 1. \tag{3.2}$$

Let N and D denote the numerator and denominator of the left term of Equation 3.2, respectively. Since N is a product of $2m-3$ consecutive terms and D is a product of m consecutive even terms, it is easy to see that that $N > D$. Thus C is the smallest size class as required.

We now create a graph, Γ. Let the *vertex set* of Γ be the set of subsets $\{x, x^{-1}\}$ where x is a 3-cycle. If $x = (i, j, k)$, then we identify the vertex $\{x, x^{-1}\}$ with the set $\{i, j, k\}$. Thus, we will view this vertex set as the set of all size 3 subsets of $\{1, 2, ..., n\}$. Two vertices are connected by an *edge* in Γ if they have two elements in common.

We now observe that Γ is a connected graph. For any two vertices, $\{a, b, c\}$ and $\{d, e, f\}$, with $\{a, b, c\} \cap \{d, e, f\} = \emptyset$, we have the following path connecting them: $\{a, b, c\} \to \{d, a, b\} \to \{d, e, a\} \to \{d, e, f\}$. The cases where $\{a, b, c\} \cap \{d, e, f\} \neq \emptyset$ are similar.

Lemma 3.2.3. *Any weak Cayley table isomorphism ϕ of A_n acts as an automorphism of the graph Γ.*

Proof. Since $\phi(g^{-1}) = \phi(g)^{-1}$, ϕ sends vertices to vertices. We now show that if x and y are adjacent, then $\phi(x)$ and $\phi(y)$ are adjacent. Write $x = (a, b, c)$ and $y = (c, b, d)$, with a, b, c, d all distinct. Since $\phi(C) = C$, by conjugating, if necessary, we can change ϕ so that we can assume $\phi(x) = (a, b, c)$. Suppose $\phi(y) = (i, j, k)$. We have $\phi(xy) = \phi((a, b, c)(c, b, d)) = \phi(a, d, c) \in C$. But$\phi(xy) \sim \phi(x)\phi(y) = (a, b, c)(i, j, k)$. Thus $(a, b, c)(i, j, k)$ must be a 3-cycle. But this is true only if $|\{a, b, c\} \cap \{i, j, k\}| = 2$ or if $(i, j, k) = (a, b, c)$, which can not happen. So we have that $\phi(x)$ is adjacent to $\phi(y)$. Thus, ϕ preserves adjacency in the graph Γ and ϕ acts as an automorphism of Γ. □

Certainly, the action of conjugating by an element of S_n is an automorphism of Γ. By [6], these make up all of the automorphism of Γ. Thus, we have that ϕ acts on Γ as a conjugation by some element g of S_n. By conjugating by g^{-1}, we may assume that ϕ acts as the identity on Γ.

Thus, $\phi((i,j,k)) \in \{(i,j,k),(i,k,j)\}$, for all i,j,k. Now we show that $\phi((i,j,k)) = (i,j,k)$, for all i,j,k.

Lemma 3.2.4. *Suppose x and y are adjacent vertices with $x = \{(a,b,c),(a,c,b)\}$ and $y = \{(a,b,d),(a,d,b)\}$. Suppose further that $\phi((a,b,c)) = (a,b,c)$ and $\phi((a,c,b)) = (a,c,b)$. Then $\phi((a,b,d)) = (a,b,d)$ and $\phi((a,d,b)) = (a,d,b)$.*

Proof. By assumption $\phi((a,b,c)) = (a,b,c)$ and $\phi((a,c,b)) = (a,c,b)$. It suffices to show that $\phi((a,b,d)) = (a,b,d)$. We proved above that $\phi((a,b,d)) \in \{(a,d,b),(a,b,d)\}$. We have $\phi((a,c,b)(a,b,d)) = \phi((a,c,d)) \in C$. But

$$\phi((a,c,b)(a,b,d)) \sim \phi((a,c,b))\phi((a,b,d)) = (a,c,b)\phi((a,b,d)).$$

Thus, we have that $(a,c,b)\phi((a,b,d))$ is a 3-cycle. And since $(a,c,b)(a,d,b) = (a,c)(d,b)$ is not a 3-cycle, we must have that $\phi((a,b,d)) = (a,b,d)$. □

Repeating the argument of the lemma above, we see that if ϕ acts as the identity on a particular vertex x then ϕ acts as the identity on all vertices that are path connected to x. But this completes the proof of the proposition since the graph Γ is connected and we may assume up to a conjugation that $\phi((123)) = (123)$ and $\phi(132) = (132)$. □

We now show that hypothesis (2) of Lemma 3.1.9 is satisfied.

Proposition 3.2.5. *Assuming the hypotheses of the previous proposition, we have that $\phi(x) = x$ for all $x \in C^2$.*

Proof. Since C is the class of 3-cycles, we have that the elements of C^2 are one of the following four types: 5-cycles, type 2-2, 3-cycles and type 3-3.

We first show that $\phi(x) \sim x$ for all $x \in C^2$. Write $x = cd$ where $c, d \in C$. By the previous proposition, we have that $\phi(c) = c$ and $\phi(d) = d$. Thus, $\phi(x) = \phi(cd) \sim \phi(c)\phi(d) = cd = x$ as required.

By the previous proposition, we have shown that ϕ fixes all 3-cycles. We now show that ϕ fixes all 5-cycles. Suppose g is a 5-cycle. Without loss of generality, write $g = (12345)$. Since $\phi(x) \sim x$, we have that $\phi(x)$ is a 5-cycle.

Write $\phi((12345)) = (i, j, k, l, m)$. We have

$$\phi((12345)(132)) \sim \phi((12345))(132) = (i, j, k, l, m)(132).$$

But $\phi((12345)(132)) = \phi((345)) = (345)$. Thus, $(i, j, k, l, m)(132)$ is a 3-cycle. We have then that $\{1, 2, 3\} \cap \{i, j, k, l, m\} = \{1, 2, 3\}$. Moreover, $(i, j, k, l, m)(132)$ is a 3-cycle only if (i, j, k, l, m) has the form $(1, 2, 3, l, m)$. By a similar argument using (354) instead of (132), we see that $\{l, m\} = \{4, 5\}$ and that $(1, 2, 3, l, m)(354)$ is a 3-cycle only if $(1, 2, 3, l, m) = (12345)$. Thus, $\phi((12345)) = (12345)$.

We now show that ϕ fixes 2-2 types. Without loss, we show that $\phi((12)(34)) = (12)(34)$. By arguing as before, we see that $\phi((12)(34)) = (i, j)(k, l)$. Since $(12)(34)(123) = (134)$, we have that $(i, j)(k, l)(123)$ is a 3-cycle. We can then check that $\{i, j, k, l\} \cap \{1, 2, 3\} = \{1, 2, 3\}$. Similarly, by multiplying by (234), we have that $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Since we just proved $\phi((12345)) = (12345)$ and $(12)(34)(12345)$ is a 3-cycle, we must have that $(i, j)(k, l)(12345)$ is a 3-cycle. This happens only if $(i, j)(k, l) = (12)(34)$.

Finally, we show $\phi((123)(456)) = (123)(456)$. Since

$$(123) = \phi((123)) = \phi((123)(456)(654)) \sim (i, j, k)(l, m, n)(654),$$

we have that $\phi((i, j, k)(l, m, n)(654)$ is a 3-cycle. We then have that $\{i, j, k, l, m, n\} \cap \{6, 5, 4\} = \{6, 5, 4\}$. Similarly, by multiplying by (321), we have that $\{i, j, k, l, m, n\} = \{1, 2, 3, 4, 5, 6\}$. By similar computations as above, we have that $(i, j, k)(l, m, n) = (123)(456)$,

as required.

Thus, we have that $\phi(x) = x$ for all $x \in C^2$. □

To finish the proof of the theorem, we prove the following proposition.

Proposition 3.2.6. *Suppose $x, y \in A_n$ with $x \neq y$ and $x \sim y$. Then there exists $c \in C$ such that $cx \nsim cy$.*

Proof. We consider the disjoint cycle decomposition for x and y. We do not include 1-cycles in our decomposition.

Lemma 3.2.7. *Both x and y must have the same two cycles else we can find a $c \in C$ such that $cx \nsim cy$.*

Proof. We suppose (i, j) is a cycle in a cycle decomposition for x. Write $x = (i, j)x_1$, where x_1 consists of the rest of the cycles of x. We first show that i, j are both in the cycle decomposition of y and each must be in a 2-cycle of y. If not, let $c = (j, i, k)$, where k is an element of any nontrivial cycle of x. Such a k exists since $x \in A_n$. We then have that $cx \nsim cy$.

We now show that (i, j) is a cycle in the decomposition for y. Suppose not, write $y = (i, k)(j, m)y_1$ for some $k, m \in [n]$. We have two possibilities for x: $x = (i, j)(k, a_1)(m, b_1)x_1$ or $x = (i, j)(k, a_1, m, b_1)x_1$, where a_1, b_1 are subsequences of $[n]$ representing the rest of the elements in the decomposition. Here, we allow a_1, b_1 to be empty sets. In the first case, where $x = (i, j)(k, a_1)(m, b_1)x_1$, we have that $(i, m, k)x = (i, b_1, m, a_1, k, j)x_1$ and $(i, m, k)y = (i, j, m)y_1$. In the second case, where $x = (ij)(k, a_1, m, b_1)x_1$, we have $(j, m, t)x = (j, b_1, k, a_1, m, t, i)$. Thus, in both cases, since $x \sim y$, we have that $(i, m, k)x \nsim (i, m, k)y$. □

Now we consider cycles of length at least 3.

Lemma 3.2.8. *If $\{i, j, k\}$ occurs in some cycle in the decomposition of x, then it also occurs in some cycle in the decomposition for y in the same cyclic order else there exists a $c \in C$ such that $cx \nsim cy$.*

Proof. We show that if $\{i, j, k\}$ occurs in some cycle in the decomposition of x, then it also occurs in some cycle in the decomposition for y else we can find a $c \in C$ such that $cx \nsim cy$. Thus, suppose that $x = (i, a_1, j, b_1, k, c_1)x_1$ where a_1, b_1, c_1 are subsequences, possibly empty, of $[n]$ and y doesn't have all of i, j, k all in the same cycle. Then we have either $y = (i, d_1)(j, e_1)(k, f_1)y_1$ or $y = (i, d_1, j, e_1)(k, f_1)y_1$, where d_1, e_1 and f_1 are subsequences, possibly empty, of $[n]$.

In the first case, where $y = (i, d_1)(j, e_1)(k, f_1)y_1$, we have

$$(i, j, k)y = (i, e_1, j, f_1, k, d_1)y_1$$

and $(i, j, k)x = (i, b_1, k, a_1, j, c_1)x_1$. Since $x \sim y$, we have that $(i, j, k)x \nsim (i, j, k)y$.

In the second case, where $y = (i, d_1, j, e_1)(k, f_1)y_1$, we have

$$(i, k, j)y = (i, f_1, k, e_1)(j, d_1)y_1$$

and $(i, k, j)x = (i, c_1)(k, b_1)(j, a_1)x_1$. Again, we have $(i, k, j)x \nsim (i, k, j)y$.

Thus, if $x = (i, a_1, j, b_1, k, c_1)x_1$ then y must be either $y = (i, d_1, j, e_1, k, f_1)y_1$ or $y = (i, d_1, k, e_1, j, f_1)y_1$ for some subsets d_1, e_1, f_1 of $[n]$. If it's the second case, then $(i, j, k)x = (i, b_1, k, a_1, j, c_1)x_1 \nsim (i, j, k)y = (i, f_1)(j, e_1)(k, d_1)y_1$. Thus, we must have that

$$y = (i, d_1, j, e_1, k, f_1)y_1.$$

We have just shown that if $\{i, j, k\}$ is in some cycle of x, then it is also in some cycle of y in that same order else there exists a $c \in C$ such that $cx \nsim cy$. □

Thus from the above lemma, if $x = (i, a_1, j, b_1, k, c_1)x_1$, then $y = (i, d_1, j, e_1, k, f_1)y_1$. We have that $(i, j, k)x = (i, c_1)(k, b_1)(j, a_1)x_1$ and $(i, j, k)y = (i, f_1)(k, e_1)(j, d_1)y_1$. Thus $(i, j, k)x \nsim (i, j, k)y$ unless $\{|a_1|, |b_1|, |c_1|\} = \{|d_1|, |e_1|, |f_1|\}$.

We next show that unless $|a_1| = |d_1|$, $|b_1| = |e_1|$ and $|c_1| = |f_1|$, we can find $c \in C$ such

that $cx \nsim cy$. Suppose not, that is, suppose without loss of generality that $|a_1| < |d_1|$. But then this means that there are less elements of $[n]$ between i and j in that cycle of x than in the same cycle of y. But this contradicts the requirement we proved earlier that for all $\{i, j, k\}$ occuring in some cycle of x, the same set of elements must also occur in some cycle of y in the same cyclic order.

Thus, we have shown that for all $x, y \in A_n$, $x \sim y$, unless $x = y$, we can always find a $c \in C$ such that $cx \nsim cy$. □

□

3.3 The Projective Special Linear Groups $PSL(2, p^n)$

Let $G = PSL(2, p^n)$ for some prime p. We wish to investigate the group $\mathcal{W}(G)$. Our first observation is that Humphries' lemma, Lemma 3.1.9, cannot be used in this case. We run into two main issues. The first issue arises because the group $PSL(2, p^n)$ is different from A_n and S_n and hence his techniques will not generalize. The second issue arises from the fact that the class C we are interested in generates G "too quickly." More precisely, the set C^2 constitutes most of the elements of G and $C^3 = G$.

In resolving the first issue, we again resort to analyzing graph automorphisms and in resolving the second, we modify Humphries' lemma.

The strategy for proving the theorem is indicated by the following modification of Humphries' lemma.

Lemma 3.3.1. *Let G be a group and C a nontrivial class of G. Suppose also that for every $\alpha \in \mathcal{W}(G)$, there is a $\phi \in \mathcal{W}_0(G)$ such that the following three statements are true:*

(1) $\phi\alpha(x) = x$, for all $x \in C$;

(2) $\phi\alpha(x) \sim x$, for all $x \in G$;

(3) For all $x \neq y$, $x \sim y$, there exists $c \in C$ such that $cx \nsim cy$.

Then $\mathcal{W}(G)$ is trivial.

Proof. We replace $\phi\alpha$ with ϕ in the following proof. It suffices to show that ϕ is the identity map. Suppose not, that is, $\phi(x) \neq x$ for some $x \in G$. By assumption (2), $\phi(x) \sim x$. By assumption (3), there exists a $c \in C$ such that $cx \nsim c\phi(x)$. But using (1), we have $\phi(cx) \sim \phi(c)\phi(x) = c\phi(x) \nsim cx$, which is a contradiction to (2). □

We note that if $C^2 = G$ then (2) is automatically satisfied if (1) is true.

Consider $SL(2, p^n)$. The center of $SL(2, p^n)$ is $Z = \{I, -I\}$. The projective special linear group $G = PSL(2, p^n)$ is the quotient $SL(2, p^n)/Z$. For ease of notation, we will denote elements of G by elements of $SL(2, p^n)$ without explicitly referring to the quotient. We include in the Appendix the conjugacy classes and character table of G. We will quote freely these facts throughout sections 3.3, 3.4 and 3.5.

Let C be the class of G containing $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then C is a class of elements of order p and $|C| = (p^{2n} - 1)/2$. From Lemma A.0.14, the class D is another class of elements of order p and size $(p^{2n} - 1)/2$.

Let $\phi \in \mathcal{W}(G)$. By conjugating by an element of $GL(2, p^n)$, there is an outer automorphism of G taking one class to the other. Thus, we may assume that ϕ sends C to itself. This implies, in addition, that ϕ sends the class D to itself because these two classes are the only classes of size $(p^{2n} - 1)/2$. We note also that the class $L^{(p^n-1)/4}$ is the unique class of involutions. Thus $\phi(L^{(p^n-1)/4}) = L^{(p^n-1)/4}$.

We first define the trace of each class of G. By picking the conjugacy class representatives for G given in Lemma A.0.14 and define the trace of those classes as the trace of the representatives in the usual way. If $X \in G$, then we define the trace of X, denoted by $Tr(X)$, to be the trace of the representative of the conjugacy class to which X belongs. Thus, we have that for all $X, Y \in G$, if $X \sim Y$, then $Tr(X) = Tr(Y)$. In particular, $Tr(I) = 2$ for the identity element of G and $Tr(X) = 2$ for all X belonging to the class of C or D. We also note that the elements of the class $L^{(p^n-1)/4}$ have trace 0.

We first prove part (2) of Lemma 3.3.1 if (1) holds.

