



All Theses and Dissertations

---

2015-06-01

# Topics Pertaining to the Group Matrix: $k$ -Characters and Random Walks

Randall Dean Reese

*Brigham Young University - Provo*

Follow this and additional works at: <https://scholarsarchive.byu.edu/etd>



Part of the [Mathematics Commons](#)

---

## BYU ScholarsArchive Citation

Reese, Randall Dean, "Topics Pertaining to the Group Matrix:  $k$ -Characters and Random Walks" (2015). *All Theses and Dissertations*. 5570.

<https://scholarsarchive.byu.edu/etd/5570>

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact [scholarsarchive@byu.edu](mailto:scholarsarchive@byu.edu), [ellen\\_amatangelo@byu.edu](mailto:ellen_amatangelo@byu.edu).

Topics Pertaining to the Group Matrix:  $k$ -Characters and Random Walks

Randall D. Reese

A thesis submitted to the faculty of  
Brigham Young University  
in partial fulfillment of the requirements for the degree of  
Master of Science

Stephen Humphries, Chair  
David Cardon  
Pace Nielsen

Department of Mathematics  
Brigham Young University  
June 2015

Copyright © 2015 Randall D. Reese  
All Rights Reserved

## ABSTRACT

Topics Pertaining to the Group Matrix:  $k$ -Characters and Random Walks

Randall D. Reese  
Department of Mathematics, BYU  
Master of Science

Linear characters of finite groups can be extended to take  $k$  operands. The basics of such a  $k$ -fold extension are detailed. We then examine a proposition by Johnson and Sehgal [29] pertaining to these  $k$ -characters and disprove its converse.

Probabilistic models can be applied to random walks on the Cayley groups of finite order. We examine random walks on dihedral groups which converge after a finite number of steps to the random walk induced by the uniform distribution. We present both sufficient and necessary conditions for such convergence and analyze aspects of algebraic geometry related to this subject.

Keywords:  $k$ -characters, group determinant, random walks, branched covering

# CONTENTS

<b>Contents</b>	<b>iii</b>
<b>List of Tables</b>	<b>iv</b>
<b>List of Figures</b>	<b>v</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Introduction and History . . . . .	1
1.2 Representations . . . . .	1
1.3 Characters . . . . .	2
<b>2 <math>k</math>-Characters: The Preliminaries</b>	<b>5</b>
2.1 The Group Matrix . . . . .	5
2.2 Factoring the Group Determinant . . . . .	8
<b>3 A Conjecture on <math>k</math>-Characters</b>	<b>14</b>
3.1 Proposal and Conjecture . . . . .	14
3.2 The $S_k$ Filigree . . . . .	16
3.3 Proof of Theorem 3.4 . . . . .	26
3.4 The Cases $k = 5, 6$ and Conjecture 3.3 . . . . .	30
<b>4 <math>k</math>-Characters of Several Groups and the Associated Group Determinant</b>	<b>32</b>
4.1 The Dihedral Groups . . . . .	32
4.2 The Non-abelian Groups of Order $p^3$ . . . . .	38
4.3 The Group $AGL(1, p)$ . . . . .	42
<b>5 Random Walks on Finite Groups</b>	<b>45</b>
5.1 Definitions and Preliminaries . . . . .	45
5.2 The Dihedral Group $D_{2q}$ . . . . .	49
<b>6 Further Questions for Future Examination</b>	<b>77</b>
<b>A Cross Sections of 4-fold Cover Over the Variables <math>x_9, x_{10}</math>, and <math>x_{11}</math></b>	<b>78</b>
<b>B MAGMA Code</b>	<b>87</b>
B.1 Code for Solving $e^2 = 0$ in $D_{2q}$ . . . . .	87
B.2 Code for Finding Branch Curve Projections . . . . .	89
<b>Bibliography</b>	<b>91</b>

## LIST OF TABLES

1.1	Regular Character for $G$ . . . . .	3
1.2	Character Table $D_{10}$ . . . . .	4
2.1	Irreducible Characters of $D_8$ . . . . .	12
3.1	Admissible Polynomials for $\pi^{(2)}$ . . . . .	15
3.2	Admissible Polynomials for $\pi^{(3)}$ . . . . .	23
3.3	Admissible Polynomials for $\pi^{(4)}$ . . . . .	25
4.1	Character Table $D_{2n}$ for $n$ <b>odd</b> . . . . .	32
4.2	Character Table $D_{2n}$ for $n$ <b>even</b> . . . . .	33
4.3	Character Table for non-abelian groups of order $p^3$ . . . . .	38
4.4	Character Table for $AGL(1, p)$ , $p$ an odd prime . . . . .	44
5.1	Labeling the Elements of $D_{2q}$ . . . . .	49
5.2	Character Table of $D_{2q}$ . . . . .	54
5.3	Branch Curve types for $D_{14}$ . . . . .	76

## LIST OF FIGURES

3.1	The $S_3$ filigree . . . . .	22
3.2	Using the $S_3$ filigree to find an admissible polynomial (I) . . . . .	22
3.3	Using the $S_3$ filigree to find an admissible polynomial (II) . . . . .	23
3.4	The $S_4$ Filigree . . . . .	24
4.1	The $S_3$ filigree for $\phi_u^{(3)}$ : Central Products . . . . .	41
5.1	The 2-simplex for $x_5$ and $x_6$ . . . . .	57
5.2	Explicit 2-simplex for $x_5$ and $x_6$ under constraint $x_i \geq -\frac{1}{6}$ . . . . .	58
5.3	Subspace of solutions to $e^2 = 0$ ( $D_{10}$ ) . . . . .	61
5.4	Space containing solutions to $e^2 = 0$ ( $D_{14}$ ) . . . . .	64
5.5	Projections of subset of branch points $(x_9, x_{10}, x_{11})$ . . . . .	68
5.6	Projections of subset of branch points $(x_9, x_{11}, x_{12})$ . . . . .	72
5.7	Projections of subset of branch points $(x_{10}, x_{11}, x_{12})$ . . . . .	74
A.1	Cross sections of 4-fold cover in $x_9, x_{10}, x_{11}$ . . . . .	78

# CHAPTER 1. INTRODUCTION

## 1.1 INTRODUCTION AND HISTORY

Following preliminary work by C.F. Gauss and R. Dedekind, representation theory was formalized by F.G. Frobenius about 120 years ago in a series of seminal papers published in 1896 and 1897 (See [5, p. 41,59],[12]). Frobenius' work focused on the factorization of the group determinant and generalized the representation theory of finite abelian groups to that of *any* finite group. Scholars such as Burnside, Maschke, Schur,<sup>1</sup> and Brauer furthered the field of representation theory leading into the twentieth century.

In this thesis we consider several topics relevant to the group matrix, namely factoring the group determinant (Chapters 2 to 4) and random walks on finite groups (Chapter 5). The thesis concludes with suggestions for further research (Chapter 6).

## 1.2 REPRESENTATIONS

Throughout this work,  $G$  is an arbitrary finite group.  $\mathbb{R}$  and  $\mathbb{C}$  represent the real and complex numbers respectively. Unless otherwise noted,  $p$  can be taken to be a prime integer. We use  $\rho$  to denote a representation, as defined below.

**Definition 1.1.** A *representation* of a group  $G$  over a finite-dimensional complex vector space  $V$  is a homomorphism  $\rho$  from  $G$  to  $\text{GL}(V)$ .

The *degree* of  $\rho$  is the dimension of  $V$ . We say that  $\rho$  is *irreducible* if the corresponding  $\mathbb{C}G$ -module given by  $vg = v \cdot \rho(g)$  (with  $v \in V$ ,  $g \in G$ ) is non-zero and has no  $\mathbb{C}G$ -submodules besides  $\{0\}$  and  $V$ . As is seen by this notation our action will be on the right.

**Proposition 1.2.** *Any representation of degree 1 is irreducible.*

*Proof.* Let  $\rho$  be a degree 1 representation. Then  $\rho$  must correspond to a  $\mathbb{C}G$  module of

---

<sup>1</sup>A student of Frobenius!

dimension 1 over  $\mathbb{C}$ . As the only submodules of such a  $\mathbb{C}G$  module are  $\{0\}$  and the whole module,  $\rho$  must be irreducible.  $\square$

**Proposition 1.3.** [25, p. 82] *If  $G$  is abelian, every irreducible representation of  $G$  has dimension 1.*

**Definition 1.4.** Two representations  $\rho_1 : G \rightarrow GL(V)$  and  $\rho_2 : G \rightarrow GL(V)$  are said to be *equivalent* (or *similar*) if there is a  $T \in GL(V)$  such that  $T \circ \rho_1(g) \circ T^{-1} = \rho_2(g)$  for all  $g \in G$ . This is equivalent to the associated  $\mathbb{C}G$  modules of  $\rho_1$  and  $\rho_2$  being isomorphic (see [8, p. 846–847].)

**Definition 1.5.** One fundamental representation is the *trivial representation*. The trivial representation takes all elements of  $G$  to the identity element of  $GL(\mathbb{C})$ .

**Definition 1.6.** Another important representation is the *regular representation*. The regular representation is given by the natural action of  $G$  on the group algebra  $\mathbb{C}G$ . Explicitly,  $G = \{g_1, g_2, \dots, g_n\}$  (these forming the basis of  $\mathbb{C}G$ ),  $g \cdot g_i = gg_i$ .

### 1.3 CHARACTERS

Unless otherwise noted,  $\chi$  denotes a character of  $G$ , as defined below.

**Definition 1.7.** Given a representation  $\rho$  of  $G$ , we associate to  $\rho$  a function  $\chi : G \rightarrow \mathbb{C}$  defined by  $\chi(g) = \text{tr } \rho(g)$ . Here  $\text{tr}$  is the trace function. We refer to  $\chi$  as the *character afforded* by  $\rho$ .

As with representations, the *degree* of a character is the degree of the associated representation and module. Furthermore, an *irreducible* character is one associated with an irreducible representation. The set of irreducible characters of  $G$  is denoted  $\text{Irr}(G)$ . Any character is a class function on  $G$ , meaning that for all  $g, h \in G$ ,  $\chi(g) = \chi(hgh^{-1})$ . Characters of a number of groups will play a critical role in the first portion of this thesis.



**Theorem 1.8.** [25, p. 246] *If  $\chi$  is a character of  $G$  and  $g \in G$ , then  $\chi(g)$  is an algebraic integer.*

The most rudimentary of characters is the *trivial character*, the character afforded by the trivial representation (Definition 1.5). The trivial character has degree 1, and for each  $g \in G$ ,  $\chi(g) = 1$ . A character of particular interest is the *regular character*, the character afforded by the regular representation (Definition 1.6). Here we denote the regular character by  $\pi : G \rightarrow \mathbb{C}$ . The regular character has values as described in Table 1.1, where  $|G| = n$ . The next theorem is an alternate version of a theorem found on [25, p. 127] (the proof of

Table 1.1: Regular Character for  $G$

	id	$g \neq \text{id}$
$\pi$	$n$	0

which employs module theory and will not be discussed herein).