Proposition 3.3.2. *Let $G = PSL(2, p^n)$. Suppose that $\alpha \in \mathcal{W}(G)$ satisfies (1) of Lemma 3.3.1. Then there exists a map $\phi \in \mathcal{W}_0(G)$ such that for all $X \in G$, $\phi\alpha(X) \sim X$.*

Proof. We replace $\phi\alpha$ with ϕ in this proof.

If $x \in C^2$, then $\phi(x) \sim x$. To see this, write $x = c_1c_2$, for some c_1, c_2 in C. By assumption, $\phi(c_1) = c_1, \phi(c_2) = c_2$, we have that

$$x = c_1c_2 = \phi(c_1)\phi(c_2) \sim \phi(c_1c_2) = \phi(x).$$

We first show that the classes D and B^m, for $1 \leq m \leq (p^n - 1)/4$ lie in C^2. Then we will show that ϕ sends each diagonal matrix to itself. Since the classes represented by the diagonal matrices are the only classes outside of C^2, this completes the proof for all the representatives of all of the classes in G and hence all the classes of G.

To show $D \subset C^2$, we use character theory. We introduce some notation from James and Liebeck [14]. Let $C_1, ..., C_l$ be all the classes of a finite group G. We consider the group algebra $\mathbb{C}G$. For $C \subseteq G$, we define $\bar{C} = \sum_{x \in C} x$. Then it's easy to show that there exists integers $a_{i,j,k}$ such that for $1 \leq i, j, \leq l$, $\bar{C}_i\bar{C}_j = \sum_{k=1}^{l} a_{i,j,k}\bar{C}_k$. Moreover, for all $g \in C_k$, and for all i, j, we have

$$a_{i,j,k} = \#\{(a, b) \,|\, a \in C_i, b \in C_j \text{ such that } ab = g\}.$$

In addition, the $a_{i,j,k}$'s are given by the formula,

$$a_{i,j,k} = \frac{|G|}{|C_G(g_i)||C_G(g_j)|} \sum_{\chi} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_k)}}{\chi(1)},$$

where $g_i \in C_i$ and the sum runs over all irreducible characters χ of G. The $a_{i,j,k}$'s are called the *structure constants* of G [14].

Now denote $C_1 = C, C_2 = D$. To show that $D \subset C^2$, it suffices to show a_{112} is nonzero. Note that $|C_G(g_1)| = |C_G(g_2)| = p^n$ if $g_1 \in C$, $g_2 \in D$ by Lemma A.0.14. From the formula

for $a_{i,j,k}$, we have that

$$\begin{aligned}
a_{112} &= \frac{|G|}{|C_G(g_1)||C_G(g_1)|}\sum_{\chi}\frac{\chi(g_1)\chi(g_1)\overline{\chi(g_2)}}{\chi(1)} \\
&= \frac{p^n(p^{2n}-1)}{2p^{2n}}(1+\frac{p^n-5}{4(p^n+1)}-\frac{p^n-1}{4(p^n-1)} \\
&\quad +(\frac{1+\sqrt{p^n}}{2})^2(\frac{1-\sqrt{p^n}}{2})(\frac{2}{p^n+1})+(\frac{1-\sqrt{p^n}}{2})^2(\frac{1+\sqrt{p^n}}{2})(\frac{2}{p^n+1})) \\
&= \frac{(p^{2n}-1)p^n}{2p^{2n}}(1+\frac{p^n-5}{4(p^n+1)}-\frac{p^n-1}{4(p^n-1)}+\frac{2-2p^n}{4(p^n+1)}) \\
&= \frac{p^n-1}{4}.
\end{aligned}$$

Similarly, if we let $C_1 = C$ and $C_m = B^m$, we have

$$\begin{aligned}
a_{11m} &= \frac{|G|}{|C_G(g_1)||C_G(g_1)|}\sum_{\chi}\frac{\chi(g_1)\chi(g_1)\overline{\chi(g_m)}}{\chi(1)} \\
&= \frac{p^n(p^{2n}-1)}{2p^{2n}}\left(1-\frac{1-\sum_{i=1}^{(p^n-1)/4}(\sigma^{2i}+\sigma^{-2i})}{p^n-1}\right),
\end{aligned}$$

where σ is a $(p+1)$th root of unity. Notice that $-(p-1)/2 \equiv (p-1)/2+2 \bmod (p+1)$. Thus,

$$\begin{aligned}
a_{11m} &= \frac{p^n(p^{2n}-1)}{2p^{2n}}\left(1-\frac{\sigma^{2m}+\sigma^{4m}+\sigma^{6m}+\cdots+\sigma^{(p^n-3)m}+\sigma^{(p^n-1)m}}{p^n-1}\right) \\
&= \frac{p^n(p^{2n}-1)}{2p^{2n}}(1-\frac{-1}{p^n-1}) \\
&= \frac{p^n(p^{2n}-1)}{2p^{2n}}(\frac{p^n}{p^n-1}) \\
&= \frac{p^n+1}{2}.
\end{aligned}$$

To complete the proof of the proposition, we now show that ϕ sends each diagonal matrix

to itself. Let $L^l = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right), x \in \mathbb{F}_p^n, x \neq \pm 1$, for some l with $1 \leq l \leq (p^n - 5)/4$. Suppose that $\phi(L^l) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Let $M_\lambda = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$, where λ is a nonzero square in $\mathbb{F}_{p^n}$ so that M_λ is in C. We note that $M_\lambda L^l \sim L^l$. Then

$$\phi(L^l) \sim \phi(M_\lambda L^l) \sim \phi(M_\lambda)\phi(L^l) = M_\lambda \phi(L^l).$$

Thus, we have that Tr($M_\lambda \phi(L^l)$)=Tr($\phi(L^l)$). But Tr($\phi(L^l)$)=$a + d$ and

$$Tr(M_\lambda \phi(L^l)) = a + d + \lambda c.$$

Thus, $c = 0$. Similarly, by using $M_{-\lambda}^T \sim M_\lambda$ and multiplying on the right, we can show that $b = 0$. Thus ϕ sends a diagonal matrix to a diagonal matrix.

Now, we show that $\phi(L^l) = L^l$. Suppose $\phi(L^l) = \left(\begin{smallmatrix} y & 0 \\ 0 & y^{-1} \end{smallmatrix}\right)$. We note that $y \neq \pm 1$. Pick

$$A_{a,c} = \left(\begin{smallmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{smallmatrix}\right) \in C$$

such that $L^l A_{a,c}$ is in either C or D and Tr($L^l A_{a,c}$)=2. We will show that such an $A_{a,c}$ exists by a similar argument using the structure constants as above. If l is even, we show that such an $A_{a,c}$ can be picked so that $L^l A_{a,c}$ is in C. And if l is odd, we will pick $A_{a,c}$ so that $L^l A_{a,c}$ is in D. Let $C_1 = L^l$, $C_2 = C$ and $C_3 = D$. If l is even, recall that ρ is a $(p-1)$th root of unity and we have from Lemma B.0.15,

$$\begin{aligned} a_{122} &= (p^n + 1)(1 + \frac{\rho^{2l} + \rho^{-2l} + \cdots + \rho^{l(p^n-5)/2} + \rho^{-l(p^n-5)/2}}{p^n + 1} \\ &\quad + \frac{2(-1)^l(\frac{1+\sqrt{p^n}}{2})^2}{p^n+1} + \frac{2(-1)^l(\frac{1-\sqrt{p^n}}{2})^2}{p^n+1}) \\ &= (p^n + 1)(1 + \frac{\rho^{2l} + \rho^{4l} + \cdots + \rho^{l(p^n-5)/2} + \rho^{l((p^n-5)/2+4)} + \cdots + \rho^{(p^n-3)l}}{p^n+1} + (-1)^l). \end{aligned}$$

Since l is even, we have $\rho^{l(p-1)/2} = 1$ and the above sum involving the ρ's is -2. Thus,

$$\begin{aligned} a_{122} &= (p^n+1)(1+\frac{-2}{p^n+1}+(-1)^l) \\ &= 2p^n. \end{aligned}$$

If l is odd, then we have $\rho^{l(p^n-1)/2} = -1$ and the above sum involving the ρ's is 0. In this case, we also have $a_{122} = 0$. Thus, in order to show that we can find $A_{a,c}$ so that $L^l A_{a,c}$ is in D, we show a_{123} is nonzero. In this case, we have,

$$\begin{aligned} a_{123} &= (p^n+1)\left(1+\frac{\sum_{i=1}^{(p^n-5)/4}(\sigma^{2li}+\sigma^{-2li})}{p^n+1}+\frac{(-1)^l(1+\sqrt{p^n})(1-\sqrt{p^n})}{p^n+1}\right) \\ &= (p^n+1)\left(1+\frac{(-1)^l(1-p^n)}{p^n+1}\right) \\ &= 2p^n. \end{aligned}$$

Since $\phi(D) = D$, we have $\phi(L^l A_{a,c}) \sim L^l A_{a,c}$. But $\phi(L^l A_{a,c}) \sim \phi(L^l)\phi(A_{a,c}) = \phi(L^l)A_{a,c}$. Thus, Tr($\phi(L^l)A_{a,c}$)=2. So

$$2 = Tr(L^l A_{a,c}) = x + x^{-1} + ac(x^{-1} - x),$$

which gives $ac = (x-1)/(x+1)$. Now,

$$2 = Tr(\phi(L^l)A_{a,c}) = y + y^{-1} + ac(y^{-1} - y),$$

and substituting $ac = (x-1)(x+1)$, into the above equation, we get,

$$y^2 - y(x+1) + x = 0,$$

which is quadratic in y. We solve to obtain $y = x$ or $y = 1$. Thus, $y = x$, and $\phi(L^l) = L^l$, as required.

Thus, for all $X \in G$, $\phi(X) \sim X$. □

Now we show part (3) of Lemma 3.3.1.

Proposition 3.3.3. *For all $X, Y \in G, X \neq Y$, satisfying $X \sim Y$, there exists $A_{a,c} \in C$ such that $A_{a,c}X \nsim A_{a,c}Y$.*

Proof. We assume that $p^n > 3$. The case $p = 3$ can be checked computationally by Magma. We first assume that $X, Y \in C$. By conjugating, if necessary, we may assume $X = A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Write $Y = \begin{pmatrix} 1-bd & b^2 \\ -d^2 & 1+bd \end{pmatrix}$. We have that

$$Tr(A_{a,c}X) = 2 - c^2$$

and

$$Tr(A_{a,c}Y) = 2 - a^2d^2 - b^2c^2 + abcd.$$

Let $c = 0$. If $d \neq 0$, then pick $a \neq 0$ such that $a^2 \neq 4/d^2$ so that

$$\pm Tr(A_{a,c}X) = \pm 2 \neq Tr(A_{a,c}Y) = 2 - a^2d^2.$$

We can do this since $p^n > 3$. If $d = 0$ then $b^2 \neq 1$ else $X = Y$. But $Tr(A_{a,c}X) = 2 - c^2$ and $Tr(A_{a,c}Y) = 2 - b^2c^2$. So we need to find a $c \in \mathbb{F}_{p^n}$ such that

$$2 - c^2 \neq \pm(2 - b^2c^2).$$

Choosing $c \neq 0$ such that

$$c^2(1 + b^2) \neq 4$$

will do this.

Suppose that $X, Y \in D$. Without loss, assume $X = \left(\begin{smallmatrix} 1 & \epsilon \\ 0 & 1 \end{smallmatrix}\right)$, where ϵ is a generator of $\mathbb{F}_{p^n}^*$. Since $X \sim Y$, $Y = \left(\begin{smallmatrix} 1+gh\epsilon & h^2\epsilon \\ -g^2\epsilon & 1-gh\epsilon \end{smallmatrix}\right), he - gf = 1$. We note that

$$Tr(A_{a,c}X) = 2 - c^2\epsilon$$

and

$$Tr(A_{a,c}Y) = 2 - 2acgh\epsilon - g^2a^2\epsilon - c^2h^2\epsilon.$$

We want to show that there exist $a, c \in \mathbb{F}_{p^n}$ such that $Tr(A_{a,c}X) \neq \pm Tr(A_{a,c}Y)$. If $h^2 \neq 1$, then choose $a = 0$ so that $Tr(A_{a-c}X) \neq Tr(A_{a,c}Y$. Also choose $c \neq 0$ so that $\epsilon c^2(1 + h^2) \neq 4$ so that $Tr(A_{a,c}X) \neq -Tr(A_{a,c}Y)$. If $h^2 = 1$, then $g \neq 0$ else $X = Y$. In this case, choose nonzero a, c such that $2ch + ga \neq 0$ and $\epsilon c^2 \neq 2$ to get $Tr(A_{a,c}X) \neq \pm Tr(A_{a,c}Y)$. We can do this since $p^n > 3$.

Suppose now that X, Y are in the class represented by L^l, where $1 \leq l \leq (p^n - 3)/4$. Thus, $p^n > 3$ else classes of this type do not exist. As before, without loss, assume that $X = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right), x \neq \pm 1$ and $Y = \left(\begin{smallmatrix} hex - gfx^{-1} & fhx - hfx^{-1} \\ gex^{-1} - gex & hex^{-1} - fgx \end{smallmatrix}\right), he - gf = 1$. Consider $A_{a,0}$ in C. Then

$$Tr(A_{a,0}X) = x + x^{-1},$$

and

$$Tr(A_{a,0}Y) = x - x^{-1}(1 - a^2ge).$$

Notice if g or e is zero, then any nonzero a will give different traces. If both g, e are nonzero, choose a so that $2 \neq a^2ge$ and $2x^2 \neq -a^2ge$ so that $Tr(A_{a,c}X) \neq \pm Tr(A_{a,c}Y)$.

Suppose now that $X, Y \in B^m$. Then we assume $X = \left(\begin{smallmatrix} x & y \\ \epsilon y & x \end{smallmatrix}\right), y \neq 0, x \neq \pm 1$ and $Y = \left(\begin{smallmatrix} x - fye\epsilon + ghy & h^2y - f^2y\epsilon \\ y(e^2\epsilon - g^2) & x + fye\epsilon - hgy \end{smallmatrix}\right), he - gf = 1$. Then,

$$Tr(A_{a,c}X) = 2x - yc^2 + a^2y\epsilon,$$

and

$$Tr(A_{a,c}Y) = 2x + 2acfye\epsilon - 2acghy + a^2(e^2y\epsilon - g^2y) - c^2(h^2y - f^2y\epsilon).$$

We want to find $a, c \in \mathbb{F}_{p^n}$ such that $Tr(A_{a,c}X) \neq \pm Tr(A_{a,c}Y)$. Equivalently, we find a, c such that

$$c^2(1 + f^2\epsilon - h^2) + a^2(\epsilon e^2 - g^2 - \epsilon) + 2ac(fe\epsilon - gh) \neq 0, \tag{3.3}$$

and

$$4x/y + c^2(-1 + f^2\epsilon - h^2) + a^2(\epsilon e^2 - g^2 + \epsilon) + 2ac(fe\epsilon - gh) \neq 0. \tag{3.4}$$

We first note that not all three parentheses expressions from Equation (3.3) can be 0 else $X = Y$. Since $fe\epsilon - gh$ is in both equations, if it's nonzero, we can find a, c such that both expressions are nonzero and we are done.

Thus, suppose now that $fe\epsilon - gh = 0$. Also suppose that at least one of $e^2\epsilon - g^2 + \epsilon$ and $f^2\epsilon - h^2 - 1$ from Equation (3.4) is nonzero. Then since we also know that at least one of $1 + f^2\epsilon - h^2$ and $\epsilon e^2 - g^2 - \epsilon$ is also nonzero, we can find a, c such that both equations are nonzero as required.

Thus, suppose that both $e^2\epsilon - g^2 + \epsilon$ and $f^2\epsilon - h^2 - 1$ are zero. If $x \neq 0$, then again we are done. Thus suppose also that $x = 0$. Then $Y = \left(\begin{smallmatrix} 0 & -y \\ -\epsilon & 0 \end{smallmatrix}\right)$ which gives $y = -1/\epsilon$ and from $X = \left(\begin{smallmatrix} 0 & y \\ \epsilon y & 0 \end{smallmatrix}\right)$, we get that $\epsilon = -1$, which is a contradiction.

Thus, if $X \neq Y$, we can always find $A_{a,c} \in C$ such that $A_{a,c}X \nsim A_{a,c}Y$. □

We can not, at this time, prove part (1) of Lemma 3.3.1 for the general case $G = PSL(2, p^n)$. We will be able to prove it for the special cases $PSL(2, p)$ and $PSL(2, p^2)$. We will do this in the next two sections.

3.4 The Projective Special Linear Groups $PSL(2, p)$

Let $G = PSL(2, p)$, for a prime p. Let C be the class of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in G. For simplicity, we treat the case $p \equiv 1 \bmod 8$. (The general cases are proven in the Appendix.) In particular, this

implies that -1 and 2 are quadratic residues in $\mathbb{F}_p$ [16, Theorem 5.3 and 5.5]. Let $r, s \in \mathbb{F}_p$ be such that $r^2 \equiv -1 \bmod p$ and $s^2 \equiv 2 \bmod p$. By the results of the previous section, we only need to prove part (1) of Lemma 3.3.1.