**Theorem 1.9.** *For a finite group  $G$ , let  $\text{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$ . The regular character  $\pi$  can be decomposed into a sum of irreducible characters of  $G$ , with summand multiplicity being given by the degree,  $d_i$ , of the irreducible character in question. (With  $\chi_1$  being the trivial character,  $d_1 = 1$  of course.) Thus*

$$\pi = \chi_1 + d_2\chi_2 + \dots + d_k\chi_k.$$

**Corollary 1.10.** [31, p. 18]

- (a) *The degrees  $d_i$  satisfy  $\sum_{i=1}^k d_i^2 = |G|$ ;*
- (b) *If  $s \in G$  is not the identity, then  $\sum_{i=1}^k d_i\chi_i(s) = 0$ .*

**Theorem 1.11.** [31, p. 19] *The number of irreducible characters of a group  $G$  is equal to the number of conjugacy classes of  $G$ . That is,  $|\text{Irr}(G)| = k$ , where  $k$  is the number of conjugacy classes of  $G$ .*

Characters for arbitrary finite groups were first defined by Frobenius in his 1896 work *Über Gruppencharaktere* [12] (as cited in [3]) for use in factoring the group determinant. Chapter 2 will further explicate this topic. Character values for different characters of  $G$  can be summarized in a *character table*.

**Definition 1.12.** [25, p. 159] Let  $\text{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$  and let  $g_1, g_2, \dots, g_k$  be conjugacy class representatives. The  $k \times k$  matrix with  $ij$ -entry  $\chi_i(g_j)$  is the *character table* of  $G$ .

**Theorem 1.13.** [25, p. 160] *The character table of a group  $G$  is an invertible matrix.*

**Example.** A group of relative importance in this thesis is the dihedral group of order 10, denoted herein as  $D_{10} = \langle r, s \mid r^5 = s^2 = \text{id}, s^{-1}rs = r^{-1} \rangle$ .  $D_{10}$  has four conjugacy classes:  $\{\text{id}\}$ ,  $\{r, r^4\}$ ,  $\{r^2, r^3\}$ , and  $\{s, sr, sr^2, sr^3, sr^4\}$ . The associated character table of  $D_{10}$  is given in Table 1.2 with columns designated by conjugacy class representative. See also [25, p. 182]. Let  $\zeta = e^{2\pi i/5}$ .

Table 1.2: Character Table  $D_{10}$

	id	$r$	$r^2$	$s$
$\chi_1$	1	1	1	1
$\chi_2$	1	1	1	-1
$\chi_3$	2	$\zeta + \zeta^4$	$\zeta^2 + \zeta^3$	0
$\chi_4$	2	$\zeta^2 + \zeta^3$	$\zeta + \zeta^4$	0

## CHAPTER 2. $k$ -CHARACTERS: THE PRELIMINARIES

As previously mentioned in Chapter 1, attempts to factor the group determinant provided a major impetus for the development of character theory. We begin this chapter with a collection of definitions and theorems relevant to this pursuit.

### 2.1 THE GROUP MATRIX

**Definition 2.1.** [26] Let  $G = \{g_1, g_2, \dots, g_n\}$  be a finite group of order  $n$ . We define the *group matrix* as the  $n \times n$  matrix  $[\xi_{g_i g_j^{-1}}]$ , where the  $\xi_{g_k}$  are indeterminates in the ring  $\mathbb{C}[\xi_{g_1}, \xi_{g_2}, \dots, \xi_{g_n}]$  corresponding to the  $g_k \in G$ , and the rows and columns of the matrix are indexed by the elements of  $G$ . We denote the group matrix by  $X_G$ .

**Example.** [27] Let  $G = S_3$ . We label the elements of  $S_3$ :

$$\text{id} = g_1, \quad (123) = g_2, \quad (132) = g_3, \quad (12) = g_4, \quad (13) = g_5, \quad (23) = g_6.$$

We can then write the  $6 \times 6$  matrix  $X_{S_3}$  as below:

$$\begin{bmatrix} \xi_1 & \xi_3 & \xi_2 & \xi_4 & \xi_5 & \xi_6 \\ \xi_2 & \xi_1 & \xi_3 & \xi_6 & \xi_4 & \xi_5 \\ \xi_3 & \xi_2 & \xi_1 & \xi_5 & \xi_6 & \xi_4 \\ \xi_4 & \xi_6 & \xi_5 & \xi_1 & \xi_2 & \xi_3 \\ \xi_5 & \xi_4 & \xi_6 & \xi_3 & \xi_1 & \xi_2 \\ \xi_6 & \xi_5 & \xi_4 & \xi_2 & \xi_3 & \xi_1 \end{bmatrix}.$$

Here  $\xi_i = \xi_{g_i}$ .

We will see later in this work that the  $\xi_k$  can be associated with probability distributions if desired. The results given in this chapter will, however, treat the  $\xi_k$  as indeterminates.

The following proposition relates the group matrix to the group algebra.

**Proposition 2.2.** *Let  $G$  be a finite group of order  $n$ . Define the following map*

$$\varphi : \mathbb{C}G \rightarrow M_n(\mathbb{C}) \quad \text{where} \quad \sum_{k=1}^n x_{g_k} g_k \mapsto \left[ x_{g_i g_j^{-1}} \right].$$

*Then  $\varphi$  is a ring monomorphism.*

*Proof.* Take  $x, y \in \mathbb{C}G$ . We can first write

$$x = \sum_{i=1}^n x_{g_i} g_i \quad \text{and} \quad y = \sum_{i=1}^n y_{g_i} g_i.$$

Observe that

$$x + y = \sum_{i=1}^n (x_{g_i} + y_{g_i}) g_i,$$

so that

$$\begin{aligned} \varphi(x + y) &= [(x + y)_{g_i g_j^{-1}}] \\ &= \left[ x_{g_i g_j^{-1}} + y_{g_i g_j^{-1}} \right] \\ &= \left[ x_{g_i g_j^{-1}} \right] + \left[ y_{g_i g_j^{-1}} \right] \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

This establishes that  $\varphi$  is an additive homomorphism.

Now write  $x = \sum_G x_i g_i$  and  $y = \sum_G y_j g_j^{-1}$ . Note that in the case of  $y$ , cycling through  $G$  by inverses is done for later convenience.

Let  $\xi_{ij} = x_{g_i g_j^{-1}}$  and  $v_{ij} = y_{g_i g_j^{-1}}$ . Let  $X_G = [\xi_{ij}]$  and  $Y_G = [v_{ij}]$ . Then the  $ij^{\text{th}}$  entry of  $X_G Y_G$ , call it  $\lambda_{ij}$ , is given by

$$\sum_{k=1}^n \xi_{ik} v_{kj}.$$

For any fixed  $i, j$  pair, as the index  $k$  in the above sum ranges from 1 to  $n$ , the product

$g_i g_k^{-1} g_k g_j^{-1}$  gives all instances of the element  $g_i g_j^{-1}$  occurring in

$$xy = \sum_{\ell, m=1}^n x_\ell y_m g_\ell g_m^{-1}. \quad (2.1)$$

So indeed the total or “collected” coefficient of the element  $g_i g_j^{-1}$  in (2.1) is

$$\sum_{k=1}^n x_{ik} y_{kj} = \lambda_{ij},$$

where  $\lambda_{ij}$  is as above. Thus  $\varphi(xy)$  is an  $n \times n$  matrix with  $ij$  entry  $\lambda_{ij}$ , the same as the  $ij$  entry of  $X_G Y_G = \varphi(x)\varphi(y)$ . We can conclude that  $\varphi(xy) = \varphi(x)\varphi(y)$ , which shows that  $\varphi$  is a ring homomorphism.

We now show the injectivity of  $\varphi$ . Again take  $x, y \in \mathbb{C}G$ . Suppose that  $\varphi(x) = \varphi(y)$ . Then for any  $i, j$  pair  $x_{g_i g_j^{-1}} = y_{g_i g_j^{-1}}$ . Specifically this implies that if we let  $g_j = \mathbf{id}$  then we have  $x_{g_i} = y_{g_i}$  for  $1 \leq i \leq n$ . We have in turn that  $x = y$ . Hence  $\varphi$  is injective.  $\square$

This proposition is utilized without proof in the results presented in [3, p. 375–380].

Of particular importance to our immediate discussion is the *group determinant*.

**Definition 2.3.** The *group determinant of  $G$*  is defined as

$$\Theta_G = \det(X_G),$$

where  $X_G$  denotes the group matrix of  $G$ .

The group determinant will be a polynomial over the entries of  $X_G$ .

**Theorem 2.4.** [30] *The group determinant  $\Theta_G$  is independent from the indexing of the elements of  $G$ .*

*Proof.* We assume that  $G$  is a finite group of order  $n$ . Suppose we index the elements of  $G$  in a different way; this means you take an element  $\sigma$  of the symmetric group  $S_n$ , and you

order your element as  $g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(n)}$ . With this new ordering, the matrix becomes

$$X_G^\sigma = [x_{g_{\sigma(i)}g_{\sigma(j)}^{-1}}].$$

Now, let  $P$  be the permutation matrix associated to  $\sigma$ , that is,  $P = [\delta_{\sigma(i),j}]$ , where  $\delta_{k,\ell}$  is 1 if  $k = \ell$  and 0 else. If  $M$  is any  $n \times n$  matrix, then the matrix  $PM$  is obtained by reordering the rows of  $M$  by applying  $\sigma$ ; similarly,  $MP^{-1}$  is obtained by reordering the columns of  $M$  by applying  $\sigma$ . Combining these two observations, you get that  $X_G^\sigma = PX_G P^{-1}$ . Taking the determinant, you have  $\det(X_G^\sigma) = \det(X_G)$ .  $\square$

## 2.2 FACTORING THE GROUP DETERMINANT

**2.2.1 Prefacing the result.** The following definition is used in a subsequent proposition and is provided for the understanding thereof.

**Definition 2.5.** [9, p. 62] Let  $G$  be an abelian group. Let  $\widehat{G}$  denote the set of irreducible characters of  $G$  (we have  $\widehat{G} = \text{Irr}(G)$  since  $G$  is abelian). We refer to  $\widehat{G}$  as the *character group of  $G$* . Note that  $\widehat{G}$  is an abelian group of order  $|G|$ , as each element of  $G$  forms its own conjugacy class.

**Theorem 2.6.** *Assume that  $G$  is abelian. For any  $\chi \in \widehat{G}$  and  $g \in G$ ,  $\chi(g)$  is a root of unity.*

*Proof.* Since  $G$  is abelian, all representations of  $G$  are of dimension 1 by Corollary 1.3. Hence if  $\chi \in \widehat{G}$ , then  $\chi(gh) = \chi(g)\chi(h)$ . This comes from the fact that the trace of a  $1 \times 1$  matrix is equal to the sole entry of that matrix. As every element of  $G$  has order divisible by  $n = |G|$ , then  $1 = \chi(\text{id}) = \chi(g^n) = (\chi(g))^n$ . Hence the desired result has been obtained.  $\square$

*Remark.* Definition 2.5 can be expanded to include non-abelian groups by defining  $\widehat{G}$  as the set of all mappings  $\chi : G \rightarrow \mathbb{C}^\times$  such that

$$\chi(gh) = \chi(g)\chi(h), \quad g, h \in G$$

Such mappings are called *linear characters* of  $G$ . It is in general then not the case that  $\widehat{G} = \text{Irr}(G)$ . See [19] for further development of this topic. In this light, Theorem 2.6 can be relaxed to include non-abelian groups.

In the latter half of the nineteenth century a significant pursuit among algebraists was the factorization of the group determinant. Chief among these were Dedekind and Burnside, both of whom independently proved (using distinct methods) the following proposition for finite *abelian* groups.

**Proposition 2.7.** [3] *Let  $G$  be a finite abelian group. Then we have the following factorization of  $\Theta_G$ :*

$$\Theta_G = \prod_{\chi \in \widehat{G}} \left( \sum_{g \in G} \chi(g)x_g \right).$$

Of note here is that when  $G$  is abelian, the group determinant factors as a product of linear factors in  $\mathbb{C}[x_1, x_2, \dots, x_n]$  with every coefficient of the factors being (by Theorem 2.6) a root of unity.

The establishment of the above proposition led Dedekind to broaden his examination to include that of non-abelian groups. After obtaining the factorization of the group determinant of  $S_3$  and  $Q_8$ , he found that in the case that  $G$  is non-abelian, some of the irreducible factors of  $\Theta_G$  may not be linear [6, p. 423–425] (See also [3, p. 368–370] & [5, p. 52]). Dedekind’s results are summarized below.

**Example.** The first group considered by Dedekind was the symmetric group on three elements. Label the elements of  $S_3$  as in the previous example in Section 2.1.<sup>1</sup> Let  $\omega$  be a primitive third root of unity. We then have the relationship  $\omega^2 + \omega = -1$ . Define the

---

<sup>1</sup>Dedekind labeled the elements of  $S_3$  in an alternative manner, but *mutatis mutandis* his results are as given here.

following polynomials in  $\mathbb{C}[x_1, \dots, x_6]$ :

$$\begin{aligned} u &= x_1 + x_2 + x_3; & v &= x_4 + x_5 + x_6; \\ u_1 &= x_1 + \omega x_2 + \omega^2 x_3; & v_1 &= x_4 + \omega x_5 + \omega^2 x_6; \\ u_2 &= x_1 + \omega^2 x_2 + \omega x_3; & v_2 &= x_4 + \omega^2 x_5 + \omega x_6. \end{aligned}$$

Dedekind found that

$$\Theta_{S_3} = (u + v)(u - v)(u_1 u_2 - v_1 v_2)^2.$$

The final factor  $(u_1 u_2 - v_1 v_2)$  can be expanded as

$$x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2 - x_1 x_2 - x_1 x_3 - x_2 x_3 + x_4 x_5 + x_4 x_6 + x_5 x_6.$$

In  $\mathbb{C}[u, u_1, u_2, v, v_1, v_2]$  the polynomial  $u_1 u_2 - v_1 v_2$  is irreducible. Hence we have a nonlinear, irreducible factor of  $\Theta_{S_3}$ . Also of note is the fact that this nonlinear factor is of degree 2 and occurs twice in the factorization. This is not a mere coincidence.

**Example.** The second group considered by Dedekind was  $Q_8$ , the quaternion group

$$\langle -1, i, j, k \mid (-1)^2 = 1, i = j = k = ijk = -1 \rangle.$$

Label the elements of  $Q_8$  as follows, with the lower index being associated with the + element:

$$\pm 1 = g_1, g_2; \quad \pm i = g_3, g_4; \quad \pm j = g_5, g_6; \quad \pm k = g_7, g_8.$$

Dedekind then defines the following polynomials:

$$u_1, v_1 = x_1 \pm x_2, \quad u_2, v_2 = x_3 \pm x_4, \quad u_3, v_3 = x_5 \pm x_6, \quad u_4, v_4 = x_7 \pm x_8.$$



Then  $\Theta_{Q_8}$  has four linear factors and one repeated nonlinear factor as follows:

$$\Theta_{Q_8} = (u_1+u_2+u_3+u_4)(u_1+u_2-u_3-u_4)(u_1-u_2+u_3-u_4)(u_1-u_2-u_3+u_4)(v_1^2+v_2^2+v_3^2+v_4^2)^2.$$

One can verify that the last factor is indeed irreducible over  $\mathbb{C}$ . Moreover, note that the degree of the factor matches its multiplicity in the factorization, which again is not by happenstance.

After being apprised of these examples by Dedekind in 1896, Frobenius sought to develop a more generalized result for the factorization of  $\Theta_G$  for general finite groups. In a rather short length of time, just three months, Frobenius solved the problem and published his results in a series of three papers [13], [12], [11] (in that order). These results are discussed in the proceeding section.

**2.2.2  $k$ -Characters.** We now extend Definition 1.7 to create from a unary function on  $G$  a  $k$ -nary function on  $G^k$ .

**Definition 2.8.** Let  $G$  be a finite group of order  $n$ . Let  $\chi$  be in  $\text{Irr}(G)$ . We then define the  $k$ -character in a recursive manner by

$$\chi^{(1)}(g) = \chi(g),$$

and for  $k \geq 2$

$$\begin{aligned} \chi^{(k)}(g_1, g_2, \dots, g_k) &= \chi(g_1)\chi^{(k-1)}(g_2, \dots, g_k) - \chi^{(k-1)}(g_1g_2, \dots, g_k) \\ &\quad - \chi^{(k-1)}(g_2, g_1g_3, \dots, g_k) - \dots - \chi^{(k-1)}(g_2, g_3, \dots, g_1g_k). \end{aligned}$$

Many times the superscript is omitted when it is clear what is being discussed.

**Example.** Given a finite group  $G$  and an irreducible character  $\chi$ , we have the 2- and 3-characters

$$\chi^{(2)}(g_1, g_2) = \chi(g_1)\chi(g_2) - \chi(g_1g_2),$$

$$\chi^{(3)}(g_1, g_2, g_3) = \chi(g_1)\chi^{(2)}(g_2, g_3) - \chi^{(2)}(g_1g_2, g_3) - \chi^{(2)}(g_2, g_1g_3).$$

**Example.** Let  $G = D_8 = \langle r, s \mid r^4 = s^2 = 1, srs = r^3 \rangle$ . Let  $\chi$  be the irreducible character of degree 2 given in Table 2.1.

Table 2.1: Irreducible Characters of  $D_8$

	id	$r^2$	$\{r, r^3\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
$\chi$	2	-2	0	0	0

We then have values of the associated 2-character such as the following:

$$\chi^{(2)}(r, r) = \chi(r)\chi(r) - \chi(r^2) = 0 - (-2) = 2$$

$$\chi^{(2)}(r, s) = \chi(r)\chi(s) - \chi(rs) = 0 - 0 = 0$$

A question proposed by R. Brauer relating to  $k$ -characters that remained unanswered for some time dealt with the possibility of uniquely determining the structure of a given group from the character table and a requisite set of  $k$ -characters (see, for example, [22] & [26]). Hoehnke and Johnson [21] prove the following theorem:

**Theorem 2.9.** *Let  $G$  be a finite group. Then  $G$  is determined up to isomorphism by the regular 3-character  $\pi^{(3)}$ .*

Johnson and Sehgal further show in [28] that the 1- and 2-characters alone are not sufficient for determining the group. A later paper [29] by the same authors shows that the two non-isomorphic and non-abelian groups of order 27 provide a pair of such groups whose 1- and 2-characters are identical. Moreover, it can be verified by inspection that these groups form the smallest pair of nonisomorphic groups with identical 1- and 2-characters [29, p. 624]. Section 4.2 explores these groups further.

**2.2.3 Frobenius factors  $\Theta_G$ .** The original utility of  $k$ -characters, and the central result discussed in this chapter, is that of factoring the group determinant  $\Theta_G$  for any finite group.

In [12], Frobenius proved the following theorem, which employs  $k$ -characters to factor the group determinant (See also [26, p. 301]):

**Theorem 2.10.** *Let  $G$  be a finite group. Let  $\text{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_r\}$  be the irreducible characters of  $G$ . For each  $\chi_i$ , define the following polynomial, where  $f_i$  is the degree of  $\chi_i$ :*

$$\phi_i = (1/f_i!) \sum_{G^{f_i}} \chi_i^{(f_i)}(g_1, g_2, \dots, g_{f_i}) x_{g_1} x_{g_2} \dots x_{g_{f_i}}$$

where the sum runs over all  $f_i$ -tuples of  $G$ . We then have that the group determinant factors in  $\mathbb{C}[x_{g_1}, x_{g_2}, \dots, x_{g_{f_i}}]$  into irreducible factors as follows:

$$\Theta_G = \prod_{i=1}^r \phi_i^{f_i}.$$

The next two chapters explore further results pertaining to  $k$ -characters.

## CHAPTER 3. A CONJECTURE ON $k$ -CHARACTERS

### 3.1 PROPOSAL AND CONJECTURE

In [29] Johnson and Sehgal present and prove the following proposition:

**Proposition 3.1.** *Let  $\pi$  be the regular character of the group  $G$ . Fix  $k \geq 1$ . Suppose that for  $g_1, g_2, \dots, g_k$  in  $G$ , no product of the form  $g_{\mu(1)} \cdots g_{\mu(k)}$  is the identity for any permutation  $\mu$  of  $\{1, \dots, k\}$ . Then  $\pi^{(k)}(g_1, g_2, \dots, g_k) = 0$ .*

*Proof.* The proposition is clearly true for  $k = 1$ . Suppose that the result is true for  $k < r$ . Let  $\{g_1, g_2, \dots, g_r\}$  be such that no product of the form  $g_{\mu(1)} \cdots g_{\mu(r)}$  is the identity for any permutation  $\mu$ . We have the following:

$$\pi^{(r)}(g_1, g_2, \dots, g_r) = \pi(g_1)\pi^{(r-1)}(g_2, \dots, g_r) - \pi^{(r-1)}(g_1g_2, \dots, g_r) - \cdots - \pi^{(r-1)}(g_2, g_3, \dots, g_1g_r).$$

Under the inductive assumption, a term on the right hand side of the above equality is 0 unless both  $g_1$  and  $g_{\tau(2)} \cdots g_{\tau(r)}$  are the identity for some permutation  $\tau$  (in the case of the first term) or a product of  $g_2, g_3, \dots, g_1g_j, \dots, g_r$  (in some order) is the identity. In any case, if no product  $g_{\mu(1)} \cdots g_{\mu(r)}$  is the identity, all the terms on the right hand side will be zero.  $\square$

They then make the following conjecture:

**Conjecture 3.2.** The converse of Proposition 3.1 also holds. That is, if

$\pi^{(k)}(g_1, g_2, \dots, g_k) = 0$ , then no product of the form  $g_{\mu(1)} \cdots g_{\mu(k)}$  is the identity for any permutation  $\mu$  of  $\{1, \dots, k\}$ .