Proposition 3.4.1. *Let $\phi \in \mathcal{W}(G)$. Then there exists $\alpha \in \mathcal{W}_0(G)$ such that $\alpha\phi(x) = x$ for all $x \in C$.*

Proof. We define a graph Γ as follows. The vertices of Γ are elements of the class C. Two vertices M and N are connected by an edge if $MN \in L^{(p-1)/4}$, that is MN is an involution. Recall that up to an automorphism of G, we may assume that $\phi(C) = C$. We show that ϕ acts as an automorphism of Γ. By assumption, ϕ is a bijection. Suppose M, N are adjacent in Γ. Then $MN \in L^{(p-1)/4}$. By the above, we have $\phi(MN) \in L^{(p-1)/4}$. But $\phi(MN) \sim \phi(M)\phi(N)$, thus $\phi(M)\phi(N) \in L^{(p-1)/4}$ and $\phi(M), \phi(N) \in C$ are also adjacent.

We analyze the graph Γ. We fix a vertex $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of Γ. Since $\phi(A) \in C$, by conjugation if necessary, we may assume that $\phi(A) = A$. We investigate the immediate neighbors of A. Any element of C is conjugate to A and can be written in the form

$$A_{a,c} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{smallmatrix}\right),$$

for some $a, c \in \mathbb{F}_p$.

Since

$$AA_{a,c} = \left(\begin{smallmatrix} 1-ac-c^2 & a^2+1+ac \\ -c^2 & 1+ac \end{smallmatrix}\right), \tag{3.5}$$

$AA_{a,c} \in L^{(p-1)/4}$ implies that $Tr(AA_{a,c}) = 2 - c^2 = 0$. Thus $c = \pm\sqrt{2} = \pm s$. Thus the neighbors of A are precisely the elements $A_{a,c}$ such that $c = \pm s$ and $a \in \mathbb{F}_p$. But since $A_{a,c} = A_{-a,-c}$, these are precisely the elements $A_{a,c}$ such that $c = \sqrt{2} = s$ and $a \in \mathbb{F}_p$.

Lemma 3.4.2. *The graph Γ is connected.*

Proof. Suppose that Γ decomposes into multiple components. We first notice that these components must have the same size since any two vertices of the graph are images of each

other by an automorphism of G. Thus to show that Γ has only one component, we only need to show that the component containing A contains more than $|C|/2 = (p^2-1)/4$ elements.

We show that the neighbors of A form a cycle of length p around A, where $A_{a,s}$ is adjacent to $A_{a+1,s}$, for all $a \in \mathbb{F}_p$. The neighbors of A can visualized below in Figure 3.1.

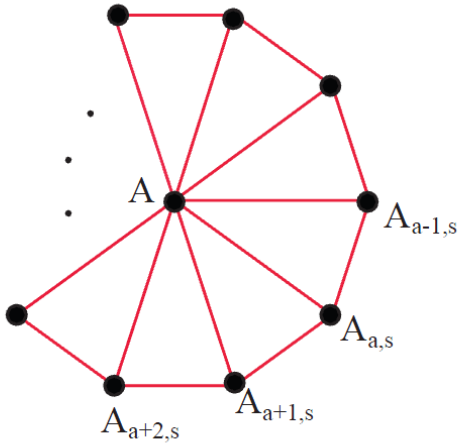

Figure 3.1: The neighbors of A in Γ.

We can check that the trace of $A_{a,s}A_{a+1,s}$ is 0 for all $a \in \mathbb{F}_p$, showing that $A_{a,s}$ and $A_{a+1,s}$ form an edge of Γ. We call the $A_{a,s}$'s the cycle neighbors of A.

Each cycle neighbor $A_{a,s}$ of A, has its own cycle neighbors. These can be found by conjugating by a fixed element D such that $D^{-1}AD = A_{a,s}$. If we let $D = \left(\begin{smallmatrix} 0 & -1/s \\ s & -a \end{smallmatrix}\right)$, then we have that $D^{-1}AD = A_{a,s}$. Thus the cycle neighbors of $A_{a,s}$ are

$$D^{-1}A_{x,s}D = \begin{pmatrix} 1+sx-sax^2 & (ax-1)^2 \\ -2x^2 & 1-sx+sax^2 \end{pmatrix},$$

for all $x \in \mathbb{F}_p$.

Now, we show that for each $a \in \mathbb{F}_p$, A and $A_{a,s}$ have exactly two cycle neighbors in common, $A_{a-1,s}$ and $A_{a+1,s}$. To see this, we suppose that $D^{-1}A_{x,s}D$ is a cycle neighbor of both $A_{a,s}$ and A. Then the trace of $AD^{-1}A_{x,s}D$ must be 0. But the trace of $AD^{-1}A_{x,s}D$ is $2-2x^2$. Thus, $x = \pm 1$. But substituting $x = \pm 1$ into $D^{-1}A_{x,s}D$ gives $A_{a-1,s}$ and $A_{a+1,s}$ as

required. This shows, in particular, that among the cycle neighbors of A, the only adjacencies are the ones formed by the p-cycle $A_{0,s}$, $A_{1,s}$,...,$A_{p-1,s}$, $A_{0,s}$.

Next, for all $a, b \in \mathbb{F}_p$, $a \neq b$, we show that $A_{a,s}$ and $A_{b,s}$ have two cycle neighbors in common, namely A and $\begin{pmatrix} 1+sx-sax^2 & (ax-1)^2 \\ -2x^2 & 1-sx+sax^2 \end{pmatrix}$, where $x \equiv 2/(a-b) \bmod p$. To see this, we solve

$$\begin{pmatrix} 1+sx-sax^2 & (ax-1)^2 \\ -2x^2 & 1-sx+sax^2 \end{pmatrix} = \begin{pmatrix} 1+sy-sby^2 & (by-1)^2 \\ -2y^2 & 1-sy+sby^2 \end{pmatrix}.$$

The $(2,1)$ entry yields $y = \pm x$. But the $(1,2)$ entry implies $a \neq b$, so we have either $y = x = 0$ or $y = -x$. The first case gives A as a common cycle neighbor. In the second case, we substitute $y = -x$ into the above matrices and equate their $(1,1)$ entries to get

$$1 + \sqrt{2}x - \sqrt{2}ax^2 = 1 - \sqrt{2}x - \sqrt{2}bx^2.$$

This gives $x \equiv 2/(a-b) \bmod p$, as required.

Now we find a lower bound for the number of elements in the same component as A. We start with A and its p cycle neighbors for a total of $p+1$ elements. Since any two distinct cycle neighbors, $A_{a,s}$ and $A_{b,s}$, of A have exactly one common cycle neighbor, not including A, we have that we can get at least

$$(p-3) + (p-4) + \cdots + 2 + 1 = (p-3)(p-2)/2$$

distinct cycle neighbors of the $A_{a,s}$'s not including A and its cycle neighbors, for all $a \in \mathbb{F}_p$. Thus we have at least $(p^2-3p+8)/2$ elements in the same component as A. But this number is strictly bigger than $|C|/2 = (p^2-1)/4$, for all p. Thus Γ can have at most one component and hence must be connected. □

Lemma 3.4.3. *The stabilizer of A under the action of $Aut(\Gamma)$ is isomorphic to the dihedral group of order $2p$, D_{2p}.*

Proof. We first show that D_{2p} is a subgroup of the stabilizer group. Let $P = \left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right)$, where

$d = -1/s$. Then P commutes with A and we can check that $P^{-1}AP = A$ and $P^{-1}A_{a,s}P = A_{a+1,s}$, for all a. Thus conjugating by P rotates Γ about A. Now let $Q = \left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & x \end{smallmatrix}\right)$, where $x^2 = -1$. Then, by composing the inverse map with conjugation by Q, we get the map $\beta : \Gamma \to \Gamma$, which sends A to itself and $A_{a,s}$ to $Q^{-1}A_{a,s}^{-1}Q = A_{-a,s}$, realizing a reflection fixing A's cycle neighbor $A_{0,s}$.

We next show that the elements of D_{2p} are the only automorphisms that fix A. To do this, we show that any automorphism fixing A and its cycle neighbors fixes all of Γ.

Since Γ is connected, we use an inductive argument on the distance from the vertex A. By assumption, all vertices with distance 1 away from A are fixed. Suppose that all vertices with distance less than n away from A is fixed. Let A_n be any vertex whose distance from A is $n \geq 2$. Let $A_0 = A, A_1, .., A_{n-1}, A_n$ be a path of length n from A to A_n. By assumption, $A_0, A_1, ..., A_{n-1}$ are fixed. Consider the vertex A_{n-2}. By assumption, all of the cycle neighbors of A_{n-2} are fixed and A_{n-1} is one such neighbor. By the argument above, A_{n-1} and A_{n-2} have two neighbors in common, say B_1 and B_2, both of which are fixed. Thus A_{n-1}, B_1, B_2, and A_n are cycle neighbors of A_{n-1}. Since A_{n-2}, B_1, B_2 are all fixed, the rest of the cycle neighbors of A_{n-1} are fixed and hence A_n is also fixed.

Thus D_{2p} is the stabilizer group of automorphisms of Γ fixing A. □

We have just shown by Lemma 3.4.3 that $\mathcal{W}_0(G)$ can realize all of the elements of the stabilizer group, D_{2p}, fixing A. Thus, we have that $\mathcal{W}_0(G)$ acting on Γ can realize all of $Aut(\Gamma)$.

Now, we prove Proposition 3.4.1. The weak Cayley table isomorphism ϕ acts as an automorphism on Γ. Since $\mathcal{W}_0(G)$ can realize any element of $Aut(\Gamma)$, let α be the element of $\mathcal{W}_0(G)$ which is the inverse element of ϕ in $Aut(\Gamma)$. Then $\alpha\phi(x) = x$, for all $x \in C$ as required. □

We have shown that ϕ satisfies all three of the conditions of Lemma 3.3.1, for $p \equiv 1 \bmod 8$. Thus, in this case, $\mathcal{W}(G)$ is trivial. For the general case, see the Appendix.

3.5 The Projective Special Linear Groups $PSL(2, p^2)$

Theorem 3.5.1. *For all primes $p \equiv 5$ mod 8, $\mathcal{W}(PSL(2, p^2))$ is trivial.*

Proof. Let $G = PSL(2, p^2)$. It suffices to show part (1) of Lemma 3.3.1. In other words, we show that given $\phi \in \mathcal{W}(G)$, there exists a trivial weak Cayley table isomorphism α such that $\alpha\phi(x) = x$ for all $x \in C$.

In this case, we have that 2 is a quadratic nonresidue in $\mathbb{F}_p$ [16, Theorem 5.5]. But it is a quadratic residue in $\mathbb{F}_{p^2}$ since all quadratics over $\mathbb{F}_p$ split over $\mathbb{F}_{p^2}$. As before let C be the class of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $\phi \in \mathcal{W}(G)$. We show that there exists $\alpha \in \mathcal{W}_0(G)$ such that $\alpha\phi(x) = x$ for all $x \in C$.

We define a graph Γ with colored edges as follows. The vertices of Γ are elements of the class C. Two vertices A, B are connected by a red edge if $AB \in L^{(p-1)/4}$, that is, if AB is an involution. If $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in C$, then let S denotes the set of all neighbors that are red-adjacent to A in Γ. Let $s = \sqrt{2}$ in $\mathbb{F}_{p^2}$. Then as proven in the previous case in Section 3.3, $S = \{A_{a,s} | a \in \mathbb{F}_{p^2}\}$. Thus $|S| = p^2$.

We want to understand the red-adjacencies among the elements of S. And as in Section 3.3, given $a \in \mathbb{F}_{p^2}$, one can show that the only elements of S that are red-adjacent to $A_{a,s}$ are $A_{a+1,s}$ and $A_{a-1,s}$. Moreover, $A_{a,s}, A_{a+1,s}, ..., A_{a+p-1,s}, A_{a,s}$ form a p-cycle in Γ. Thus S decomposes into p distinct p-cycles, where given an element of S, $A_{a,s}$, we get the full p-cycle that $A_{a,s}$ belongs to by repeatedly adding 1 to the argument a. This is the complete local picture of red-adjacencies for all of the neighbors of A. See Figure 3.2 below.

Now we add to Γ a new set of colored edges joining elements of S. Two vertices $A, B \in S$ are connected by a blue edge if $AB \in C$. Solving the equations $Tr(A_{a,s}A_{b,s}) = \pm 2$ where $a \neq b$, we get that given $A_{a,s} \in S$, its blue-adjacent neigbors in S are $A_{a+s,s}$ and $A_{a-s,s}$. Thus, $A_{a,s}, A_{a+s,s}, ..., A_{a+(p-1)s,s}, A_{a,s}$ form a p-cycle in blue edges in Γ.

A geometric way of visualizing the vertices of S is to recognize that the vertices of S along with the red and blue edges form the skeleton for a torus. See Figure 3.3.

Given a vertex $A_{a,s}$ in S, adding ± 1 to a gives us the vertices $A_{a\pm 1,s}$ connected to $A_{a,s}$ by

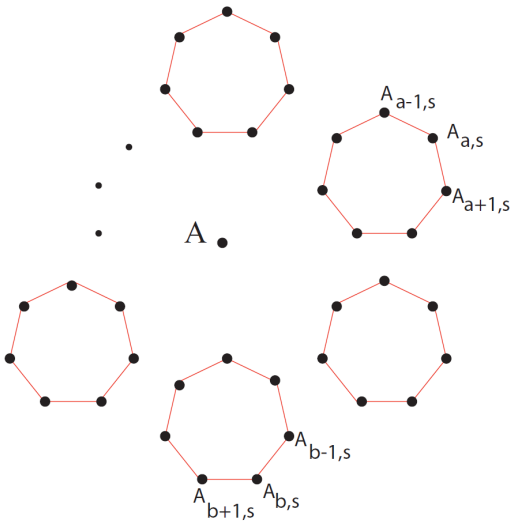

Figure 3.2: The p^2 neighbors of A in Γ.

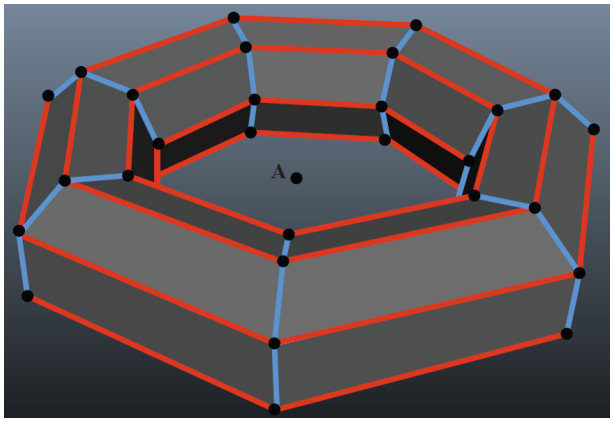

Figure 3.3: The neighbors of A with both red and blue edges form the skeleton of a torus.

red edges. But adding $\pm\sqrt{2}$ to a gives us vertices $A_{a\pm\sqrt{2},s}$ connected to $A_{a,s}$ by blue edges. These four vertices are the only vertices in S connected to $A_{a,s}$ by red and blue colored edges. See Figure 3.4.

Since $\{1, \sqrt{2}\}$ forms a basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, any two vertices in S, $A_{a,s}$ and $A_{b,s}$, can be connected to one another by a path of red and blue edges by adding the appropriate $\mathbb{F}_p$-multiples of 1's and $\sqrt{2}$'s.

Given a vertex $A_{a,s}$ in S, the p red-adjacencies path cycle $A_{a,s}, A_{a+1,s}, ..., A_{a+p-1,s}, A_{a,s}$ forms a circle along the longitudinal direction of the torus skeleton. Denote this set by

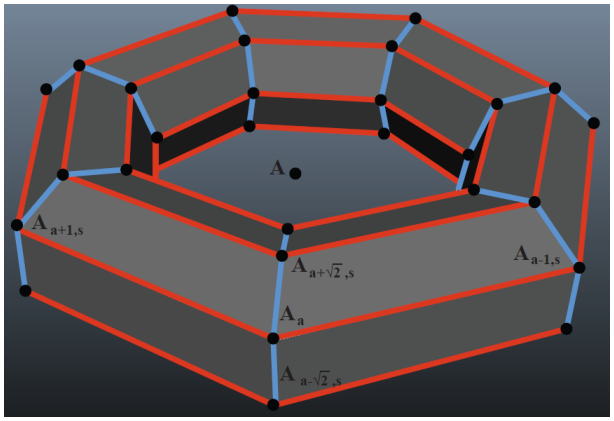

Figure 3.4: Adjacent neighbors of A.