However, it is extremely easy to find a counter example among abelian groups: All that is required is the trivial group. If we let  $\text{id}$  be the identity and  $G$  be the group generated by it, then the regular 2-character provides a counter example.

$$\pi^{(2)}(\text{id}, \text{id}) = \pi(\text{id})\pi(\text{id}) - \pi(\text{id} \cdot \text{id}) = 1 \cdot 1 - 1 = 0,$$

yet there was a permutation of the arguments of  $\pi^{(2)}$  whose product was the identity. In light of this, we will restrict our examination to *non-abelian* groups. We restate the conjecture, this time including this small caveat.

**Conjecture 3.3.** The converse of Proposition 3.1 also holds if  $G$  is *non-abelian*. That is, if  $\pi^{(k)}(g_1, g_2, \dots, g_k) = 0$ , then no product of the form  $g_{\mu(1)} \cdots g_{\mu(k)}$  is the identity for any permutation  $\mu$  of  $\{1, \dots, k\}$ .

Throughout this work we will speak of “admissible” polynomials. Because the regular character takes on values of either  $n$  or  $0$ , a given  $k$ -character will be a polynomial in  $n$  with integer coefficients. We call these polynomials *admissible polynomials*.

As a matter of notation, let  $|G| = n$  and  $g_1, g_2, \dots, g_n$  be the elements of  $G$  in no particular order. In line with determining the validity of Conjecture 3.3 we can ask several questions, to wit,

- (1) What are the admissible polynomials for  $\pi^{(k)}$ ?
- (2) Do these admissible polynomials factor into linear polynomials over  $\mathbb{Z}$ ?
- (3) If the conjecture fails in general, are there specific classes of groups for which it still holds (e.g. Dihedral groups,  $p$ -groups, etc.)?

We will examine (1) and (2) in this chapter. Question (3) will not be discussed in this work and will be left for examination at a future date. It is a relatively simple exercise to determine the following table (Table 3.1) of admissible polynomials for  $\pi^{(2)}$ .

Table 3.1: Admissible Polynomials for  $\pi^{(2)}$

$\pi^{(2)}(g_1, g_2)$	<b>Admissible Polynom.</b>	<b>Factors</b>
$g_1 = g_2 = \text{id}$	$n^2 - n$	$n(n - 1)$
$g_1 \neq \text{id}, g_1 g_2 = \text{id}$	$-n$	$-n$
$g_1 \neq \text{id}, g_1 g_2 \neq \text{id}$	$0$	$0$

Note here that these three distinct admissible polynomials all factor in  $\mathbb{Z}$  into linear factors. Linear factors are of course especially nice in that they explicitly indicate the roots of the admissible polynomial in question. Another noteworthy observation to make is the relation between products of operands of  $\pi^{(k)}$  being equal to the identity and the resulting admissible polynomial under  $\pi^{(k)}$  associated with these operands. When we speak of operands of  $\pi^{(k)}$ , we are speaking of the elements of  $G$  which are placed into  $\pi^{(k)}$  as arguments.

As discussed above, we are only considering non-abelian groups in our examination. We assume that the reader is familiar with the fact that the smallest non-abelian group is of order 6. As the nonzero admissible polynomials for  $\pi^{(2)}$  only have roots 1 or 0, this actually proves Conjecture 3.3 for  $k = 2$ . That is, the roots of the non-zero admissible polynomials for  $\pi^{(2)}$  are strictly smaller than the order of the smallest non-abelian group, so the conjecture must hold for  $k = 2$ .

In order to further investigate the admissible polynomials for  $\pi^{(k)}$  for general  $k$ , we use the group  $S_k$ , the symmetric group on  $k$  objects, as we now describe.

## 3.2 THE $S_k$ FILIGREE

**3.2.1 Determining admissible polynomials.** As previously alluded to, a significant amount of information on the admissible polynomials of  $\pi^{(k)}$  can be found by examining the products of operands which are the identity.

We first establish notation used throughout this thesis. Let  $k$  be a positive integer. Take a permutation  $\sigma = (a_{11}a_{12} \cdots a_{1s_1})(a_{21}a_{22} \cdots a_{2s_2}) \cdots (a_{r1}a_{r2} \cdots a_{rs_r}) \in S_k$  here written in disjoint cycle notation. If we include cycles of length 1 in  $\sigma$  (which we always will), then

$$\sum_{i=1}^r s_i = k.$$

Take any  $k$  elements of  $G$  and index them as  $g_{11}, g_{12}, \dots, g_{1s_1}, g_{21}, \dots, g_{2s_2}, \dots, g_{rs_r}$ . In this

way we can correspond the products  $(g_{11} \cdots g_{1s_1}), (g_{21} \cdots g_{2s_2}), \dots, (g_{r1} \cdots g_{rs_r})$  with the cycles of  $\sigma$  by replacing  $a_{ij}$  with  $g_{ij}$ . That is,

$$(a_{i1}a_{i2} \cdots a_{is_i}) \longleftrightarrow (g_{i1}g_{i2} \cdots g_{is_i})$$

for each cycle of  $\sigma$ . We similarly associate the product  $(g_{11} \cdots g_{1s_1})(g_{21} \cdots g_{2s_2}) \cdots (g_{r1} \cdots g_{rs_r})$  of these elements with  $\sigma$ .

When we speak of an *identity product* we are indicating a product of one or more elements of  $G$  whose product is the identity of  $G$ .

**Example.** For  $k = 7$  and  $\sigma = (16)(254)(37)$  we can associate the products  $g_1g_6, g_2g_5g_4, g_3g_7$  with  $\sigma$ . Extending the cycle notation, we denote these products as  $(g_1g_6)(g_2g_5g_4)(g_3g_7)$ .

In general, for  $\sigma \in S_k$ , let  $\mathcal{Z}_\sigma$  be the associated products, written in cycle notation, of the  $g_1, g_2, \dots, g_k$  corresponding to  $\sigma$  for a given set of  $k$  elements in  $G$ .

**Theorem 3.4.** *Let  $G$  be a group of order  $n$ , and let  $1 \leq k \leq n$ . Take any  $g_1, g_2, \dots, g_k$  in  $G$  (not necessarily distinct). Then*

$$\pi^{(k)}(g_1, g_2, \dots, g_k) = c_k n^k - c_{k-1} n^{k-1} + c_{k-2} n^{k-2} + \dots + (-1)^{k-2} c_2 n^2 + (-1)^{k-1} c_1 n,$$

where the  $c_j$  are defined in the proceeding manner. Take any  $\sigma \in S_k$  and let  $\nu(\sigma)$  designate the number of disjoint cycles in  $\sigma$ .

Let  $C_j$  be the set of all elements  $\sigma$  of  $S_k$  such that  $\nu(\sigma) = j$  and each product of  $\mathcal{Z}_\sigma$  equals the identity of  $G$ . Then the coefficient  $c_j$  is given by  $c_j = |C_j|$ . In other words, the coefficient  $c_j$  is the number of permutations in  $S_k$  with precisely  $j$  disjoint cycles, each cycle of which being associated with an identity product using the  $g_1, g_2, \dots, g_k$ .

Theorem 3.4 can perhaps best be elucidated by several examples. The proof of the theorem will be postponed until further results have been established (see Section 3.3). As a matter of notation, I will let  $e$  designate the identity of the group  $G$  and I will let  $\text{id}$  designate the identity permutation of  $S_k$ .

**Example.** Perhaps the simplest of examples is for  $k = 2$ . Let  $g_1$  and  $g_2$  be non-identity elements of a group  $G$ . Further suppose that  $g_1g_2 = \text{id}$ . We have two coefficients to consider:  $c_2$  and  $c_1$ .

Here  $S_k = S_2$  is just the cyclic group of order 2. There is a single permutation,  $(1)(2) = \text{id}$ , with two disjoint cycles. But, since  $(g_1), (g_2)$  are not both  $\text{id}$ , we have  $c_2 = 0$ . There is also a single permutation,  $(12)$ , of length one in  $S_2$ . The corresponding product  $(g_1g_2)$  is the identity (in  $G$ ), so  $c_1 = 1$ . Hence the associated admissible polynomial is  $-n$  (taking note to observe the requisite sign change). It can be confirmed in Table 3.1 that when  $g_1$  and  $g_2$  are both not the identity, but their product is the identity, then the corresponding minimal polynomial is indeed  $-n$ .

**Example.** As an extension of the previous example, take  $g_1 = g_2 = e$ . Now the single products  $(g_1)(g_2)$  associated with  $(1)(2)=\text{id}$  in  $S_2$  are both the identity, so  $c_2 = 1$ . As before,  $c_1 = 1$ . Now the corresponding admissible polynomial is  $n^2 - n$ . This again agrees with Table 3.1.

**Example.** Here let  $k = 3$ . Take  $g_1, g_2, g_3$  with  $g_1 = e$  being the only operand equal to the identity. Assume however that  $g_2g_3 = e$ . We examine the six permutations in  $S_3$ , where trivial cycles are included for emphasis.

$$\text{id} \rightarrow (g_1)(g_2)(g_3), \quad (123) \rightarrow (g_1g_2g_3), \quad (132) \rightarrow (g_1g_3g_2),$$

$$(12)(3) \rightarrow (g_1g_2)(g_3), \quad (13)(2) \rightarrow (g_1g_3)(g_2), \quad (1)(23) \rightarrow (g_1)(g_2g_3).$$

There is one element of  $S_3$  comprised of three disjoint cycles (viz. the identity). The corresponding terms of the product  $(g_1)(g_2)(g_3)$  (i.e.  $g_1$  by itself,  $g_2$  by itself, and  $g_3$  by itself) are not the identity however. So  $c_3 = 0$ . Continuing, we note that  $S_3$  contains three elements with precisely two disjoint cycles. Among the associated products  $(g_1g_2)(g_3)$ ,  $(g_1g_3)(g_2)$ , and  $(g_1)(g_2g_3)$ , only the last set (which we can refer to as  $\mathcal{Z}_{(1)(23)}$  in the notation of the theorem) is a set of identity products. Hence  $c_2 = 1$ . There are two elements of  $S_3$  with a single cycle.



The corresponding products  $(g_1g_2g_3)$  and  $(g_1g_3g_2)$  are both identity products, so  $c_1 = 2$ . All told we have the associated admissible polynomial  $-n^2 + 2n$ .

As an aside, note that this polynomial factors over  $\mathbb{Z}$  into all linear factors and that none of the roots is 6 or larger. Hence in this case, Conjecture 3.3 still holds. Although  $g_1g_2g_3 = e$ ,  $\pi(g_1, g_2, g_3) = -n^2 + 2n$  will never equal zero, as  $|G| = n > 2$ .

It should be pointed out that our association of products of elements of  $G$  with the elements of  $S_k$  is sufficiently well defined with respect to cycle representation, as we are only truly interested in products equal to the identity. (If a product of elements equals the identity, any permutation of the order of multiplication of those elements also results in the identity).

**3.2.2 The  $S_k$  filigree defined.** In order to obtain more general results in our pursuit of proving Theorem 3.4 and obtaining admissible polynomials, we give the following definitions.

**Definition 3.5.** Take a permutation  $\sigma$  in  $S_k$ . Let  $\sigma = \alpha_1\alpha_2 \cdots \alpha_r$ , where the  $\alpha_i$  are the disjoint cycles of  $\sigma$ . A *consequence of coalescence*,  $\alpha_i \diamond \alpha_j$ , of disjoint cycles  $\alpha_i$  and  $\alpha_j$  is a cycle obtained by concatenating a cycle representative for  $\alpha_i$  with a cycle representative for  $\alpha_j$ . This is best illustrated by the following example.

**Example.** Below are three ways that two disjoint cycles of  $S_5$  can be coalesced.

$$(12) \diamond (354) \rightarrow (12354),$$

$$(12) \diamond (354) \rightarrow (13542),$$

$$(12) \diamond (354) \rightarrow (31254) = (12543).$$

The notation here is rather loose in that  $\alpha_i \diamond \alpha_j$  can represent either a single consequence of coalescence or the set of all such consequences of coalescence. This ambiguity of notation will be of relatively small significance.

**Proposition 3.6.** *Let  $\alpha$  and  $\beta$  be disjoint cycles in  $S_k$ . If both  $\mathcal{Z}_\alpha$  and  $\mathcal{Z}_\beta$  are the identity in  $G$ , then  $\mathcal{Z}_{\alpha\circ\beta}$  is also the identity. In other words, if the products associated with  $\alpha$  and  $\beta$  are both equal to the identity in  $G$ , then any consequence of coalescence of  $\alpha$  and  $\beta$  will also correspond to an identity product in  $G$ .*

*Proof.* Assume that  $\alpha$  both and  $\beta$  correspond to identity products in  $G$ . Then any consequence of coalescence of  $\alpha$  and  $\beta$  will either be a product of two identity products or one identity product surrounded by two products whose combined product is the identity, yielding in turn the identity.  $\square$

**Proposition 3.7.** *Let  $\alpha$  and  $\beta$  be disjoint cycles in  $S_k$ . Define  $\alpha \diamond \beta$  to be the set of all consequences of coalescence of  $\alpha$  and  $\beta$ . The size of  $\alpha \diamond \beta$  as a set is  $|\alpha| \cdot |\beta|$ , where  $|\cdot|$  indicates the length of the cycle in question.*

*Proof.* Write  $\alpha = (a_1 a_2 \cdots a_r)$  and  $\beta = (b_1 b_2 \cdots b_t)$ . So  $|\alpha| = r$  and  $|\beta| = t$ . Note that we have  $r$  options up to permutation of where we can place  $\beta$  among the entries of  $\alpha$ . That is to say, we can create the following consequences of coalescence:

$$(a_1 \beta a_2 \cdots a_r), (a_1 a_2 \beta \cdots a_r), \dots, (a_1 a_2 \cdots \beta a_r), (a_1 a_2 \cdots a_r \beta)$$

We have  $t$  ways to write  $\beta$  as a cycle. Thus we have all told  $|\alpha| \cdot |\beta| = rt$  distinct ways of coalescing  $\alpha$  and  $\beta$ .  $\square$

As a means of depicting consequences of coalescence for  $S_k$ , we introduce the concept of the  $S_k$  *filigree*.

**Definition 3.8.** We define the  $S_k$  *filigree* to be the graph whose nodes are the elements of  $S_k$ , ordered in levels by cycle number, and whose edges indicate consequences of coalescence. In this sense we can describe  $S_k$  as a poset with ordering based on coalescence, making the  $S_k$  filigree a Hasse Diagram (see [16, p. 508] for example).

*Remark.* We will sometimes refer to the *filigree condition*. The filigree condition is the premise on which the filigree is constructed. In Chapter 3, the filigree condition is products of operands which are the identity. In Chapter 4, we will see other conditions used. When the filigree condition is satisfied, this indicates that the associated  $k$ -character will not be identically zero.

As an example, if  $k = 5$  and if our filigree condition is products which are the identity in  $G$ , then  $(g_1g_3g_5)(g_2g_4)$  would indicate that the products  $g_1g_3g_5$  and  $g_2g_4$  yield the identity. This would be associated with (135)(24) in the filigree. As another example, let  $k = 6$ . Now let our filigree condition be products which lie in a certain subgroup of  $G$ . We will see such a filigree condition in later results. Then  $(g_1)(g_5)(g_2g_3)(g_4g_6)$  means that  $g_1, g_5$  are both themselves in the given subgroup, as are the products  $g_2g_3$  and  $g_4g_6$ . This is associated with (1)(5)(23)(46) in the corresponding  $S_6$  filigree.

Figure 3.1 gives the filigree for  $S_3$  as well as the associated products in  $G$  among the arbitrary operands  $g_1, g_2$ , and  $g_3$  of  $\pi^{(3)}$ . Note the leveling based on number of cycles. Another aspect of the  $S_3$  filigree to observe is that any term on a lower level of the filigree is a consequence of coalescence of everything above it. This is not the case for general  $k$ , as we will see with  $k = 4$ .

Note that we can use the filigree for  $S_3$  and Theorem 3.4 to calculate different admissible polynomials for  $\pi^{(3)}$ . Figures 3.2 and 3.3 demonstrate this procedure. The dark red indicates a product that is the identity. First assume that all operands are the identity  $e$ :

Figure 3.1: The  $S_3$  filigree

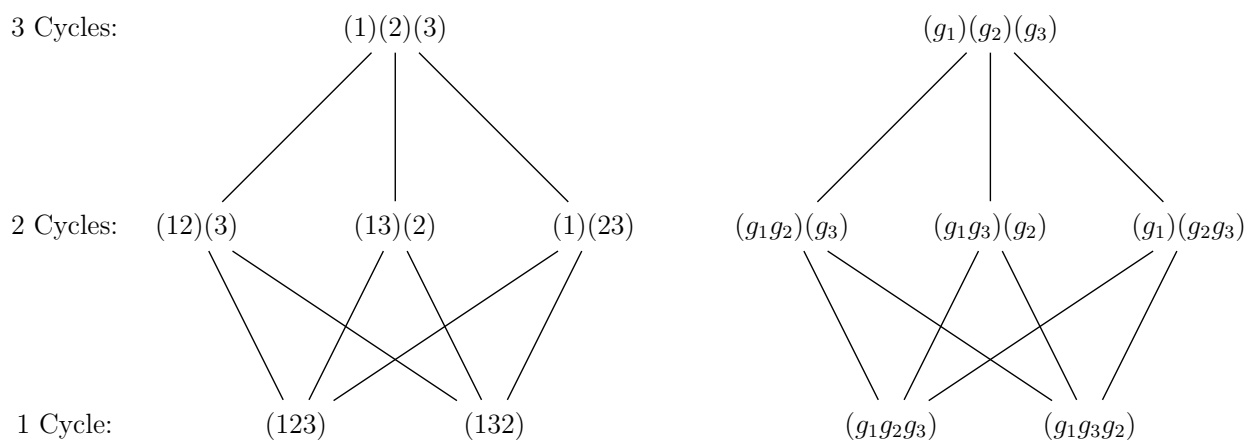
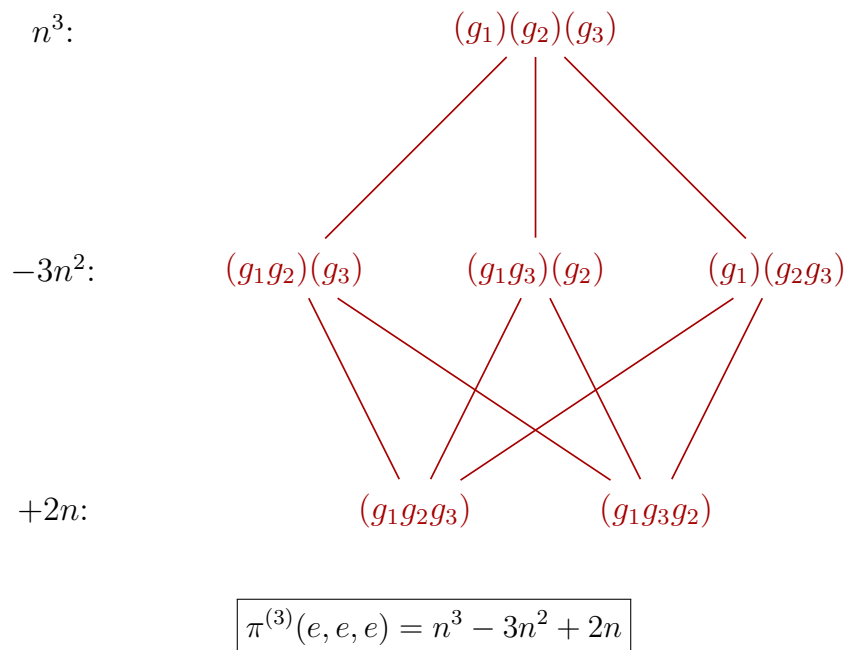
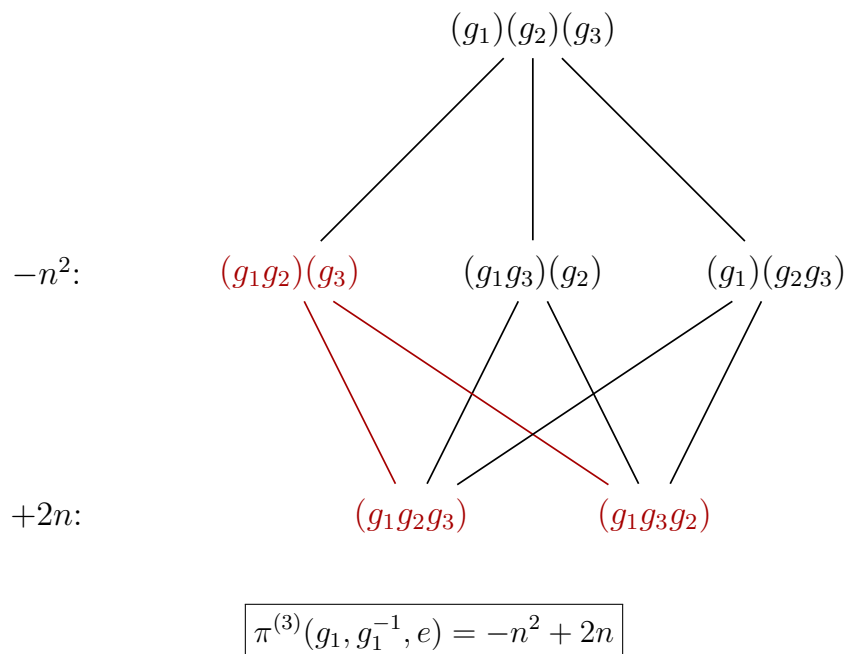


Figure 3.2: Using the  $S_3$  filigree to find an admissible polynomial (I)



Now assume that of the three operands  $g_1, g_2, g_3$ , only the last is the identity. Assume as well, however, that the product of the first two is the identity (i.e.  $g_1g_2 = e$ ).