L_a. The blue-adjacencies path cycle $A_{a,s}, A_{a+s,s}, ..., A_{a+(p-1)s,s}, A_{a,s}$ forms a circle along the meridian direction of the torus skeleton. Denote this set by M_a. Thus S can be partitioned as $\{M_a | a \in \mathbb{F}_p\}$ or by fixing an element $a \in \mathbb{F}_{p^2}$, S can also be partitioned as $\{L_x \,|\, x = a + ns, n \in \mathbb{F}_p\}$.

Lemma 3.5.2. *The graph Γ is connected.*

Proof. The proof is similar to the $PSL(2,p)$ case. We show that the component containing A contains more than $|C|/2 = (p^4-1)/4$ elements.

As shown in the $\mathbb{F}_p$ case, for each $a \in \mathbb{F}_{p^2}$, A and $A_{a,s}$ have exactly two neighbors in common, $A_{a-1,s}$ and $A_{a+1,s}$. And for all $a, b \in \mathbb{F}_{p^2}$, $a \neq b$, we have that $A_{a,s}$ and $A_{b,s}$ have two neighbors in common, namely A and $\begin{pmatrix} 1+sx-sax^2 & (ax-1)^2 \\ -2x^2 & 1-sx+sax^2 \end{pmatrix}$, where $x \equiv 2/(a-b) \bmod p^2$.

Now we find a lower bound for the number of elements in the same component as A. We start with A and its p^2 cycle neighbors for a total of p^2+1. Since any two distinct neighbors, $A_{a,s}$ and $A_{b,s}$, of A have exactly one common neighbor, not including A, we can get at least

$$(p^2-3) + (p^2-4) + \cdots + 2 + 1 = (p^2-3)(p^2-2)/2$$

distinct neighbors of $A_{a,s}$ not including A and its neighbors, for all $a \in \mathbb{F}_{p^2}$. Thus we have

at least $(p^4 - 3p^2 + 8)/2$ elements in the same component as A. But this number is strictly bigger than $|C|/2 = (p^4 - 1)/4$, for all p. Thus Γ can have at most one component and hence must be connected. $\square$

Lemma 3.5.3. *The stabilizer of A under the action of $Aut(\Gamma)$ has $4p^2$ elements. In addition, all of the elements of this subgroup can be realized by trivial weak Cayley table isomorphisms.*

In fact, the stabilizer subgroup is isomorphic to $D_{2p} \times D_{2p}$. But we will not need this fact.

Proof. Let $Stab_{Aut(\Gamma)}(A)$ denote the stabilizer of A under the action of $Aut(\Gamma)$. Fix $a = 0 \in \mathbb{F}_p$. Consider the set $L_a = L_0 = \{A_{0,s}, A_{1,s}, A_{2,s}, ..., A_{p-1,s}\}$.

We first show that the subgroup of elements $\phi \in Stab_{Aut(\Gamma)}(A)$ such that $\phi(L_0) = L_0$ has at least $2p$ elements. This is clear since the set of vertices in L_0 forms a p-cycle in Γ. Thus its stabilizer subgroup contains D_{2p}, which has $2p$ elements as required. Moreover, we found in the proof of the $PSL(2, p)$ case, the trivial weak Cayley table isomorphisms can realize all of D_{2p}.

We next show that the subgroup of elements $\phi \in Stab_{Aut(\Gamma)}(A)$ such that $\phi(x) = x$ for all $x \in L_0$ has 2 elements. Pick an element of L_0, say $A_{0,s}$. Since $\phi(A_{0,s}) = A_{0,s}$, we have that $\phi(M_0) = M_0$, where $M_0 = \{A_{0,s}, A_{s,s}, A_{2s,s}, ..., A_{(p-1)s,s}\}$. But M_0 is a p-cycle whose vertex $A_{0,s}$ is fixed under the action of ϕ. Thus the only possibility for the action of ϕ on M_0 is a reflection of the p-cycle in M_0 fixing the vertex $A_{0,s}$. Thus, it suffices to show that if $\phi(A_{s,s}) = A_{s,s}$ then $\phi(A_{t,s}) = A_{t,s}$ for all elements $t \in \mathbb{F}_{p^2}$; that is, ϕ fixes all elements of S. First, since $\phi(A_{s,s}) = A_{s,s}$, we must have that $\phi(A_{t,s}) = A_{t,s}$ for all t such that $t = ns, n \in \mathbb{F}_p$, that is, ϕ fixes all elements of both M_0 and L_0. Now consider an arbitrary element of S, say $A_{r,s}$, where $r = a + bs$, $a, b \in \mathbb{F}_p$. We notice that $M_a = M_r$ and $L_{bs} = L_r$ by definition. Since ϕ fixes all elements of L_0 and M_0, we have that $\phi(A_{a,s}) = A_{a,s}$ and $\phi(A_{bs,s}) = A_{bs,s}$. Thus $\phi(M_a) = \phi(M_r) = M_r$ and $\phi(L_{bs}) = \phi(L_r) = L_r$. But $M_r \cap L_r = \{A_{r,s}\}$. Thus $\phi(A_{r,s}) = A_{r,s}$ as required.

Now we show that the reflection fixing all of L_0 and sending $A_{s,s}$ to $A_{-s,s}$ can be realized by a trivial weak Cayley table isomorphism. Consider the Frobenius field automorphism $\rho : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ given by $\rho(x) = x^p$, for all $x \in \mathbb{F}_{p^2}$. This field automorphism induces an automorphism, $\bar{\rho}$, of $PSL(2, p^2)$, where

$$\bar{\rho}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \rho(a) & \rho(b) \\ \rho(c) & \rho(d) \end{pmatrix} = \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}.$$

We can check that $\bar{\rho}(A) = A$, $\bar{\rho}(A_{t,s}) = A_{t,s}$ for all $A_{t,s} \in L_0$.

We show that $\bar{\rho}(A_{s,s}) = A_{-s,s}$. It suffices to show that $\rho(s) = s^p = -s$. We first state without proof Euler's Criterion [16, Theorem 3.23].

Theorem 3.5.4. *If p is an odd prime, then for arbitrary $a \in \mathbb{Z}$,*

$$a^{(p-1)/2} \equiv (a/p)(mod\ p),$$

where $(a/p) = 1$ if a is a quadratic residue and $(a/p) = -1$ if a is quadratic nonresidue.

Now, $\rho(s) = s^p = (s^2)^{(p-1)/2}s = (2)^{(p-1)/2}s = -s$, where the last equality follows because 2 is a quadratic nonresidue in $\mathbb{F}_{p^2}$.

We now show that the action of $Stab_{Aut(\Gamma)}(A)$ on $S = \{L_0, L_s, L_{2s}, ..., L_{(p-1)s}\}$ is transitive. This is clear since if we let $D = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$, then $D^{-1}AD = A$ and $D^{-1}A_{0,s}D = A_{ns,s}$, for all $n \in \mathbb{F}_p$. Thus $D^{-1}L_0D = L_{ns}$. This shows, in particular, that the orbit under $Stab_{Aut(\Gamma)}(A)$ of L_0 has p elements.

To complete the proof that $|Stab_{Aut(\Gamma)}(A)| = 4p^2$, we show that any element of $Aut(\Gamma)$ fixing all elements of S fixes all of Γ. Let V be some vertex in Γ. If the distance between V and A is 1, then $V \in S$ and we are done. Suppose now that the distance is 2. Let $A_{t,s}, t \in \mathbb{F}_{p^2}$, be an element in S such that $A_{t,s}$ is adjacent to V. Then, as shown in the $PSL(2, p)$ case, V has the form $V = \begin{pmatrix} 1+sx-stx^2 & (tx-1)^2 \\ -2x^2 & 1-sx+stx^2 \end{pmatrix}$ for some $x \in \mathbb{F}_{p^2}$. Now, as argued above, if $b = t - 2/x$ then $A_{a,s}$ and $A_{b,s}$ have exactly two common neighbors, A and V. And since A, $A_{a,s}$ and $A_{b,s}$ are all fixed by ϕ, we must have that $\phi(V) = V$. By repeating

this argument, we get that ϕ fixes all elements in the same component of A. But we proved above that Γ is connected, thus ϕ fixes all of Γ as required.

Thus the stabilizer group of automorphisms of Γ fixing A has size $4p^2$ as required. Moreover, all of the elements of this subgroup can be realized by trivial weak Cayley table isomorphisms. □

Thus, we have that $\mathcal{W}_0(G)$ acting on Γ can realize all of $Aut(\Gamma)$. Thus any weak Cayley isomorphism acting on Γ can be changed by a trivial weak Cayley table isomorphism to give the identity isomorphism. □

3.6 The Coxeter Groups C_n

Set $[n] = \{1, 2..., n\}$. We define the *Coxeter Group of type* C_n as

$C_n = \langle r_0, r_1, ..., r_{n-1} | r_i^2 = 1, 0 \leq i \leq n-1, (r_i r_{i+1})^3 = 1, 1 \leq i \leq n-2, (r_0 r_1)^4 = 1, r_i r_j = r_j r_i, |i-j| \geq 1. \rangle$

However, for clarity, we embed C_n as a subgroup of S_{2n}. As a set of generators for C_n, we take the set

$$\{(12), (13)(24), (35)(46), ..., (2n-3, 2n-1)(2n-2, 2n)\}.$$

Thus, we can view C_n as the group of signed permutation acting on the set of pairs in

$$P = \{\{1, 2\}, \{3, 4\}, ..., \{2n-1, 2n\}\}.$$

The group C_n is a semidirect product of the normal subgroup $K = \langle (12), (34), ..., (2n-1, 2n) \rangle \cong \mathbb{Z}_2^n$ with $H = \langle (13)(24), (35)(46), ..., (2n-3, 2n-1)(2n-2, 2n) \rangle \cong S_n$. Denote these generators of H as

$$\sigma_1 = (13)(24), \sigma_3 = (35)(46), ..., \sigma_{2n-3} = (2n-3, 2n-1)(2n-2, 2n).$$

Thus, $H = \langle \sigma_1, \sigma_3, ..., \sigma_{2n-3} \rangle$. For each generator $\sigma_i = (i, i+2)(i+1, i+3)$ of H, we let $\sigma_i' = (i, i+3)(i+1, i+2)$.

Let C_1 be the class of $(13)(24)$ in C_n and C_2 the class of (12) in C_n. The center of C_n is generated by the involution $z = (12)(34)\cdots(2n-1, 2n)$. Since C_n acts on the n pairs in P, we have that $|C_1| = 2\binom{n}{2} = n(n-1)$ and $|C_2| = n$. There are two classes of C_n of size n, C_2 and zC_2. Let $C = C_1 \cup C_2$.

We show that C_n has only trivial weak Cayley table isomorphisms.

Theorem 3.6.1. *The group $\mathcal{W}(C_n)$ is trivial for all n.*

Proof. Suppose $\phi \in \mathcal{W}(C_n)$. We first show that $\phi(K) = K$. Since $C_2 \subset K$, $zC_2 \subset K$ are the only two classes of size n in C_n, we have that $\phi(C_2 \cup zC_2) = C_2 \cup zC_2$. By 2.1.6, $\phi(K)$ is a normal subgroup of C_n. Thus $\phi(K)$ is a normal subgroup of C_n containing $C_2 \cup zC_2$. But $\langle C_2 \cup zC_2 \rangle = K$. Thus $\phi(K) = K$ as required.

Lemma 3.6.2. *Up to composing with a trivial weak Cayley table isomorphism of C_n, we may assume that $\phi(hK) = hK$ for all $h \in H$.*

Proof. Since $\phi(K) = K$, by Lemma 2.1.6 part (3), for each $h \in H$, we have that $\phi(hK) = h'K$ for some $h' \in H$. By part (4), this induces a weak Cayley table isomorphism $\bar{\phi}$ on $G/K \cong H \cong S_n$. By Theorem 3.1.8, $\bar{\phi}$ is a trivial weak Cayley table isomorphism on H. Thus $\bar{\phi}$ is either an inner automorphism on H or an inner automorphism composed with the inverse map.

In the first case, suppose that $\bar{\phi}$ is an inner automorphism on H, that is, suppose that for some $x \in H$, $\bar{\phi}(h) = h^x$ for all $h \in H$. Then $\phi(hK) = h^x K$ for $h \in H$. Thus by composing with a conjugation by x^{-1} on C_n, we may assume that $\phi(hK) = hK$ for $h \in H$.

In the second case, suppose that $\bar{\phi}$ is an inner automorphism composed with the inverse map. By the argument in the preceding paragraph, without loss, we may assume that $\bar{\phi}$ is the inverse map. Then by composing ϕ with the inverse map on C_n, we may assume that $\phi(hK) = hK$ for all $h \in H$. □

Thus, we may assume that ϕ sends each coset of K to itself.

Lemma 3.6.3. *Up to composing with a trivial weak Cayley table isomorphism, we may assume that* $\phi((13)(24)) = (13)(24)$. *Thus* $\phi(C_1) = C_1$.

Proof. Let $h = (13)(24)$. Since ϕ sends each coset of K to itself, we have that $\phi(h) = hk_h$, for some $k_h \in K$. But $h^2 = 1$, and so $1 = \phi(h^2) \sim \phi(h)^2$, and so $\phi(h)^2 = 1$. Thus, we have $(hk_h)^2 = 1$. Since every element of K is an involution, $k_h \in C_K(h)$. Also we have that $|h^G| = |(hk_h)^G|$ since ϕ sends each class to a class of the same size.

First we show that $C_K(h)$ consists of exactly the elements in K with $(12)(34)$ in the cycle decomposition or the elements of K whose cycle decomposition does not involve elements of the set $\{1, 2, 3, 4\}$. Since $(12)(34)$ centralizes h, we have that this set of elements of K is a subset of $C_K(h)$. But this set has 2^{n-1} elements which is half the size of K. Since (12) does not centralize h, we must have equality. Since $|h^G| = |(hk_h)^G|$, we must have that $k_h \in \{1, z, (12)(34), (12)(34)z\}$.

Thus $\phi(h) = hk_h \in \{h, hz, h(12)(34), h(12)(34)z\}$. By Proposition 2.8 of Franzsen [9], we have that multiplying each generator of H by z while fixing each generator of K is an outer automorphism of C_n. Thus, we may assume that $\phi(h) = hk_h \in \{h = (13)(24), h(12)(34) = (14)(23)\}$. And since $(14)(23)$ is conjugate to $(13)(24)$ by (12), we may assume finally that $\phi((13)(24)) = (13)(24)$. As a consequence, we also have that $\phi(C_1) = C_1$. □

Now we show that ϕ fixes pointwise all of the elements of C_1.

Lemma 3.6.4. *We can compose* ϕ *with some trivial weak Cayley table isomorphism so that for all* $x \in C_1$, $\phi(x) = x$.

Proof. Without loss, we write $x = (a, c)(a + 1, c + 1)$ where $\{a, a + 1\}, \{c, c + 1\} \in P$. Since $x(a, a + 1) = (a, c, a + 1, c + 1)$, $x(c, c + 1) = (a, c + 1, a + 1, c)$ and $x(a, a + 1)(c, c + 1) = (a, c + 1)(c, a + 1)$, we see that the intersection of $x^G = (13)(24)^G$ and xK is the set $\{x = (a, c)(a+1, c+1), (a, c+1)(c, a+1)\}$. Thus $\phi(x) \in \{x = (a, c)(a+1, c+1), (a, c+1)(c, a+1)\}$, for all $x \in (13)(24)^G$. This shows also that $\phi((14)(23)) = (14)(23)$.

We next show that $\phi(\sigma_i) = \sigma_i = (i, i+2)(i+1, i+3)$ and $\phi(\sigma_i') = \sigma_i' = (i, i+3)(i+1, i+2)$ for all odd $i \in [n]$. We already showed that $\phi(\sigma_1) = \phi((13)(24)) = (13)(24) = \sigma_1$. Consider $\sigma_3 = (35)(46)$. As above, we have that $\{\phi((35)(46)), \phi((36)(45))\} = \{(35)(46), (36)(45)\}$. But by conjugating by (56), if necessary, we can assume that $\phi((35)(46)) = (35)(46)$. Notice this conjugation does not effect what ϕ does to the previous generator (13)(24). Similarly by conjugating by (78) if necessary, we can assume that $\phi((57)(68)) = (57)(68)$. Continuing this process, we see that $\phi(\sigma_i) = \sigma_i$ and $\phi(\sigma_i') = \sigma_i'$ for all i odd in $[n]$.

Every element $x \in (13)(24)^G$ determines a swapping of two pairs in P. Given any two pairs in P, say $\{a, a+1\}$ and $\{b, b+1\}$ with $b > a$, define

$$D(\{a, a+1\}, \{b, b+1\} = (b-a)/2.$$

Thus, D measures the distance between any two pairs in P.