Figure 3.3: Using the  $S_3$  filigree to find an admissible polynomial (II)



Using a process similar to that of Figures 3.2 and 3.3, we can find all of the admissible polynomials for  $\pi^{(3)}$ . The admissible polynomials for  $\pi^{(3)}$  are summarized in Table 3.2.

Table 3.2: Admissible Polynomials for  $\pi^{(3)}$

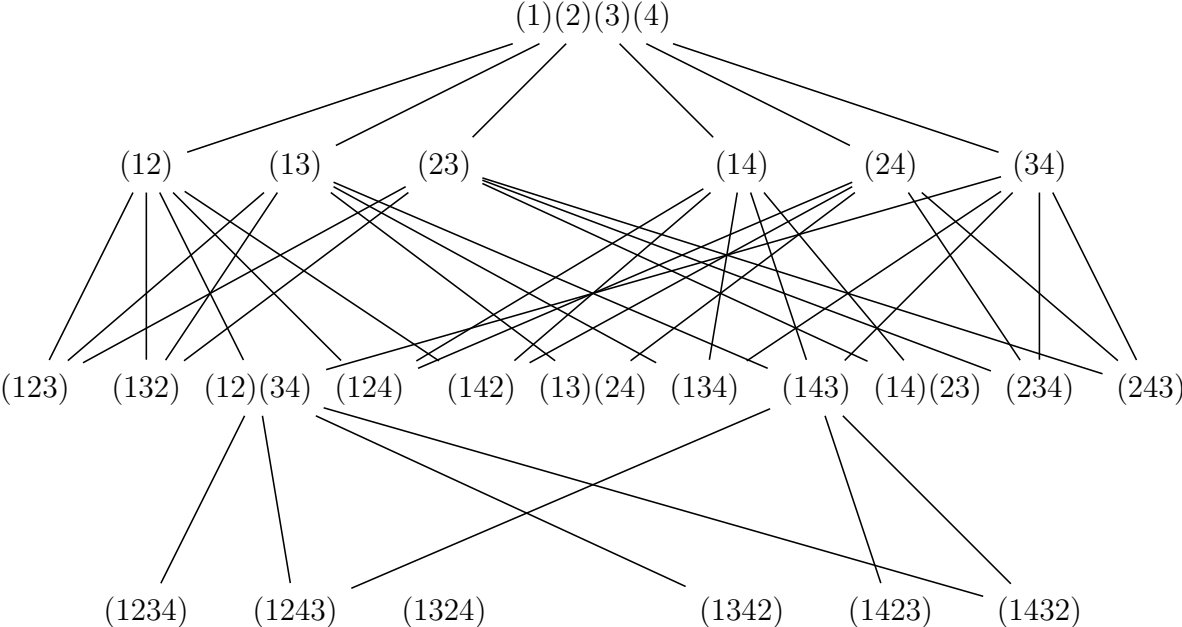
Identity Product	Admissible Polynomials	Factors
$(g_1)(g_2)(g_3)$	$n^3 - 3n^2 + 2n$	$n(n-1)(n-2)$
$(g_1)(g_2g_3)$	$-n^2 + 2n$	$-n(n-2)$
$(g_1g_2g_3)$	$n$	$n$
$(g_1g_2g_3) \ \& \ (g_1g_3g_2)$	$2n$	$2n$
None	$0$	$0$

Note that here also all of the polynomials factor completely over  $\mathbb{Z}$ , but that none of the

nonzero admissible polynomials have a root larger than 2. In a similar vein to the comments given at the end of Section 3.1, the factoring in Table 3.2 proves Conjecture 3.3 for  $k = 3$ .

In general, as  $k$  increases, constructing the  $S_k$  filigree becomes significantly more difficult. Figure 3.4 gives a partial filigree for  $k = 4$ . The lowest level depicts consequences of coalescence for a single double transposition and for a 3-cycle. The complete filigree would show consequences of coalescence for each double transposition as well as for each 3-cycle. Note also that trivial cycles have in many cases been removed for pictorial simplicity.

Figure 3.4: The  $S_4$  Filigree



As with  $k = 2, 3$ , when  $k = 4$  we can use the filigree of  $S_4$  to get the admissible polynomials for  $\pi^{(4)}$ . These results are summarized in Table 3.3 on the following page. The left hand column provides one way to get the associated admissible polynomial, however multiple operand combinations could, and often will, yield the same polynomial. Again note that each admissible polynomial factors linearly over  $\mathbb{Z}$ . We will see for  $k = 5$ , however, that not every admissible polynomial for  $\pi^{(k)}$  factors linearly over  $\mathbb{Z}$ .

Table 3.3: Admissible Polynomials for  $\pi^{(4)}$

Ident. Product	Admissible Polynom.	Factors
$(g_1)(g_2)(g_3)(g_4)$	$n^4 - 6n^3 + 11n^2 - 6n$	$n(n-1)(n-2)(n-3)$
$(g_1g_2)(g_3)(g_4)$	$-n^3 + 5n^2 - 6n$	$-n(n-2)(n-3)$
All double transpositions	$3n^2 - 6n$	$3n(n-2)$
$(g_1g_2g_3)$ & $(g_1g_3g_2)$	$2n^2 - 6n$	$2n(n-3)$
$(g_1g_2)(g_3g_4)$ & All 4-cycles	$n^2 - 6n$	$n(n-6)$
$(g_1g_2g_3)$ & $(g_1g_2g_4)$	$n^2 - 4n$	$n(n-4)$
$(g_1g_2g_3)$	$n^2 - 3n$	$n(n-3)$
All 4-cycles	$-6n$	$-6n$
2 pairs (inverses) of 4-cycles	$-4n$	$-4n$
$(g_1g_2g_3g_4)$ , $(g_1g_3g_4g_2)$ & $(g_1g_4g_2g_3)$	$-3n$	$-3n$
$(g_1g_2g_3g_4)$ & $(g_1g_4g_2g_3)$	$-2n$	$-2n$
Only $(g_1g_2g_3)$	$-n$	$-n$
None	0	0

One important item to take note of is that we have an admissible polynomial  $n^2 - 6n$  which has 6 as a root. However, we can show that when  $G$  is  $S_3$ ,  $\pi^{(4)}$  never admits the polynomial  $n^2 - 6n$ .

**Corollary 3.9.** *If  $G \cong S_3$ , then the admissible polynomial  $n^2 - 6n$  is never obtained by  $\pi^{(4)}$ . Thus Conjecture 3.3 holds for  $k = 4$ .*

*Proof.* Let  $g_1, g_2, g_3$ , and  $g_4$  be the operands of  $\pi^{(4)}$  selected from  $G$ . From Table 3.3, the polynomial  $n^2 - 6n$  is only<sup>1</sup> obtained when we have operands satisfying (without loss of generality)  $g_1g_2 = e$ ,  $g_3g_4 = e$ , as well as any product of all four operands being the identity, and for which no simpler relationship exists. That is to say, no smaller product of operands is

<sup>1</sup>Any use of 3-cycles will fail.

the identity, nor is any other element of two disjoint cycles associated with identity products in  $G$ .

Since we have  $g_1g_2 = e$  and  $g_3g_4 = e$ , then  $g_2 = g_1^{-1}$  and  $g_4 = g_3^{-1}$ . Furthermore we know that  $g_1g_3 \neq e$ , since this would otherwise imply that  $g_2g_4 = e$ , giving an additional relationship (13)(24) not previously accounted for. Similarly,  $g_1g_4 \neq e$ . It is thus impossible to have both  $g_1$  and  $g_3$  be 3-cycles in  $S_3$ . It is a simple exercise to find that any choice of distinct 2-cycles for  $g_1$  and  $g_3$  does not satisfy  $g_1g_3g_2g_4 = e$ , as it otherwise must if we are to obtain the admissible polynomial in question. It is also quite easy to verify that letting  $g_1$  be any 2-cycle in  $S_3$  and  $g_3$  be any 3-cycle fails to satisfy  $g_1g_3g_2g_4 = e$ . This exhausts the possible combinations of operands. Hence if  $G \cong S_3$ , then the admissible polynomial  $n^2 - 6n$  is never obtained by  $\pi^{(4)}$ .  $\square$

This corollary is significant in that it shows that while  $\pi^{(4)}$  can in general admit the polynomial  $n^2 - 6n$ , this polynomial is never obtained when  $G \cong S_3$ . As every other admissible polynomial has roots smaller than 6, this proves that indeed Conjecture 3.3 holds when  $k = 4$ .

### 3.3 PROOF OF THEOREM 3.4

We begin with a notational definition.

**Definition 3.10.** Let  $k \geq 2$  be fixed and  $G$  a group. Take  $\sigma \in S_k$  and  $g_1, g_2, \dots, g_k \in G$ . Write  $\sigma = \alpha_1\alpha_2 \cdots \alpha_r$  in disjoint cycle notation. Let  $\pi(\sigma(g_1, g_2, \dots, g_k))$  indicate the product  $\pi(\alpha_1)\pi(\alpha_2) \cdots \pi(\alpha_r)$  where the entries of  $\alpha_i$  are taken to correspond with the relevant elements among  $g_1, \dots, g_k$  and where  $\pi(\alpha_i)$  is the regular character of  $G$  applied to the product of the operands corresponding to  $\alpha_i$ .

**Example.** Let  $k = 3$  and take  $g_1, g_2, g_3$  in  $G$ . If  $\sigma = (132)$ , then

$$\pi(\sigma(g_1, g_2, g_3)) = \pi(g_1g_3g_2).$$



**Example.** Let  $k = 5$  and take  $g_1, \dots, g_5$  in  $G$ . If  $\sigma = (145)(23)$ , then

$$\pi(\sigma(g_1, \dots, g_5)) = \pi(g_1 g_4 g_5) \pi(g_2 g_3).$$

**Example.** Let  $k = 8$  and take  $g_1, \dots, g_8$  in  $G$ . If  $\sigma = (1357)(24)(68)$ , then

$$\pi(\sigma(g_1, \dots, g_8)) = \pi(g_1 g_3 g_5 g_7) \pi(g_2 g_4) \pi(g_6 g_8).$$

We now provide a lemma on the decomposition of  $\pi^{(k)}$  as a function of  $\pi$ .

**Lemma 3.11.** *Let  $k$  be a positive integer. Then  $\pi^{(k)}$  can be written as*

$$\sum_{\sigma \in S_k} \text{sgn}(\sigma) \pi(\sigma(g_1, g_2, \dots, g_k))$$

where  $\sigma(g_1, g_2, \dots, g_k)$  is as above.

*Proof.* First notice that for  $k = 2$ , we have  $\pi^{(2)}(g_1, g_2) = \pi(g_1)\pi(g_2) - \pi(g_1 g_2)$ , a product and sum of the regular character. In a similar vein, we can decompose  $\pi^{(3)}$  into a product and sum of the regular character as follows:

$$\begin{aligned} \pi^{(3)}(g_1, g_2, g_3) &= \pi(g_1)\pi(g_2)\pi(g_3) \\ &- \pi(g_1)\pi(g_2 g_3) - \pi(g_2)\pi(g_1 g_3) - \pi(g_3)\pi(g_1 g_2) \\ &+ \pi(g_1 g_2 g_3) + \pi(g_1 g_3 g_2). \end{aligned}$$

Note how each element of  $S_3$  can be associated with one of the above summands (e.g.  $(1)(23)$  can be associated with  $\pi(g_1)\pi(g_2 g_3)$  in the sum).

In general  $\pi^{(k)}$  comes from

$$\sum_{\sigma \in S_k} \text{sgn}(\sigma) \sigma.$$

We have seen this for  $k = 2, 3$  above. We now prove the general result by induction on  $k \geq 2$ .

Assume, for some positive integer  $k$ , that the lemma holds for  $\pi^{(k-1)}$ . We can write  $\pi^{(k)}$  as below:

$$\begin{aligned} \pi^{(k)}(g_1, g_2, \dots, g_k) = & \pi(g_1)\pi^{(k-1)}(g_2, \dots, g_k) - \pi^{(k-1)}(g_1g_2, g_3, \dots, g_k) \\ & - \pi^{(k-1)}(g_2, g_1g_3, \dots, g_k) - \dots - \pi^{(k-1)}(g_2, g_3, \dots, g_1g_k). \end{aligned}$$

Note that here  $g_1$  is either fixed (as in the case of the first summand) or is not fixed (as in the remaining cases). We can rewrite  $\pi^{(k)}$  as

$$\begin{aligned} \pi^{(k)}(g_1, g_2, \dots, g_k) = & \pi(g_1) \sum_{\sigma \in S_{k-1}} \pi(\sigma(g_2, g_3, \dots, g_k)) - \sum_{\sigma \in S_{k-1}} \pi(\sigma(g_1g_2, g_3, \dots, g_k)) \\ & - \sum_{\sigma \in S_{k-1}} \pi(\sigma(g_2, g_1g_3, \dots, g_k)) - \dots - \sum_{\sigma \in S_{k-1}} \pi(\sigma(g_2, g_3, \dots, g_1g_k)). \end{aligned}$$

Each permutation of  $S_k$  will either have a trivial cycle,  $(1)$ , containing 1 or will take 1 to some other index between 2 and  $k$  both inclusive (i.e. permutations of form  $(1i\dots)$ , where  $2 \leq i \leq k$ ).

We similarly can associate with each summand of  $\pi^{(k)}$ , as given in the expansion directly above, a permutation of  $S_k$ . This is done as follows: Each summation is indexed by the elements of  $S_{k-1}$ . The summands in the first summation are associated with all permutations of  $S_k$  that have 1 as a trivial cycle. Such elements of  $S_k$  are in one-to-one correspondence with the elements of  $S_{k-1}$ . The summands in the second summation are associated with all permutations of  $S_k$  that have 1 and 2 appearing consecutively in the same cycle. This second summation is indexed by  $S_{k-1}$ . Note that the elements of  $S_k$  which have 1 and 2 appearing consecutively in the same cycle are in one-to-one correspondence with the elements of  $S_{k-1}$ . To wit, taking “12” as a single “letter” and  $3, 4, \dots, k$  as “letters,” we can take  $S_{k-1}$  as the group of permutations on this set of  $k-1$  “letters.” Similarly, the summands in the third summation are associated with all permutations of  $S_k$  that have 1 and 3 appearing consecutively in the same cycle. This association is done up and through the  $k$ -th summation,

where the summands there are associated with the elements of  $S_k$  which have 1 and  $k$  appearing consecutively. Thus we have shown that every element of  $S_k$  is represented in the given expansion of  $\pi^{(k)}$ . Indeed we can write this as

$$\sum_{\sigma \in S_k} \text{sgn}(\sigma) \pi(\sigma(g_1, g_2, \dots, g_k)).$$

□

We now have the terminology and tools required to prove Theorem 3.4. The proof is again by induction.

*Proof of Theorem 3.4.* By Lemma 3.11, we know that we can write  $\pi^{(k)}$  as a product and sum of the standard regular character. The same lemma indicated a method of matching the elements of  $S_3$  with the terms of  $\pi^{(3)}$  when written in terms of the regular character. This concept can be extended to matching  $S_k$  with the terms of the decomposition of  $\pi^{(k)}$  in the following manner.

Considering the  $S_k$  filigree, the first summand  $\pi(g_1)\pi^{(k-1)}(g_2, \dots, g_k)$  of  $\pi^{(k)}(g_1, \dots, g_k)$  decomposes into a product and sum of the regular character whose summands correspond to the entries of the filigree which leave (1) as a trivial cycle (i.e. all those that correspond to  $g_1 = e$ ). The remaining terms of  $\pi^{(k)}(g_1, \dots, g_k)$  are all of the form  $\pi^{(k-1)}(g_2, \dots, g_1g_j, \dots, g_k)$ . Each of these terms will have a decomposition into a product and sum of the regular character whose summands correspond to the entries of the filigree where 1 and  $j$  are found in cycle with one another (i.e. all those entries of the filigree that have the product  $g_1g_j$  associated with them).

In this manner we can associate with each entry of the  $S_k$  filigree a term of the decomposition of  $\pi^{(k)}(g_1, \dots, g_k)$ . Take an arbitrary entry of the filigree, say with disjoint cycles  $\alpha_1\alpha_2 \cdots \alpha_r$ . This entry of the filigree will correspond to the term

$$(-1)^{k-r} \pi(\alpha_1)\pi(\alpha_2) \cdots \pi(\alpha_r)$$

in the decomposition of  $\pi^{(k)}(g_1, \dots, g_k)$ , where  $\pi(\alpha_j)$  is the regular character applied to the product of the operands corresponding to  $\alpha_j$ , as seen in Definition 3.10. Hence if each of  $\alpha_1, \alpha_2, \dots, \alpha_r$  corresponds to an identity product in  $G$ , then  $\pi(\alpha_1)\pi(\alpha_2) \cdots \pi(\alpha_r)$  gives us a  $(-1)^{k-r}n^r$  term in the admissible polynomial. Per the recursive definition of  $\pi^{(k)}$ , we can write the regular  $k$ -character as a product and sum of the regular character. A decomposition of the regular  $k$ -character into a product and sum of the regular character  $\pi$  will yield the result given pertaining to the sign of the coefficient. This completes the proof.  $\square$

### 3.4 THE CASES $k = 5, 6$ AND CONJECTURE 3.3

**3.4.1 Counterexample to Conjecture 3.3.** The previous sections have established Conjecture 3.3 for  $k = 2, 3, 4$ . However, for  $k = 5$ , a counterexample can be produced. Let  $G = S_3$ , and take  $h = (123)$  and  $g = (13)$  as elements of  $S_3$ . Now consider the  $S_5$  filigree associated with  $g_1 = g_2 = g_3 = h$  and  $g_4 = g_5 = g$ . The element  $(123)(45)$  in  $S_5$  corresponds to the set of identity products  $\mathcal{Z}_{(123)(45)} = \{(hhh), (gg)\}$ . Note as well that since the first three operands are the same, the permutation  $(132)(45)$  in  $S_5$  also corresponds to an identity product among the operands. Hence  $\mathcal{Z}_{(132)(45)} = \{(hhh), (gg)\}$  will also correspond to an identity product of the operands. By Theorem 3.4, we will have a term  $-2n^2$  in the admissible polynomial associated with these operands. Further calculation finds that exactly 12 of the 24 5-cycles in  $S_5$  correspond to identity products among the operands. So by Theorem 3.4 we have the following:

$$\pi^{(5)}(h, h, h, g, g) = -2n^2 + 12n = -2n(n - 6) = 0.$$

A counter example to the conjecture has been found. We have  $\pi^{(5)}(h, h, h, g, g) = 0$ , yet clearly  $h \cdot h \cdot h \cdot g \cdot g = e$ . So indeed we have a set of operands for which the 5-character is equal to 0, but for which there exists a product of all the operands which equals the identity in  $G$ .

**3.4.2 Factoring admissible polynomials.** Another finding to take note of is the factorization of the admissible polynomials for  $\pi^{(k)}$ . While we have seen that for small  $k$  (viz.  $k = 1, 2, 3, 4$  are confirmed) the admissible polynomials for  $\pi^{(k)}$  all factor into linear factors over  $\mathbb{Z}$ , such is not the case for larger values of  $k$ .

**Observation 3.12.** For  $k = 6$ , we can find using MAGMA [1] that we have admissible polynomials that do not factor completely into linear factors over  $\mathbb{Z}$ . Some examples of irreducible nonlinear factors of admissible polynomials are as follows:

$$n^2 - 16n + 56, \quad n^2 - 12n + 56, \quad n^2 - 11n + 36, \quad n^2 - 11n + 32, \quad n^2 - 12n + 48.$$

For further questions on this subject see Chapter 6.

The next chapter will examine the  $k$ -characters of select classes of groups.

CHAPTER 4.  $k$ -CHARACTERS OF SEVERAL GROUPS AND THE  
ASSOCIATED GROUP DETERMINANT

4.1 THE DIHEDRAL GROUPS

One class of non-abelian groups that is of ubiquitous importance is the class of dihedral groups. We have previously seen in Tables 1.2 and 2.1 the irreducible characters of degree 2 for  $D_{10}$  and  $D_8$  respectively. In this section we find the 2-character for the general dihedral group  $D_{2n}$  ( $n \geq 3$ ), with presentation as follows:

$$D_{2n} = \langle r, s \mid r^n = s^2 = \text{id}, \quad s^{-1}rs = r^{-1} = r^{n-1} \rangle.$$

The conjugacy classes of  $D_{2n}$  are as follows, with the cases of  $n$  odd and  $n$  even being distinct.

**odd**  $n = 2m + 1$  :  $\{\text{id}\}, \{r^a, r^{-a}\} (1 \leq a \leq m), \{s, sr, \dots, sr^{n-1}\}.$

**even**  $n = 2m$  :  $\{\text{id}\}, \{r^a, r^{-a}\} (1 \leq a < m), \{r^m\}, \{sr^b \mid b \text{ odd}\}, \{sr^b \mid b \text{ even}\}.$

As with conjugacy classes, the irreducible characters of  $D_{2n}$  are determined by the parity of  $n$ . Tables 4.1 ( $n$  odd) and 4.2 ( $n$  even) summarize the two cases. (See [25, p. 182–183].) Let  $\zeta = e^{2\pi i/n}$ . In the case of  $n$  odd,  $n = 2m + 1$ . In the case of  $n$  even,  $n = 2m$ .