For $x \in (13)(24)^G$, write $x = (a, c)(a+1, c+1)$, where $a < c$. We show that $\phi(x) = x$ by induction on $D(\{a, a+1\}, \{c, c+1\})$. If $D(\{a, a+1\}, \{c, c+1\}) = 1$, then $x = \sigma_i$ or $x = \sigma_i'$ for some i odd in $[2n]$. We already showed above that $\phi(x) = x$ in this case. Suppose now that $D(\{a, a+1\}, \{c, c+1\}) = m > 1$ and any swapping of pairings of distance less than m is fixed by ϕ. Pick any pair $\{e, e+1\}$ in P such that $a < e < c$.

Let $y = (a, c, e)(a+1, c+1, e+1)$.

Lemma 3.6.5. *For all x in the class containing y, we have that $\phi(x) = x$.*

Proof. We first show that $\phi(y) \in y^G$. We have $y = (a, c)(a+1, c+1)(a, e)(a+1, e+1)$. Thus, $\phi(y) \sim \phi((a, c)(a+1, c+1))\phi((a, e)(a+1, e+1))$. But we already showed that either $\phi(a, c)(a+1, c+1)$ is $(a, c)(a+1, c+1)$ or $(a, c+1)(a+1, c)$ and $\phi((a, e)(a+1, e+1)) = (a, e)(a+1, e+1)$ by the inductive hypothesis. But in both cases, we see that $\phi(y) \sim y$.

Next we show that

$$y^G \cap yK = \{y, (a, c, e+1)(a+1, c+1, e), (a, c+1, e+1)(a+1, c, e), (a, c+1, e)(a+1, c, e+1)\}.$$

To see this, we note that for $yk_y \in y^G$, then k_y must be in $\{1, (a,a+1)(c,c+1), (a,a+1)(e,e+1), (e,e+1)(c,c+1)\}$.

We now show that $\phi(y)$ can't be equal to any of $(a,c,e{+}1)(a{+}1,c{+}1,e)$, $(a,c{+}1,e{+}1)(a{+}1,c,e)$ or $(a,c{+}1,e)(a{+}1,c,e{+}1)$. To see this, suppose $\phi(y) = (a,c,e{+}1)(a{+}1,c{+}1,e)$. Let $s = (a,e)(a{+}1,e{+}1)$. We have $\phi(s) = s$ by the inductive hypothesis. Then on the one hand, we have $\phi(sy) = \phi((e,c)(e{+}1,c{+}1)) = (e,c)(e{+}1,c{+}1)$ where the last equality follows from the inductive hypothesis. On the other hand, $\phi(sy) \sim \phi(s)\phi(y) = s(a,c,e{+}1)(a{+}1,c{+}1,e) = (a,a{+}1)(e,c,e{+}1,c{+}1)$, which is a contradiction. The same s will similarly give us another contradiction for the second case. Lastly, $s = (e,c)(e+1,c+1)$ will give a contradiction for the third case.

Thus, $\phi(y) = y$. And similarly for elements in the class of y. □

We now continue the proof of Lemma 3.6.4. Suppose, for contradiction, that $\phi(x) = (a,c{+}1)(a{+}1,c)$. Then, on the one hand, $\phi(xy) = \phi((a,e)(a{+}1,e{+}1)) = (a,e)(a{+}1,e{+}1)$ by the inductive hypothesis. On the other hand, $\phi(xy) \sim \phi(x)\phi(y) = (a,c+1)(b,c)(a,c,e)(a+1,d,e+1) = (a,e+1,a+1,e)(c+1,c)$, which is a contradiction. Thus, $\phi(x) = x$ as required. □

Now we want to show that ϕ also fixes pointwise all of C_2.

Lemma 3.6.6. *For all $x \in C_2$, $\phi(x) = x$.*

Proof. We first want to show that $\phi((12)) \in (12)^G$ so that $\phi(C_2) = C_2$.

Suppose first that n is even. By Franzsen [9], we have that multiplying z by each generator of K while fixing each generator of H is an outer automorphism of C_n. Thus if $\phi((12)) \in ((12)z)^G$, then by applying the automorphism, we may assume that $\phi((12)) \in (12)^G$ as required.

Suppose now that n is odd so that $n = 2m+1$ for some m. The above argument cannot be used since no such automorphism exists for this case. Define D_1 to be the class of $(13)(24)$.

For $i > 1$ such that $4i < 2n = 4m + 2$, define D_i to be the class of $(13)(24)(57)(68)\cdots(4i - 3, 4i - 1)(4i - 2, 4i)$. We showed above that for all $x \in D_1$, we have $\phi(x) = x$.

Lemma 3.6.7. *Suppose for $x \in D_i$, we have that $\phi(x) = x$. Then for $x \in D_{i+1}$, we have $\phi(x) = x$.*

Proof. Without loss, we write $x \in D_{i+1}$ as

$$x = (13)(24)(57)(68)\cdots(4i + 1, 4i + 3)(4i + 2, 4i + 4) = \sigma_1\sigma_5\cdots\sigma_{4i+1}.$$

Then $x = (13)(24)y$ where $y \in D_i$. But by assumption, $\phi(13)(24) = (13)(24)$ and $\phi(y) = y$. Thus, we have $\phi(x) = \phi((13)(24)y) \sim \phi((13)(24))\phi(y) = (13)(24)y = x$. Thus $\phi(x) \sim x$. Since $xk_x \in x^G$ only if $k_x \in \{1, (12)(34), ..., (4i + 1, 4i + 2)(4i + 3, 4i + 4)\}$, this being the set of elements of K whose cycle decomposition contains the pairings in the cycle decomposition of x, we have $\phi(x) = \sigma_1^*\cdots\sigma_{4i-3}^*$, where σ_j^* is either σ_j or σ_j'. It suffices to show that $\sigma_j^* = \sigma_j$ for all j. For a fixed j, we have that $\sigma_j x = \sigma_1\cdots\sigma_{j-1}\sigma_{j+1}\cdots\sigma_{4i+1} \in D_i$. Thus $\phi(\sigma_j x) = \sigma_j x$. We also have $\phi(\sigma_j x) \sim \phi(\sigma_j)\phi(x) = \sigma_j\phi(x)$. Thus $\sigma_j x \sim \sigma_j\phi(x)$. But this is true only if $\sigma_j^* = \sigma_j$. □

Lemma 3.6.7 proves that we can fix pointwise all of the classes D_i with $4i < 2n$. Now we show that for $n = 2m + 1$ odd, we have $\phi((12)) \in (12)^G$. Consider the class D_m. Since n is odd, we have that $(12)z \in D_m^2$. Write $(12)z = st$ with $s, t \in D_m$. We proved above in Lemma 3.6.7 that $\phi(s) = s$ and $\phi(t) = t$. Thus $\phi((12)z) = \phi(st) \sim \phi(s)\phi(t) = st = (12)z$. Thus $\phi((12)z) \sim (12)z$ and $\phi((12)) \sim (12)$ as required.

Suppose $\phi((12) = (r, r + 1)$ for some odd $r \geq 3$. Consider $\sigma_r = (r, r + 2)(r + 1, r + 3)$. We proved above in Lemma 3.6.4 that $\phi(\sigma_r) = \sigma_r$. We have $\phi(\sigma_r(12)) \sim \phi(\sigma_r)\phi((12)) = \sigma_r(r, r + 1) = (r, r + 2, r + 1, r + 3)$. But if $r \neq 1$, the size of the class $\sigma_r(12)$ is $(n - 2)|\sigma_r^G|$ and the size of the class $(r, r + 2, r + 1, r + 3)$ is only $|\sigma_r^G|$. Thus $\phi(12) = (12)$ as required. Similarly for the rest of the conjugates of (12), we have $\phi((12)^g) = (12)^g$. □

Since $C = C_1 \cup C_2$, we have just proven that for $x \in C$, $\phi(x) = x$. We next show that ϕ fixes pointwise all of the elements of C^2. Our strategy proceeds as follows. Let $x \in C^2$. We first show that $\phi(x) \sim x$. To see this, we write $x = rs$, $r, s \in C$. But $\phi(x) = \phi(rs) \sim \phi(r)\phi(s) = rs = x$. In addition, since $\phi(x) \in xK$, we must have that $\phi(x) \in x^G \cap xK$. Next, we pick $t \in C$ such that $tx \in C$ so that $\phi(s) = s$ and $\phi(tx) = tx$. Thus, we must have

$$tx = \phi(tx) \sim \phi(t)\phi(x) = t\phi(x). \tag{3.6}$$

We will then check that none of the elements in $x^G \cap xK$ except x satisfies the necessary condition of Equation (3.6).

Lemma 3.6.8. *For all $x \in C^2, \phi(x) = x$.*

Proof. The classes in C^2 have the following set of representatives,

$$\{(12)(34), (13)(24)(57)(68), (135)(246), (13)(24)(56), (1423)\}.$$

We show that ϕ fixes each representative and the proof will follow exactly the same for the other elements of the class. We already showed in Lemma 3.6.5 that ϕ fixes pointwise every element of the class (135)(246). By Lemma 3.6.7, we also showed that ϕ fixes pointwise the whole class of (13)(24)(57)(68). We now consider the remaining three cases.

Suppose $x = (12)(34)$. Then $\phi(x) = (i, i+1)(j, j+1)$. Let $s = (34)$. Then $\phi(s) = s$. By Equation (3.6), we have $\phi(x)(34) \sim (12)$. This shows that $\phi(x)$ takes the form $(34)(i, i+1)$ for some odd $i \in [2n]$. Now let $s = (12)$ and the same calculation shows that $\phi(x)$ takes the form $(12)(i, i+1)$. Thus $\phi(x) = x$ as required.

Let $x = (13)(24)(56)$. We have in this case that $x^G \cap xK$ consists of elements of the form $(a, c)(a+1, c+1)(e, e+1)$ where $\{a, a+1\}$,$\{c, c+1\}$ and $\{e, e+1\}$ are distinct pairs in P. Let $s = (13)(24)$. Then Equation (3.6) gives us $(13)(24)\phi(x) \sim (56)$. This shows $\phi(x)$ has the form $(13)(24)(i, i+1)$. If we let $s = (34)$, the same calculation will give us $\phi(x) = x$.

Finally suppose $x = (1423)$. But $x^G \cap xK = \{x, (1324)\}$. Consider $s = (145)(236)$. We already know that $\phi(s) = s$ by Lemma 3.6.5. Suppose for contradiction that $\phi(x) =$

(1324). Then $\phi(xs) = \phi((15)(26)(34)) = (15)(24)(34)$, where the last equality comes from the previous case. On the other hand, $\phi(xs) \sim \phi(x)\phi(s) = (1324)s = (1625)$, which is a contradiction. Thus, $\phi(x) = x$. □

Lemma 3.6.9. *For all* $x \in C^3, \phi(x) = x$.

Proof. There are ten types of classes in C^3 not covered in C and C^2 cases. These types have the following set of representatives,

$$\{(12)(34)(56), (13)(24)(56)(78), (1324)(56), (14)(23)(56)(79)(8,10),$$
$$(135)(246)(78), (135246), (13)(24)(57)(68)(9,11)(10,12),$$
$$(13)(24)(5867), (1357)(2468), (13)(24)(579)(68,10)\}.$$

Since we can fix C and C^2, for all x in C^3, we have $\phi(x) \sim x$.

Suppose $x = (12)(34)(56)$. Since $\phi(x) \sim x$, we have that $\phi(x) = (i, i+1)(j, j+1)(k, k+1)$. Let $s = (34)(56)$. We have that $\phi(s) = s$. Also Equation (3.6) gives us $(i, i+1)(j, j+1)(k, k+1)s \sim (12)$. Thus we must have that $\phi(x) = (34)(56)(k, k+1)$. If we let $s = (12)$, then the same calculation gives us $(34)(56)(c, c+1)(12) \sim (34)(56)$. But this forces $\phi(x) = x$.

Suppose $x = (13)(24)(56)(78)$ and let $s = (56)(78)$. Then $\phi(x)$ has the form $(a, c)(b, d)(e, e+1)(f, f+1)$, where $\{a, b\}$ and $\{c, d\}$ are pairs in P and $(e, e+1), (f, f+1) \in (12)^G$. We have $\phi(x)s \sim (13)(24)$. This implies that $\phi(x) = (a, c)(b, d)(56)(78)$. Now let $s = (13)(24)$. Then $s\phi(x) \sim (56)(78)$ which gives us $\phi(x) = (13)(24)(56)(78)$.

Suppose $x = (1324)(56)$. Let $s = (1423)$. We have that $\phi(sx) = \phi((56)) = (56)$. We also have by Equation (3.6) $(1423)\phi(x) \sim (56)$. This gives us $\phi(x) = (1324)(i, i+1)$. Now let $s = (56)$. And $\phi(x)s \sim (1324)$ gives us $\phi(x) = x$.

Let $x = (14)(23)(56)(7, 9)(8, 10)$. For k_x satisfying the property $xk_x \sim x$, k can change the $(13)(24)$ part of x by having $(12)(34)$ in its decomposition or similarly the $(79)(8, 10)$ part by having $(78)(9, 10)$. In addition, k can switch out (56) with another pair of reflection $(i, i+1)$. Let $(13)(24)'$ denote either possibility $(13)(24)$ or $(14)(23)$ and $(79)(8, 10)'$ either

$(79)(8,10)$ or $(7,10)(89)$. Then an arbitrary conjugate of x lying in xK takes the form $(13)(24)'(79)(8,10)'(i,i+1)$. We then use $s=(14)(23)(79)(8,10)$ to get $\phi(x)s \sim (56)$. This implies that $\phi(x)$ must take the form $(14)(23)(79)(8,10)(i,i+1)$. Apply the condition again to $s=(56)$ will give us $\phi(x)=x$.

Let $x=(135)(246)(78)$. In this case, k_x can have any of $\{(12)(34),(12)(56),(34)(56)\}$ in its decomposition to change the $(135)(246)$ part of x and $(78)(i,i+1)$ to switch out (78) for $(i,i+1)$. But as before, $s=(153)(264)$ and $t=(78)$ will eliminate all but x as a possibility for $\phi(x)$.

The next five types are easy to deal with and the method used to prove that ϕ fixes each of them is the same. Suppose we want to fix x. We then show that $|x^G \cap xK|$ is either 4 or 8 independent of n. And since we know that $\phi(x) \in x^G \cap xK$, there are only 4 or 8 choices for $\phi(x)$. We then pick $s,t \in C$ or C^2 and use the necessary condition from Equation 3.6 to eliminate all but x in $x^G \cap xK$.

Let $x=(135246)$. We show that $|x^G \cap xK|=4$. Suppose that $k \in K$ is such that $xk \sim x$. Write $k=(k_1,k_1+1)\cdots(k_r,k_r+1)$. We then see that if for any pair of reflection $\{k_i,k_i+1\}$ that is not a subset of $[6]$, then $xk \nsim x$. We then can compute that $r=2$ and the only possibilities are $\{1,(12)(34),(12)(56),(34)(56)\}$. Thus $x^G \cap xK = \{x,x(12)(34),x(12)(56),x(34)(56)\}$. Now let $s=(13)(24)$ and $t=(15)(26)$, we can check that the only element that satisfies the necessary condition of Equation (3.6) is x.

Let $x=(13)(24)(57)(68)(9,11)(10,12)$. In this case, for $xk \sim x$, k must have in decomposition any combination of $(12)(34),(56)(78),(9,10)(11,12)$ and nothing else for a total of 8 possibilities. We then check the condition of Equation 3.6 for $s=(57)(68)(9,11)(10,12)$ and $t=(13)(24)(57)(68)$ to see that $\phi(x)=x$ is the only possibility.

Let $x=(13)(24)(5867)$. In this case, k must have in its decomposition only elements in $\{(12),(34),(56),(78)\}$. We can check that identity, any two pairs in that set and all four pairs are the only possibilities for a total of 8 elements in the intersection of the class of x and the coset xK. And of those, x is the only element that satisfies the condition in Equation (3.6)

for $s = (13)(24)$ and $t = (5768)$.

Let $x = (1357)(2468)$. This case yields the same set of possibilities for k as in the previous case for a total of 8. But we have to use three elements to eliminate all but x, namely, $s = (13)(24)$, $t = (57)(68)$, and $r = (35)(46)$.

Finally, $x = (13)(24)(579)(6, 8, 10)$. In this case, k can have either $(12)(34)$ in its decomposition to change $(13)(24)$ part of x or any of $\{(56)(78), (56)(9, 10), (78)(9, 10)\}$ to change the $(579)(6, 8, 10)$ but still have $xk \sim x$. Thus, there are again 8 possibilities for $\phi(x)$ and only x satisfies the necessary condition of Equation (3.6) using $s = (13)(24)$ and $t = (597)(6, 10, 8)$. □

Lemma 3.6.10. *For all $x, y \in G$, $x \neq y$ and $x \sim y$, there exists $c \in C \cup C^2$ such that $cx \nsim cy$.*

Proof. Suppose a pair say $\{1, 2\}$ is in the decomposition for x. We show that $\{1, 2\}$ must occur in the decomposition of y in the same way else we can find $c \in C \cup C^2$ such that $cx \nsim cy$. More precisely, we show that

1) If $x = (1, a_1)(2, b_1)x_1$ then $y = (1, c_1)(2, d_1)y_1$ where $|a_1| = |c_1| = |b_1| = |d_1|$, or

2) If $x = (1, a_1, 2, b_1)x_1$ then $y = (1, c_1, 2, d_1)y_1$ where $|a_1| = |c_1| = |b_1| = |d_1|$.

Since $(12)(1, a_1, 2, b_1) = (1, b_1)(2, a_1)$ and $(12)(1, a_1)(2, b_1) = (1, b_1, 2, a_1)$ we see that unless the above statements are true, $(12)x \nsim (12)y$.

Suppose now that $\{3, 4\}$ also occurs in the decomposition for x.

Lemma 3.6.11. *Suppose that we are in case (1) above so that*

$$x = (1, a_1, 3, a_2)(2, b_1, 4, b_2)x_1.$$

Then $y = (1, c_1, 3, c_2)(2, d_1, 4, d_2)y_1$ with $|a_1| = |c_1|$ else we can find a $c \in C \cup C^2$ such that $cx \nsim cy$.

Proof. If $y = (1, c_1)(2, d_1)(3, c_2)(4, d_2)y_1$, then $(13)(24)x = (1, a_2)(3, a_1)(2, b_2)(4, b_1)x_1 \nsim (13)(24)y = (1, c_2, 3, c_1)(2, d_2, 4, d_1)y_1$. Thus we have that both $\{1, 2\}$ and $\{3, 4\}$ must occur in the same two cycles in both x and y, that is $x = (1, a_1, 3, a_2)(2, b_1, 4, b_2)x_1$ and y is either $(1, c_1, 3, c_2)(2, d_1, 4, d_2)y_1$ or $(1, c_1, 4, c_2)(2, d_1, 3, d_2)y_1$. But if y takes on the form of the second case then $(13)(24)x \nsim (13)(24)y$. Thus, if

$$x = (1, a_1, 3, a_2)(2, b_1, 4, b_2)x_1$$

then $y = (1, c_1, 3, c_2)(2, d_1, 4, d_2)y_1$.

We show next that $|a_1| = |c_1|$. Let $c = (135)(246)$ and $d = (153)(264)$. Then we can check that $cx \sim cy$ only if either $|c_1| = |a_1|$ or $|a_2| = |c_1| + 1$. The first case gives us the result. If $|a_2| = |c_1| + 1$, then $dx \sim dy$ only if $|c_1| = |a_1|$. □

Lemma 3.6.12. *Suppose that we are in case 2) above so that*

$$x = (1, a_1, 3, a_2, 2, a_3, 4, a_4)x_1.$$

Then $y = (1, c_1, 3, c_2, 2, c_3, 4, c_4)y_1$ *where* $|a_1| = |c_1|$ *else we can find a* $c \in C \cup C^2$ *such that* $cx \nsim cy$.

Proof. If y is $(1, b_1, 2, b_2)(3, c_1, 4, c_2)y_1$ or $(1, b_1, 2, b_2)(3, c_1)(4, c_2)y_1$ then $(1, 3)(2, 4)x \nsim (1, 3)(2, 4)y$. Thus we must have that $y = (1, b_1, 3, b_2, 2, b_3, 4, b_4)y_1$ or

$$y = (1, b_1, 4, b_2, 2, b_3, 3, b_4)y_1.$$

We show that the second case can't happen. To see this, we suppose that

$$y = (1, b_1, 4, b_2, 2, b_3, 3, b_4)y_1.$$

We consider $c = (135)(246) \in C^2$. We have then that $cx \sim cy$ only if $|a_1| = |b_4| - 1$ and

$|a_2| = |b_1| + 1$. And if we let $d = (153)(264) \in C^2$, then $dx \sim dy$ only if $|a_1| = |b_4| + 1$ and $|a_2| = |b_1| - 1$. But these two cases are mutually exclusive. Thus we see that if $y = (1, b_1, 4, b_2, 2, b_3, 3, b_4)y_1$, then there exists a $c \in C^2$ such that $cx \nsim cy$.

Now we show that $x = (1, a_1, 3, a_2, 2, a_3, 4, a_4)x_1$ and $y = (1, c_1, 3, c_2, 2, c_3, 4, c_4)y_1$ where $|a_1| = |c_1|$. Let $c = (135)(246) \in C^2$. Then we have that $cx \sim cy$ only if $|a_1| = |c_1|$. □

The above lemmas show, in particular, that if $\{1, 2\}$ and $\{3, 4\}$ occur in the cycle decomposition of x, then they must also occur in the same way in the cycle decomposition of y and their ordering and relative distance must be the same in both cycle decompositions. But this force $x = y$. Thus, if $x \neq y$, $x \sim y$, then there exists a $c \in C \cup C^2$ so that $cx \nsim cy$ as required.

□

□

3.7 The Coxeter Groups B_n

The Coxeter group B_n is an index 2 normal subgroup of the Coxeter group C_n. We keep the notation from the previous section for C_n. The generators are all the generators of $H \leq C_n$, where $H = \langle (13)(24), (35)(46), ..., (2n-3, 2n-1)(2n-2, 2n) \rangle \cong S_n$ and the even reflections in $K \leq C_n$, that is, the set $\langle (12)(34), (12)(56), ..., (12)(2n-1, 2n) \rangle$. Thus, B_n is a semidirect product of the normal subgroup $K_1 \cong \mathbb{Z}_2^{n-1}$ and $H \cong S_n$. For n even, the group B_n has nontrivial center generated by $z = (12)(34) \cdots (2n-1, 2n)$. For n odd, B_n has trivial center.

We prove that B_n has only trivial weak Cayley table isomorphisms. The proof follows the same basic structure as the proof for the group C_n. We let C_1 be the class of $(13)(24)$ in B_n and C_2 the class of $(12)(34)$ in B_n. And let $C = C_1 \cup C_2$.

Theorem 3.7.1. *The group $\mathcal{W}(B_n)$ is trivial for all $n \geq 4$.*

Proof. As in the proof of Lemma 3.6.2, since $B_n/K_1 \cong S_n$, we assume that ϕ sends each coset of K_1 to itself.

Lemma 3.7.2. *Up to composing with a trivial weak Cayley isomorphism, we have that* $\phi((13)(24)) = (13)(24)$. *Thus* $\phi(C_1) = C_1$.

Proof. Let $h = (13)(24) \in C_1$. Suppose first that n is even. The first part of the proof of Lemma 3.6.3 we showed that $\phi(h) = hk_h \in \{h, hz, h(12)(34), h(12)(34)z\}$. By Proposition 2.8 of Franzsen [9], we have that multiplying each generators of H by z while fixing each generator of K is an outer automorphism of B_n. Thus, we may assume that $\phi(h) = hk_h \in \{h = (13)(24), h(12)(34) = (14)(23)\}$. Since $(14)(23)$ is conjugate to $(13)(24)$ by $(12)(56)$, we may assume finally that $\phi((13)(24)) = (13)(24)$. As a consequence, we also have that $\phi((14)(23)) = (14)(23)$ and $\phi((13)(24)^G) = (13)(24)^G$.

Suppose now that n is odd. Since B_n has trivial center in this case, the same argument above shows that $\phi(h) = hk_h \in \{h, h(12)(34) = (14)(23)\}$. And as above, since $(14)(23)$ is conjugate to $(13)(24)$ by $(12)(56)$, we may assume finally that $\phi((13)(24)) = (13)(24)$. □

We now show that ϕ fixes pointwise all of the elements of C_1.

Lemma 3.7.3. *For all* $x \in C_1$, $\phi(x) = x$.

Proof. The proof of Lemma 3.6.4 follows through exactly as in the C_n case. We note that the above proof also shows that ϕ fixes pointwise all of the elements of the class of $(135)(246)$. □

We next show that ϕ fixes pointwise all of the elements of C_2.

Lemma 3.7.4. *For all* $x \in C_2$, $\phi(x) = x$.

Proof. Let $x \in C_2$. Without loss of generality, we write $x = (12)(34)$. We have $\phi((12)(34)) = \phi((13)(24)(14)(23)) \sim \phi((13)(24))\phi((14)(23)) = (13)(24)(14)(23) = x$. Thus, $\phi(x) \sim x$ and $\phi(C_2) = C_2$. Now suppose that $\phi(x) = (a, a+1)(b, b+1) \in C_2$. On the one hand, we have $\phi(x(13)(24)) = \phi((14)(23)) = (14)(23)$. But on the other hand, we have $\phi(x(13)(24)) \sim \phi(x)\phi((13)(24)) = (a, a+1)(b, b+1)(13)(24)$. Thus, $(14)(23) \sim (a, a+1)(b, b+1)(13)(24)$. But this is true only if $(a, a+1)(b, b+1) = (12)(34)$. Thus $\phi((12)(34)) = (12)(34)$, as required. □

Since $C = C_1 \cup C_2$, we have shown above that for all $x \in C$, $\phi(x) = x$.

Lemma 3.7.5. *For all $x \in C^2$, $\phi(x) = x$.*

Proof. The classes in C^2 can be represented by the following set of elements,

$$\{(12)(34), (14)(23), (135)(246), (12)(34)(56)(78),$$
$$(14)(23)(56)(78), (14)(23)(57)(68), (1423)(56)\}.$$

We already showed that ϕ fixes pointwise all of the classes of $(12)(34), (14)(23), (135)(246)$. As before, since $x \in C^2$, we have that $\phi(x) \sim x$. Suppose that $x \in (12)(34)(56)(78)^G$. Without loss of generality, we write $x = (12)(34)(56)(78)$. Suppose that $\phi(x) = (a, a+1)(b, b+1)(c, c+1)(d, d+1)$. Let $t = (12)(34)$. Then $\phi(tx) = \phi((56)(78)) = (56)(78)$. But $\phi(tx) \sim \phi(t)\phi(x) = t(a, a+1)(b, b+1)(c, c+1)(d, d+1)$. Thus, we have $(12)(34)(a, a+1)(b, b+1)(c, c+1)(d, d+1) \sim (56)(78)$. But this is true only if $(a, a+1)(b, b+1)(c, c+1)(d, d+1) = (12)(34)(c, c+1)(d, d+1)$. Similarly, if $t = (56)(78)$, then the same argument will give us that $\phi(x) = x$.

Suppose now that $x = (14)(23)(56)(78)$. Suppose that $\phi(x) = (a, b)(a+1, b+1)(c, c+1)(d, d+1)$. Let $t = (14)(23)$. Then $\phi(tx) = \phi((56)(78)) = (56)(78)$. But $\phi(tx) \sim \phi(t)\phi(x) = (14)(23)(a, b)(a+1, b+1(c, c+1)(d, d+1)$. Thus, we have $(56)(78) \sim (14)(23)(a, b)(a+1, b+1(c, c+1)(d, d+1)$. But this is true only if $(a, b)(a+1, b+1(c, c+1)(d, d+1) = (14)(23)(c, c+1)(d, d+1)$. If we let $t = (56)(78)$, the same argument will force $\phi(x) = x$.

Suppose that $x = (14)(23)(57)(68)$. Suppose that $\phi(x) = (a, b)(a+1, b+1)(c, d)(c+1, d+1)$. Let $t = (14)(23)$ so that, as above, $(57)(68) \sim (14)(23)(a, b)(a+1, b+1)(c, d)(c+1, d+1)$. But this implies that $(a, b)(a+1, b+1)(c, d)(c+1, d+1) = (14)(23)(c, d)(c+1, d+1)$. The same argument using $t = (57)(68)$ forces $\phi(x) = x$.

Suppose that $x = (1423)(56)$. Write $\phi(x) = (a, b, a+1, b+1)(c, c+1)$. Let $t = (13)(24)$ so that $(12)(56) \sim (a, b, a+1, b+1)(c, c+1)(13)(24)$. But this implies that $(a, b, a+1, b+1)(c, c+1) = (1423)(c, c+1)$. Now letting $t = (12)(56)$ will force $\phi(x) = x$. □

Lemma 3.7.6. *For all $x \in C^3, \phi(x) = x$.*

Proof. The classes in C^3 not already covered in the C and C^2 cases can be represented by the following elements:

$$\{(12)(34)(56)(78)(9,10)(11,12), (14)(23)(56)(78)(9,10)(11,12),$$
$$(14)(23)(57)(68)(9,10)(11,12), (1423)(5867), (1423)(56)(78)(9,10),$$
$$(14)(23)(5768)(9,10), (146)(235)(78)(9,10), (146235)(78)\}.$$

As before, we have $\phi(x) \sim x$ for all $x \in C^3$. The first three cases are straightforward. Suppose $x = (12)(34)(56)(78)(9,10)(11,12)$. Let $s = (56)(78)(9,10)(11,12)$ so that s satisfies Equation (3.6). But this gives us $s\phi(x) \sim (12)(34)$. Thus, $\phi(x)$ must take on the form $(i, i+1)(j, j+1)(56)(78)(9,10)(11,12)$. Letting $t = (13)(24)$ in Equation (3.6) will force $\phi(x) = x$.

Let $x = (14)(23)(56)(78)(9,10)(11,12)$. If we let $s = (56)(78)(9,10)(11,12)$ and $t = 14)(23)$ and use Equation (3.6) above, we have that x is the only element in $x^G \cap xK$ that satisfies that necessary condition.

Let $x = (14)(23)(57)(68)(9,10)(11,12)$. Let $s = (14)(23)(57)(68)$ and

$$t = (9,10)(11,12)$$

will force $\phi(x) = x$.

The next case where $x = (1423)(5867)$ is the easiest case to deal with since $|x^G \cap xK| = 4$ independent of n. To eliminate all but x we use $s = (1324)(56)$ and $t = (5768)(12)$.

The remaining four cases are more involved since the set $x^G \cap xK$ is generally bigger and has a variety of different elements.

Let $x = (1423)(56)(78)(9,10)$. Then elements of $x^G \cap xK$ take on the form $(1423)'(i, i+1)(j, j+1)(k, k+1)$, where $(1423)'$ denotes either (1423) or (1324). To eliminate the (1324) possibility and force $(i, i+1) = (56)$, we use $t = (1324)(56)$ and to force $(j, j+1)(k, k+1) =$

$(78)(9,10)$ we take $s = (78)(9,10)$.

Let $x = (14)(23)(5768)(9,10)$. The set $x^G \cap xK$ consists of elements of the form $(13)(24)'(5867)'$ or $(1423)'(57)(68)'$ where $(13)(24)'$ denotes either $(13)(24)$ or $(14)(23)$, $(5867)'$ denotes either (5867) or its inverse, $(1423)'$ denotes (1423) or its inverse, and $(57)(68)'$ denotes $(57)(68)$ or $(58)(67)$. Letting $s = (14)(23)$ and $t = (5867)(9,10)$ will force $\phi(x) = x$.

Let $x = (146)(235)(78)(9,10)$. Then

$$x^G \cap xK = \{(135)(246)(i,i+1)(j,j+1), (136)(245)(i,i+1)(j,j+1), (145)(236)(i,i+1)(j,j+1), (146)(235)(i,i+1)(j,j+1)\}.$$

Letting $s = (164)(235)$ and $t = (78)(9,10)$ will give us $\phi(x) = x$.

Finally, $x = (146235)(78)$. Then

$$x^G \cap xK = \{(135246)(i,i+1), (136245)(i,i+1), (145236)(i,i+1), (146235)(i,i+1)\}.$$

We need three elements $r = (16)(25)$, $s = (12)(78)$ and $t = (13)(24)$ to eliminate all but x in $x^G \cap xK$. □

Lemma 3.7.7. *For all $x, y \in G$, $x \neq y$ and $x \sim y$, there exists $c \in C$ or C^2 such that $cx \nsim cy$.*

Proof. The proof of this lemma follows exactly as the C_n case. The only difference is instead of using the class (12) in C_n, we use the class $(12)(34)$ in B_n. □

□

Chapter 4. The Sporadic Groups

Let G be the Mathieu group of degree 11, M_{11}, with $7,920$ elements. We show that the group $\mathcal{W}(G)$ is trivial. We view M_{11} as a subgroup of A_{11}:

$$M_{11} = \langle (1,10)(2,8)(3,11)(5,7), (1,4,7,6)(2,11,10,9) \rangle.$$

We will rely on Magma to do most of our computations. All of the code for the following computations is included in the Appendix.

Let C be the class of $(1,6,8)(3,4,9)(5,11,7)$ in G. Then C has 440 elements. We show that M_{11} and C satisfy the three conditions of the following lemma.

Lemma 4.0.8. *Let G be a group and C a nontrivial class of G. Suppose that for any $\phi \in \mathcal{W}(G)$, there exists $\alpha \in \mathcal{W}_0(G)$ such that:*

(i) $\alpha\phi(x) = x$, for all $x \in C$.

(ii) $\alpha\phi(x) \sim x$, for all $x \in G$,

(iii) For all $x \neq y$, $x \sim y$, there exists $c \in C$ such that $cx \nsim cy$.

Then $\mathcal{W}(G)$ is trivial.

Theorem 4.0.9. *For the Mathieu group, $G = M_{11}$, the group $\mathcal{W}(G)$ is trivial.*

Proof. We define a graph Γ whose vertices are elements of C. Two vertices, M and N, of Γ are connected by an edge if $MN \in C$.

We first note that any element of $\mathcal{W}(G)$ acts as a graph automorphism on Γ. To see this, suppose $\phi \in \mathcal{W}(G)$. Since C is the only class in G whose size is 440, we have that $\phi(C) = C$. Then for any $M, N \in C$ connected by an edge, that is, $MN \in C$, we have $\phi(MN) \sim \phi(M)\phi(N)$. Since $\phi(MN) \in C$, we have that $\phi(M)\phi(N) \in C$. Thus $\phi(M), \phi(N)$ are also connected by an edge in Γ.

By Magma, $|Aut(\Gamma)| = 15,840 = 2|G|$ while $|Aut(G)| = 7,920 = |G|$. Since G is simple, this implies that the automorphism group of G is composed of only inner automorphisms.

In particular, we have that $|\mathcal{W}_0(G)| = 15,840$ since $\mathcal{W}_0(G) = \langle Aut(G), \mathcal{I} \rangle$. Thus $|\mathcal{W}_0(G)| = |Aut(\Gamma)|$. And since we showed above that any automorphism or anti-automorphism is a graph automorphism of Γ, this shows that any graph automorphism of Γ can be realized by an element of $\mathcal{W}_0(G)$. Now we check the first condition of the above lemma. Suppose $\phi \in \mathcal{W}(G)$. Then ϕ acts as an automorphism on Γ. But any graph automorphism of Γ can be realized by an element of $\mathcal{W}_0(G)$, say α. Thus, by composing with α^{-1} if necessary, we may assume that $\phi(x) = x$ for all $x \in C$.

To check the second condition, we show that $C^2 = \{xy : x, y \in C\} = G$. To see why this suffices, suppose $x \in G$. Since $C^2 = G$, we have that $x = rs$ for some $r, s \in C$. Since r, s are elements of C, we have, by the first condition, that $\phi(r) = r$ and $\phi(s) = s$. Thus, $\phi(x) = \phi(rs) \sim \phi(r)\phi(s) = rs = x$, as required.

A check by Magma shows, indeed, that $C^2 = G$.

Finally, we show that for all $x \neq y$, $x \sim y$, there exists $c \in C$ such that $cx \nsim cy$. Again, this is a simple Magma check. See the Appendix for the Magma code. □

We now show that the Mathieu group $G = M_{12}$ has only trivial weak Cayley table isomorphisms. We view M_{12} as a subgroup of the alternating group A_{12} generated by the set

$$\langle (1,2,3,4,5,6,7,8,9,10,11), (1,9)(2,6)(4,5)(7,8), (1,10)(2,5)(3,7)(4,8)(6,9)(11,12) \rangle.$$

The Mathieu group M_{12} has $95,040$ elements. Let C be the conjugacy class of

$$(2,5,10)(6,8,9)(7,12,11)$$

and C_2 be the class of

$$(1,11)(2,9)(3,12)(4,6)(5,10)(7,8).$$

Then C is the only class with $1,760$ elements and C_2 is the only class with 396 elements.

Theorem 4.0.10. *The group $\mathcal{W}(M_{12})$ is trivial.*

Proof. As before, we define a graph Γ whose vertices are elements of C. Two vertices, M and N, of Γ are connected by an edge if $MN \in C_2$.

In this case, a Magma computation shows that $|Aut(\Gamma)| = 380,160$ and $|Aut(G)| = 190,080$. Thus, $|\mathcal{W}_0(G)| = |\langle Aut(G), \mathcal{I}\rangle| = Aut(\Gamma)$. And thus, any action on Γ by a weak Cayley table isomorphism has an inverse in $\mathcal{W}_0(G)$. Thus we have checked the first condition of Lemma 4.0.8.

A Magma calculation shows that $C^2 = G \setminus D$, where D is the class of

$$(1,8,4,7,11,3,5,10,6,9)(2,12).$$

As above, for any $x \in C^2$, we have that $\phi(x) \sim x$. And since ϕ sends classes to classes, the fact that $C^2 = G \setminus D$ shows that $\phi(D) = D$ and thus $\phi(x) \sim x$ for any $x \in G$. A Magma check shows that the last condition of Lemma 4.0.8 is also satisfied. □

We show that the Mathieu group $G = M_{22}$, where $|G| = 443,520$, has only trivial weak Cayley table isomorphisms. The generators of G as a subgroup of A_{22} are

$$\{(1,2,4,8,16,9,18,13,3,6,12)(5,10,20,17,11,22,21,19,15,7,14),$$
$$(1,18,4,2,6)(5,21,20,10,7)(8,16,13,9,12)(11,19,22,14,17),$$
$$(1,18,2,4)(3,15)(5,9)(7,16,21,8)(10,12,20,13)(11,17,22,14)\}.$$

In this case, we let C be the class of

$$(1,12,19)(2,9,13)(4,22,7)(5,10,16)(8,20,15)(11,21,17),$$

with unique size $12,320$. Let C_2 be the unique class of involutions with $1,155$ elements.

Theorem 4.0.11. *The group $\mathcal{W}(M_{22})$ is trivial.*

Proof. As before, we define a graph Γ whose vertices are elements of C. Two vertices, M and N, of Γ are connected by an edge if $MN \in C_2$.

Since Magma shows that $|Aut(\Gamma)| = 1,774,080$ and

$$|Aut(G)| = 887,040 = 1/2|Aut(\Gamma)|,$$

we see that the trivial weak Cayley table isomorphisms can realize all of the automorphisms of the graph Γ. Thus, the first condition of Lemma 4.0.8 is satisfied.

Magma shows that $C^2 = G$. Thus for $x \in G$, we have that $\phi(x) \sim x$ and the second condition is satisfied. The last condition is similarly checked by Magma. □

We next show that the first simple group of Janko, J_1, also has only trivial weak Cayley table isomorphisms. This group is embedded in the alternating group of degree 266 and has size $175,560$. Let C be the class of

(1, 167, 120, 133, 203, 155, 198, 240, 119, 224, 33)(2, 16, 34, 26,138, 94, 196, 184, 249, 29, 124) (3, 208, 230, 67, 150, 79, 114, 194,36, 222, 221)(4, 175, 159, 263, 144, 136, 185, 158, 251, 172, 69) (5,179, 13, 256, 62, 212, 30, 178, 207, 65, 73)(6, 258, 191, 219, 56,52, 262, 244, 148, 160, 41) (7, 90, 183, 190, 134, 96, 32, 49, 106,218, 55)(8, 95, 238, 128, 137, 266, 48, 140, 126, 254, 264) (9, 46,109, 17, 50, 157, 14, 131, 70, 195, 84)(10, 27, 66, 202, 11, 187,104, 170, 139, 75, 193) (12, 177, 210, 82, 63, 214, 85, 231, 20, 182,116)(15, 227, 259, 163, 201, 110, 253, 100, 197, 23, 44) (18, 80, 77,186, 181, 211, 200, 260, 122, 92, 76)(19, 213, 43, 111, 42, 232,252, 25, 168, 250, 123) (21, 180, 237, 223, 118, 22, 246, 234, 58,54, 228)(24, 117, 135, 47, 233, 173, 147, 87, 261, 68, 102) (28, 107,45, 241, 64, 243, 74, 83, 255, 143, 129)(31, 108, 88, 161, 99, 216,86, 169, 205, 59, 164) (35, 145, 152, 242, 78, 188, 132, 226, 105,154, 265)(37, 235, 229, 93, 149, 146, 40, 239, 225, 60, 153) (38,130, 192, 53, 113, 165, 220, 217, 72, 209, 257)(39, 91, 162, 204,236, 156, 101, 247, 142, 127, 174) (51, 166, 215, 115, 206, 61, 248,81, 171, 199, 176)(57, 189, 125, 103, 89, 245, 71, 97, 121, 151,141) with $15,960$ elements and C_2 be the unique class of involutions in G.

Theorem 4.0.12. *The group $\mathcal{W}(J_1)$ is trivial.*

Proof. The vertices of the graph Γ are elements of C and two vertices of Γ, M and N, are

connected by an edge if their product MN is in C_2.

Since $|Aut(\Gamma)| = 351,120$ and $|Aut(G)| = 175,560 = 1/2|Aut(\Gamma)|$, we see that the trivial weak Cayley table isomorphisms can realize all of the automorphisms of the graph Γ. Thus, the first condition of Lemma 4.0.8 is satisfied.

Magma shows that $C^2 = G$. Thus for $x \in G$, we have that $\phi(x) \sim x$ and the second condition of Lemma 4.0.8 is satisfied. The last condition is similarly checked by a short Magma program. □

The second simple group of Janko, J_2, also has trivial weak Cayley table isomorphisms. This group can be viewed as a subgroup of A_{100} and has size $604,800$. We let C be the class of

(2, 96, 37)(3, 11, 33)(4, 78, 48)(5, 7, 53)(6, 75, 83)(8, 63, 16)(9,44, 32)(10, 21, 79)(13, 19, 39) (14, 23, 95)(15, 97, 17)(18, 49,52)(20, 61, 80)(22, 69, 28)(24, 25, 82)(26, 50, 56)(27, 42, 86) (29, 62, 77)(30, 40, 54)(31, 35, 73)(36, 60, 85)(38, 46, 87)(41, 66,92)(43, 67, 84)(45, 72, 71) (47, 90, 88)(51, 99, 81)(55, 65, 74)(57,89, 58)(59, 98, 76)(64, 100, 70)(91, 93, 94) with $16,800$ elements and C_2 be the unique class of involutions of size 315.

Theorem 4.0.13. *The group $\mathcal{W}(J_2)$ is trivial.*

Proof. The vertices of the graph Γ are elements of C and two vertices M and N are connected by an edge if $MN \in C_2$.

We have that $|Aut(\Gamma)| = 2,419,200$ and $|Aut(G)| = 1/2|Aut(\Gamma)|$. Thus, as before, all of the automorphisms of Γ can be realized by trivial weak Cayley table isomorphisms and the first condition is proven.

The second condition is satisfied since Magma does show that $C^2 = G$. The last condition is similarly checked by Magma. □

Appendix A. Conjugacy Classes of $PSL(2, p^n)$

The conjugacy classes of G is given in the following lemma. A proof can be found in [7].

Lemma A.0.14. *Let $G = PSL(2, p^n)$ where p is an odd prime. Let $z = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and ϵ be a generator of $\mathbb{F}_{p^n}^*$. Then G has exactly $p^n + 4$ classes given in Tables A.1 and A.2.*

$g \in G$	Notation	$\lvert g^G \rvert$	$\lvert C_G(g) \rvert$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	I	1	$p^n(p^{2n}-1)/2$
$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	C	$(p^{2n}-1)/2$	p^n
$\left(\begin{smallmatrix} 1 & \epsilon \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	D	$(p^{2n}-1)/2$	p^n
$\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix}\right)^n \langle z \rangle$	L^n	$p^n(p^n+1)$	$(p^n-1)/2$
$\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix}\right)^{(p^n-1)/4} \langle z \rangle$	$L^{(p^n-1)/4}$	$p^n(p^n+1)/2$	(p^n-1)
$\left(\begin{smallmatrix} x & y \\ y\epsilon & x \end{smallmatrix}\right)^m \langle z \rangle$ $x \neq \pm 1, y \neq 0$	B^m	$p^n(p^n-1)$	$(p^n+1)/2$

Table A.1: Conjugacy Classes of $PSL(2, p^n)$, $p \equiv 1 \bmod 4$, where $1 \leq n \leq (p^n-5)/4$ and $1 \leq m \leq (p^n-1)/4$.

$g \in G$	Notation	$\lvert g^G \rvert$	$\lvert C_G(g) \rvert$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	I	1	$p^n(p^{2n}-1)/2$
$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	C	$(p^{2n}-1)/2$	p^n
$\left(\begin{smallmatrix} 1 & \epsilon \\ 0 & 1 \end{smallmatrix}\right)\langle z \rangle$	D	$(p^{2n}-1)/2$	p^n
$\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix}\right)^n \langle z \rangle$	L^n	$p^n(p^n+1)$	$(p^n-1)/2$
$\left(\begin{smallmatrix} x & y \\ y\epsilon & x \end{smallmatrix}\right)^m \langle z \rangle$, $x \neq \pm 1, y \neq 0$	B^m	$p^n(p^n-1)$	$(p^n+1)/2$
$\left(\begin{smallmatrix} x & y \\ y\epsilon & x \end{smallmatrix}\right)^{(p^n+1)/4} \langle z \rangle$, $x \neq \pm 1, y \neq 0$	$B^{(p^n+1)/4}$	$p^n(p^n-1)/2$	(p^n+1)

Table A.2: Conjugacy Classes for $PSL(2, p^n)$, $p \equiv 3 \bmod 4$ where $1 \leq n \leq (p^n-3)/4$ and $1 \leq m \leq (p^n-3)/4$.

Appendix B. Character Tables of $PSL(2, p^n)$

The character table of $PSL(2, p^n)$ is given in the following lemma [7].

Lemma B.0.15. *Let p be an odd prime. Let $\rho \in \mathbb{C}$ be a $(p-1)$th root of unity and $\sigma \in \mathbb{C}$ be a $(p+1)$th root of unity. Then the character table of $G = PSL(2, p^n)$ is given in Tables B.1 and B.2.*

	I	C	D	L^n	$L^{(p^n-1)/4}$	B^m
1_G	1	1	1	1	1	1
ψ	p^n	0	0	1	1	-1
χ_i	p^n+1	1	1	$\rho^{in}+\rho^{-in}$	$\rho^{i(p^n-1)/4}+\rho^{-i(p^n-1)/4}$	0
θ_j	p^n-1	-1	-1	0	0	$-\sigma^{jm}-\sigma^{-jm}$
ζ_1	$\frac{p^n+1}{2}$	$\frac{1+\sqrt{p^n}}{2}$	$\frac{1-\sqrt{p^n}}{2}$	$(-1)^n$	$(-1)^{(p^n-1)/4}$	0
ζ_2	$\frac{p^n+1}{2}$	$\frac{1-\sqrt{p^n}}{2}$	$\frac{1+\sqrt{p^n}}{2}$	$(-1)^n$	$(-1)^{(p^n-1)/4}$	0

Table B.1: The Character Table for $PSL(2, p^n)$, $p \equiv 1 \bmod 4$ where $i = 2, 4, 6, ..., (p^n - 5)/2$, $j = 2, 4, 6, ..., (p^n - 1)/2$, $1 \leq n \leq (p^n - 5)/4$ and $1 \leq m \leq (p^n - 1)/4$.

	I	C	D	L^n	B^m	B^k
1_G	1	1	1	1	1	1
ψ	p^n	0	0	1	-1	-1
χ_i	p^n+1	1	1	$\rho^{in}+\rho^{-in}$	0	0
θ_j	p^n-1	-1	-1	0	$-\sigma^{jm}-\sigma^{-jm}$	$-\sigma^{jk}-\sigma^{-jk}$
η_1	$\frac{p^n-1}{2}$	$\frac{-1+\sqrt{p^n}}{2}$	$\frac{-1-\sqrt{p^n}}{2}$	0	$(-1)^{(m+1)}$	$(-1)^{k+1}$
η_2	$\frac{p^n-1}{2}$	$\frac{-1-\sqrt{p^n}}{2}$	$\frac{-1+\sqrt{p^n}}{2}$	0	$(-1)^{(m+1)}$	$(-1)^{k+1}$

Table B.2: The Character Table for $PSL(2, p^n)$, $p \equiv 3 \bmod 4$ where $i = 2, 4, 6, ..., (p^n - 3)/2$, $j = 2, 4, 6, ..., (p^n - 3)/2$, $1 \leq n \leq (p^n - 3)/4$, $1 \leq m \leq (p^n - 3)/4$ and $k = (p^n + 1)/4$.

Appendix C. $PSL(2,p)$

For completeness, we provide the proof that $\mathcal{W}(PSL(2,p))$ is trivial for all primes p. Let $G = PSL(2,p)$ where p is a prime.

Proposition C.0.16. *Let $\phi \in \mathcal{W}(G)$. There exists $\alpha \in \mathcal{W}_0(G)$ such that $\alpha\phi(x) = x$ for all $x \in C$.*

Proof. We first treat the case $p \equiv 1 \bmod 4$. We note that this implies that -1 is a quadratic residue [16, Therem 5.3].

We define a graph Γ as follows. The vertices of Γ are elements of the class C. Two vertices M, N are connected by an edge if $MN \in C$. We show that ϕ acts as an automorphism of Γ. By assumption, ϕ is a bijection. Recall that we may assume $\phi(C) = C$. Suppose M, N are adjacent in Γ so that $MN \in C$. By assumption, $\phi(MN) \in C$. But $\phi(MN) \sim \phi(M)\phi(N)$, thus $\phi(M)\phi(N) \in C$ and $\phi(M), \phi(N)$ are also adjacent.

We analyze the graph Γ. Consider the vertex $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of Γ. Since $\phi(A) \in C$, after conjugating if necessary, we may assume that $\phi(A) = A$. We investigate the immediate neighbors of A. Any element of C is conjugate to A and can be written in the form

$$A_{a,c} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix},$$

for some $a, c \in \mathbb{F}_p$.

Thus a neighbor of A would have to satisfy one of the following two equations.

$$AA_{a,c} = \begin{pmatrix} 1-ac-c^2 & a^2+1+ac \\ -c^2 & 1+ac \end{pmatrix} = \begin{pmatrix} 1-ef & e^2 \\ -f^2 & 1+ef \end{pmatrix} = A_{e,f} \tag{C.1}$$

or,

$$AA_{a,c} = -A_{e,f}, \tag{C.2}$$

for some $e, f \in \mathbb{F}_p$.

Equation $(C.1)$ gives four equations,

$$1 - ac - c^2 = 1 - ef, \tag{C.3}$$

$$a^2 + 1 + ac = e^2, \tag{C.4}$$

$$-c^2 = -f^2, \tag{C.5}$$

$$1 + ac = 1 + ef. \tag{C.6}$$

Adding $(C.3)$ and $(C.6)$ gives $2 - c^2 = 2$, and thus $c = 0$. It follows that $ef = 0$ and so $f = 0$. Thus, $A_{a,0} = \left(\begin{smallmatrix} 1 & a^2 \\ 0 & 1 \end{smallmatrix}\right)$ is a neighbor of A for $a \neq \pm 1, a \neq 0, a \in \mathbb{F}$, such that $a^2 + 1 = e^2$ for some $e \neq 0 \in \mathbb{F}_p$. We call these neighbors the *noncycle neighbors* of A, for reasons that will be clear later.

Equation $(C.2)$ gives us another four equations,

$$1 - ac - c^2 = -1 + ef, \tag{C.7}$$

$$a^2 + 1 + ac = -e^2, \tag{C.8}$$

$$-c^2 = f^2, \tag{C.9}$$

$$1 + ac = -1 - ef. \tag{C.10}$$

Since $p \equiv 1 \bmod 4$, Equation $(C.9)$ above does have nonzero solutions. As before, adding $(C.7)$ and $(C.10)$ gives $c = \pm 2$. Thus, if we let $c = 2$ then $A_{a,2}$ is a neighbor of A for all $a \in \mathbb{F}_p$ such that $(C.10)$ holds. But since f is nonzero by Equation (C.9), e is determined by a and thus $A_{a,2} = \left(\begin{smallmatrix} 1-2a & a^2 \\ -4 & 1+2a \end{smallmatrix}\right)$ is a neighbor of A for all a. If we let $c = -2$, we show that we do not get any new neighbors. In this case, we have $A_{a,-2} = \left(\begin{smallmatrix} 1+2a & a^2 \\ -4 & 1-2a \end{smallmatrix}\right)$ is a neighbor of A for all a. But $A_{a,2} = A_{-a,-2}$. Thus, $A_{a,2}$ for all values of $a \in \mathbb{F}_p$ gives us a second type of neighbors to A. We call these neighbors the *cycle neighbors* of A.

Next we show that the cycle neighbors of A and the noncycle neighbors of A are not

adjacent. Suppose $A_{a,2}$ is a cycle neighbor of A for some a and $A_{b,0}$ is a noncycle neighbor of A for some $b \neq \pm 1$. Since

$$A_{a,2}A_{b,0} = \left(\begin{smallmatrix} 1-2a & -4 \\ b^2-2ab^2+a^2 & -4b^2+1+2a \end{smallmatrix}\right)$$

is an element of C only if $b = \pm 1$, we have a contradiction. Thus, the cycle neighbors and noncycle neighbors of A are not adjacent.

Lemma C.0.17. *The graph* Γ *is connected.*

Proof. Suppose that Γ decomposes into multiple components. We first notice that these components must have the same size since any two vertices of the graph are images of each other by an automorphism of G. Thus to show that Γ has only one component, we only need to show that the component containing A contains more than $|C|/2 = (p^2-1)/4$ elements.

We show that the neighbors of A of the form $A_{a,2}$, that is, the cycle neighbors of A, form a cycle of length p around A, where $A_{a,2}$ is adjacent to $A_{a+1,2}$, for all $a \in \mathbb{F}_p$. We can check that $A_{a,2}A_{a+1,2} = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, which is in C, since $p \equiv 1 \bmod 4$.

Each cycle neighbor $A_{a,2}$ of A, has its own cycle neighbors. These can be found by conjugating by a fixed element D such that $D^{-1}AD = A_{a,2}$. If we let $D = \left(\begin{smallmatrix} 0 & b \\ -2 & a \end{smallmatrix}\right)$, where $2b \equiv 1 \bmod p$, then we have that $D^{-1}AD = A_{a,2}$. Thus the cycle neighbors of $A_{a,2}$ are

$$D^{-1}A_{x,2}D = \begin{pmatrix} 1+2x-2ax^2 & (ax-1)^2 \\ -4x^2 & 1-2x+2ax^2 \end{pmatrix},$$

$x \in \mathbb{F}_p$.

Now, we show that for each $a \in \mathbb{F}_p$, A and $A_{a,2}$ have exactly two cycle neighbors in common, $A_{a-1,2}$ and $A_{a+1,2}$. To see this, we suppose that $D^{-1}A_{x,2}D$ is a cycle neighbor of both $A_{a,2}$ and A. Then the trace of $AD^{-1}A_{x,2}D$ must be -2. But the trace of $AD^{-1}A_{x,2}D$ is $2-4x^2$. Thus, $x = \pm 1$. But substituting $x = \pm 1$ into $D^{-1}A_{x,2}D$ give $A_{a-1,2}$ and $A_{a+1,2}$ as required.

Next, for all $a, b \in \mathbb{F}_p$, $a \neq b$, we show that $A_{a,2}$ and $A_{b,2}$ have two cycle neighbors in

common, namely A and $\begin{pmatrix} 1+2x-2ax^2 & (ax-1)^2 \\ -4x^2 & 1-2x+2ax^2 \end{pmatrix}$, where $x \equiv -2/(b-a) \bmod p$. To see this, we solve

$$\begin{pmatrix} 1+2x-2ax^2 & (ax-1)^2 \\ -4x^2 & 1-2x+2ax^2 \end{pmatrix} = \begin{pmatrix} 1+2y-2by^2 & (by-1)^2 \\ -4y^2 & 1-2y+2by^2 \end{pmatrix}.$$

This gives $y = \pm x$ from the $(2,1)$ entry. But since $a \neq b$, from the $(1,2)$ entry, we have either $y = x = 0$ or $y = -x$. The first case gives A as a common cycle neighbor. In the second case, we substitute $y = -x$ into the above matrices and equate their $(1,1)$ entries to get

$$-2ax^2 + 1 + 2x = -2bx^2 + 1 - 2x.$$

This gives $x \equiv -2/(b-a) \bmod p$, as required.

Now we find a lower bound for the number of elements in the same component as A. We start with A and its p cycle neighbors for a total of $p+1$ elements. Since any two distinct cycle neighbors, $A_{a,2}$ and $A_{b,2}$, of A have exactly one common cycle neighbor, not including A, we have that we can get at least

$$(p-3) + (p-4) + \cdots + 2 + 1 = (p-3)(p-2)/2$$

distinct cycle neighbors of $A_{a,2}$ not including A and its cycle neighbors, for all $a \in \mathbb{F}_p$. Thus we have at least $(p^2 - 3p + 8)/2$ elements in the same component as A. But this number is strictly bigger than $|C|/2 = (p^2-1)/4$, for all p. Thus Γ can have at most one component and hence must be connected. □

Lemma C.0.18. *The stabilizer of A under the action of $Aut(\Gamma)$ is isomorphic to the dihedral group of order $2p$, D_{2p}.*

Proof. We first show that D_{2p} is a subgroup of the stabilizer group. Let $P = \left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right)$, where $d = -1/s$. Then P commutes with A and we can check that $P^{-1}AP = A$ and $P^{-1}A_{a,s}P = A_{a+1,s}$, for all a. Thus conjugating by P rotates Γ about A. Now let $Q = \left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & x \end{smallmatrix}\right)$, where $x^2 = -1$. Then, by composing the inverse map with conjugation by Q, we get the map

$\beta : \Gamma \to \Gamma$, which sends A to itself and $A_{a,s}$ to $Q^{-1}A_{a,s}^{-1}Q = A_{-a,s}$, realizing a reflection fixing A's cycle neighbor $A_{0,s}$.

We next show that the elements of D_{2p} are the only automorphisms that fix A. To do this, we show that any automorphism fixing A and its cycle neighbors fixes all of Γ.

We suppose that A and all of its cycle neighbors $A_{a,2}$, for all $a \in \mathbb{F}_p$ are fixed. We will show that any element of distance less than or equal to two from A is also fixed. To do this, we will show that all of the cycle and noncycle neighbors of $A_{a,2}$ are fixed for all a, and all of the noncycle neighbors $A_{e,0}$ of A and their cycle and noncycle neighbors are also fixed.

We now show that since A and all of its cycle neighbors $A_{a,2}$ are fixed, all of the cycle neighbors for $A_{a,2}$ for all $a \in \mathbb{F}_p$ are also fixed. This is clear since for each fixed a, each of $A, A_{a-1,2}$ and $A_{a+1,2}$ is part of the cycle neighbors for $A_{a,2}$ and is fixed by assumption. Thus all of the cycle neighbors of $A_{a,2}$ are fixed.

Now we show that all of the noncycle neighbors, $A_{e,0}$, of A for all $e \in \mathbb{F}_p$ such that $e^2 + 1$ is a square in $\mathbb{F}_p$ and their cycle neighbors are fixed. We first show that for any given $b \in \mathbb{F}_p$, the $A_{e,0}$'s cycle neighbors meet with exactly two cycle neighbors of $A_{b,2}$. As we have shown before, the cycle neighbors of $A_{b,2}$ take the form

$$\begin{pmatrix} 1+2x-2bx^2 & (bx-1)^2 \\ -4x^2 & 1-2x+2bx^2 \end{pmatrix},\ x \in \mathbb{F}_p.$$

Conjugating by $\left(\begin{smallmatrix} 1/e & 0 \\ 0 & e \end{smallmatrix}\right)$ sends the cycle neighbors of A to the cycle neighbors of $A_{e,0}$, which take the form

$$\begin{pmatrix} 1-2a & a^2e^2 \\ -4/e^2 & 1+2a \end{pmatrix}, \text{ for all } a \in \mathbb{F}_p.$$

Thus by equating the above matrices, we see that the two cycle neighbors of $A_{b,2}$ given by $x = \pm 1/e$ are also the same two cycle neighbors of $A_{e,0}$ given by $a = \dfrac{b \pm e}{e^2}$. Thus given any noncycle neighbor $A_{e,0}$ of A, we can find say two different cycle neighbors of A, $A_{b_1,2}$ and $A_{b_2,2}$ whose cycle neighbors meet with exactly four cycle neighbors of $A_{e,0}$. But the cycle neighbors of $A_{b_1,2}$ and $A_{b_2,2}$ are fixed, thus forcing the cycle neighbors of $A_{e,0}$ to be fixed. This also shows that $A_{e,0}$ itself is fixed.

Applying this same argument to $A_{a,2}$ for all a shows that all of the noncycle neighbors of $A_{a,2}$ are also fixed. And applying this argument to $A_{e,0}$ shows that their noncycle neighbors are also fixed.

Thus, we have shown that any automorphism of Γ all of elements of C of distance at most 2 away from A are fixed. By fixing A and its cycle neighbors fixes all vertices distance less than or equal to 2 away from A. Thus, by repeating the argument, we have shown that all vertices connected to A are fixed. And since Γ is connected, all of Γ is fixed. □

We have just shown by Lemma C.0.18 that $\mathcal{W}_0(G)$ can realize all of the elements of the stabilizer group, D_{2p}, fixing A. Thus, we have that $\mathcal{W}_0(G)$ acting on Γ can realize all of $Aut(\Gamma)$.

Now, we prove Proposition C.0.16. The weak Cayley table isomorphism ϕ acts as an automorphism on Γ. Since $\mathcal{W}_0(G)$ can realize any element of $Aut(\Gamma)$, let α be the element of $\mathcal{W}_0(G)$ which is the inverse element of ϕ in $Aut(\Gamma)$. Then $\alpha\phi(x) = x$, for all $x \in C$ as required. □

For the case, $p \equiv 3 \bmod 4$, the proof is the same except for the construction of Γ. In this case, we define two elements $A, B \in C$ to be connected by an edge if $AB \in D$. The rest of the proof follows as before.

Appendix D. Magma Code

We include here the Magma code for checking the last condition of Lemma 4.0.8.

```
load "M11";
g:=G;
x:=g!(1, 6, 8)(3, 4, 9)(5, 11, 7);
cc:=Classes(g);
tf:=false;
for i in {2..#cc} do
        x:=cc[i][3];
        c1:=Class(g,x);
       for y in c1 do
            if(not x eq y) then
            tf:=false;
                for z in c do
                if(not IsConjugate(g,z*x,z*y)) then
                tf:=true; break;
                end if;
                end for;
            if(tf eq false) then
            print i,tf;
            end if;
            end if;
       end for;
end for;
```

Bibliography

[1] Brown, Kenneth. *Cohomology Groups*. Springer-Verlag, New York Inc. 1982.

[2] Camina, A.R. *Some Conditions Which Almost Characterize Frobenius Groups*. Israel Journal of Mathematics, vol 31, No 2, pp 153-160. 1978.

[3] Chillag, David; Macdonald, I.D. *Generalized Frobenius Groups*. Israel Journal of Mathematics, vol 4, Nos. 2-3, 1984.

[4] Chillag, David; Mann, Avinoam; Scoppola, Carlo. *Generalized Frobenius Groups II*. Israel Journal of Mathematics, vol 62, No. 3, 1988.

[5] Dark, Rex and Scoppola, Carlo. *On Camina Groups of Prime Power Order*. Journal Of Algebra, 181, pp 787-802. 1996.

[6] Donovan, Elizabeth. *Various Parameters of Subgraphs and Supergraphs of the Hypercube*. Dissertation. Northeastern University, Boston.

[7] Dornhoff, Larry. *Group Representation Theory*. M. Dekker, 1972.

[8] Dummit, David and Foote, Richard. *Abstract Algebra*. John Wiley and Sons, Inc. 2004.

[9] Franzsen, William. *Automorphisms of Coxeter Groups*. Ph.D. Dissertation. School of Mathematics and Statistics, University of Sydney. 2001.

[10] Gorenstein, Daniel. *Finite Groups*. Chelsea Publishing Company, New York, N.Y.

[11] Humphries, Stephen. *Weak Cayley Table Groups*. Journal of Algebra, 228, pp 135-158. 1999.

[12] Isaacs, I. Martin. *Finite Group Theory*. Graduate Studies in Mathematics, Volume 92. American Mathematical Society. Providence, Rhode Island.

[13] Isaacs, I. Martin. *Character Theory of Finite Groups*. Graduate Studies in Mathematics, Volume 92. American Mathematical Society. Providence, Rhode Island. 2006.

[14] James, Gordon and Liebeck, Martin. *Representations and Characters of Groups*. Cambridge.

[15] Johnson, Kenneth; Mattarei, Sandro and Sehgal, Surinder. Weak Cayley Tables. Journal of the London Mathematical Society, 61, pp 395-411. 2000.

[16] LeVeque, William. *Fundamentals of Number Theory*. Dover Publications, Inc. New York.

[17] Macdonald, I.D. *Some p-Groups of Frobenius and Extra-Special Type*. Israel Journal of Mathematics, vol 40, Nos. 3-4, 1981.

[18] Scott, William Raymond. *Group Theory*. Englewood Cliffs, New Jersey. Prentice Hall, 1964.