Table 4.1: Character Table  $D_{2n}$  for  $n$  **odd**

	id	r <sup>a</sup>	s
$\chi_1$	1	1	1
$\chi_2$	1	1	−1
$\psi_j$ ( $1 \leq j \leq m$ )	2	$\zeta^{aj} + \zeta^{-aj}$	0

Table 4.2: Character Table  $D_{2n}$  for  $n$  even

	id	$r^m$	$r^a$ ( $a \neq m$ )	$s$	$sr$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	1	-1	-1
$\chi_3$	1	$(-1)^m$	$(-1)^r$	1	-1
$\chi_4$	1	$(-1)^m$	$(-1)^r$	-1	1
$\psi_j$	2	$2(-1)^j$	$\zeta^{aj} + \zeta^{-aj}$	0	0
$(1 \leq j \leq m-1)$					

In light of the results presented in Chapter 2, we will find the factors of  $\Theta_{D_{2n}}$  associated with the nonlinear irreducible characters of  $D_{2n}$ .

**4.1.1 The 2-character of  $\psi_j$  for  $n$  odd.** The first case we consider is the 2-character associated with the irreducible characters  $\psi_j$  ( $1 \leq j \leq m$ ) for  $n$  odd. Within this case there are multiple subcases to examine. Take general elements  $s^{\varepsilon_1}r^{\delta_1}$  and  $s^{\varepsilon_2}r^{\delta_2} \in D_{2n}$ , where  $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$  and  $0 \leq \delta_1, \delta_2 \leq (n-1)$ . Let  $1 \leq j \leq m$  be arbitrary but fixed. The 2-character of  $\psi_j$  is

$$\begin{aligned} \psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) &= \psi_j(s^{\varepsilon_1}r^{\delta_1})\psi_j(s^{\varepsilon_2}r^{\delta_2}) - \psi_j(s^{\varepsilon_1}r^{\delta_1}s^{\varepsilon_2}r^{\delta_2}) \\ &= \psi_j(s^{\varepsilon_1}r^{\delta_1})\psi_j(s^{\varepsilon_2}r^{\delta_2}) - \psi_j(s^{(\varepsilon_1+\varepsilon_2)}r^{t(\delta_1+\delta_2)}), \end{aligned}$$

where  $t = (-1)^{\varepsilon_2}$ . We have four subcases to consider.

- $\varepsilon_1 = \varepsilon_2 = 0$ :

$$\begin{aligned} \psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) &= \psi_j^{(2)}(r^{\delta_1}, r^{\delta_2}) \\ &= (\zeta^{j\delta_1} + \zeta^{-j\delta_1})(\zeta^{j\delta_2} + \zeta^{-j\delta_2}) - (\zeta^{j(\delta_1+\delta_2)} + \zeta^{-j(\delta_1+\delta_2)}) \\ &= \zeta^{j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1-\delta_2)}. \end{aligned}$$

- $\varepsilon_1 = 1, \varepsilon_2 = 0$  : Then  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, r^{\delta_2}) = 0$ .
- $\varepsilon_1 = 0, \varepsilon_2 = 1$  : Then  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = 0$ .
- $\varepsilon_1 = 1, \varepsilon_2 = 1$  :

$$\begin{aligned}
\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) &= 0 - (\zeta^{j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1-\delta_2)}) \\
&= -(\zeta^{j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1-\delta_2)}) \\
&= -\psi_j^{(2)}(r^{\delta_1}, r^{\delta_2}).
\end{aligned}$$

**Observation 4.1.** Note that  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2})$  is invariant under complex conjugation. Thus we have that  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2})$  is in fact real.

**Observation 4.2.** Note that if  $\delta_1 = \delta_2$  and  $\varepsilon_1 = \varepsilon_2$  then  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = -2$ .

**Corollary 4.3.** Let  $n$  be odd. Each  $\psi_j$  contributes the following factor of multiplicity 2 to the group determinant  $\Theta_{D_{2n}}$  :

$$\sum_{0 \leq \delta_1, \delta_2 \leq n-1} \frac{1}{2} (\zeta^{j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1-\delta_2)}) (x_{r^{\delta_1}} x_{r^{\delta_2}} - x_{sr^{\delta_1}} x_{sr^{\delta_2}})$$

*Proof.* By Theorem 2.10 each  $\psi_j$  corresponds to a factor of multiplicity 2 in the factorization of  $\Theta_{D_{2n}}$  over  $\mathbb{C}[x_{g_1}, x_{g_2}, \dots, x_{g_{2n}}]$  into irreducible factors. (Here assume that the elements of  $D_{2n}$  are ordered as  $g_1 = \mathbf{id}, g_2 = r, \dots, g_{n+1} = s, \dots, g_{2n}$ ).

By this theorem, such a factor can be written as

$$\sum_{0 \leq \delta_1, \delta_2 \leq n-1} \frac{1}{2} \psi_j^{(2)}(r^{\delta_1}, r^{\delta_2})(x_{r^{\delta_1}} x_{r^{\delta_2}}) - \sum_{0 \leq \delta_1, \delta_2 \leq n-1} \frac{1}{2} \psi_j^{(2)}(sr^{\delta_1}, sr^{\delta_2})(x_{sr^{\delta_1}} x_{sr^{\delta_2}})$$

Using the four bulleted subcases given above, this simplifies exactly to the factor claimed in the statement of the corollary.  $\square$

**Example.** Here we use Corollary 4.3 to find the factor of  $\Theta_{D_6}$  associated with the irreducible



character of degree 2 for  $D_6$ . We show this by factoring the group determinant explicitly.

$$\begin{aligned} \Theta_{D_6} &= (x_e + x_r + x_{r^2} + x_s + x_{sr} + x_{sr^2})(x_e + x_r + x_{r^2} - x_s - x_{sr} - x_{sr^2}) \\ &\cdot \left( x_e^2 + x_r^2 + x_{r^2}^2 - x_s^2 - x_{sr}^2 - x_{sr^2}^2 - (x_e x_r - x_s x_{sr}) - (x_e x_{r^2} - x_s x_{sr^2}) - (x_r x_{r^2} - x_{sr} x_{sr^2}) \right)^2. \end{aligned}$$

*Remark.* The final factor implicitly is scaled by  $\frac{1}{2}$ . However, due to symmetry, each summand occurs with multiplicity 2. Hence the final factor given above is the result of a cancellization. Further take note of the fact that this example was previously given in another form (as  $S_3$ ) in Section 2.2 as a result of Dedekind. The results demonstrated directly above verify his result.

**4.1.2 The 2-character of  $\psi_j$  for  $n$  even.** The second case we consider is the 2-character associated with the irreducible characters  $\psi_j$  ( $1 \leq j \leq m$ ) for  $n$  even. Within this case there are multiple subcases to examine. Take general elements  $s^{\varepsilon_1} r^{\delta_1}$  and  $s^{\varepsilon_2} r^{\delta_2} \in D_{2n}$ , where  $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$  and  $0 \leq \delta_1, \delta_2 \leq (n-1)$ . Let  $1 \leq j \leq m-1$  be arbitrary but fixed. The 2-character of  $\psi_j$  is

$$\begin{aligned} \psi_j^{(2)}(s^{\varepsilon_1} r^{\delta_1}, s^{\varepsilon_2} r^{\delta_2}) &= \psi_j(s^{\varepsilon_1} r^{\delta_1}) \psi_j(s^{\varepsilon_2} r^{\delta_2}) - \psi_j(s^{\varepsilon_1} r^{\delta_1} s^{\varepsilon_2} r^{\delta_2}) \\ &= \psi_j(s^{\varepsilon_1} r^{\delta_1}) \psi_j(s^{\varepsilon_2} r^{\delta_2}) - \psi_j(s^{(\varepsilon_1 + \varepsilon_2)} r^{t(\delta_1 + \delta_2)}), \end{aligned}$$

where  $t = (-1)^{\varepsilon_2}$ . We have multiple cases to consider, some with several subcases as we must make special considerations for when  $\delta_1$ ,  $\delta_2$ , or some sum thereof, equals  $m$ .

- $\varepsilon_1 = \varepsilon_2 = 0$ :
  - $\delta_1 + \delta_2 \neq m$  and  $\delta_1 \neq m$  and  $\delta_2 \neq m$ .

$$\begin{aligned} \psi_j^{(2)}(s^{\varepsilon_1} r^{\delta_1}, s^{\varepsilon_2} r^{\delta_2}) &= \psi_j^{(2)}(r^{\delta_1}, r^{\delta_2}) \\ &= (\zeta^{j\delta_1} + \zeta^{-j\delta_1})(\zeta^{j\delta_2} + \zeta^{-j\delta_2}) - (\zeta^{j(\delta_1 + \delta_2)} + \zeta^{-j(\delta_1 + \delta_2)}) \\ &= \zeta^{j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 - \delta_2)}. \end{aligned}$$

○  $\delta_1 + \delta_2 = m$  and  $\delta_1 \neq m$  and  $\delta_2 \neq m$ .

$$\begin{aligned}\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) &= \psi_j^{(2)}(r^{\delta_1}, r^{\delta_2}) \\ &= (\zeta^{j\delta_1} + \zeta^{-j\delta_1})(\zeta^{j\delta_2} + \zeta^{-j\delta_2}) - 2(-1)^m \\ &= \zeta^{j(\delta_1+\delta_2)} + \zeta^{j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1-\delta_2)} + \zeta^{-j(\delta_1+\delta_2)} - 2(-1)^m.\end{aligned}$$

○  $\delta_1 = m$  and  $\delta_2 = 0$  (Without Loss of Generality).

$$\begin{aligned}\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(r^m, e) &= 2(-1)^m \cdot 2 - 2(-1)^m \\ &= 2(-1)^m.\end{aligned}$$

○  $\delta_1 = \delta_2 = m$ .

$$\begin{aligned}\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(r^m, r^m) &= 2(-1)^m \cdot 2(-1)^m - 2(-1)^{2m} \\ &= 4(-1)^{2m} - 2(-1)^{2m} = 2.\end{aligned}$$

- $\varepsilon_1 = 1, \varepsilon_2 = 0$  : Then  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, r^{\delta_2}) = 0$ .
- $\varepsilon_1 = 0, \varepsilon_2 = 1$  : Then  $\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = \psi_j^{(2)}(r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = 0$ .
- $\varepsilon_1 = 1, \varepsilon_2 = 1$  : Here the value of  $\psi_j^{(2)}$  depends on the value of  $\delta_2 - \delta_1$ .

$$\begin{aligned}\psi_j^{(2)}(sr^{\delta_1}, sr^{\delta_2}) &= 0 - \psi_j(s^{\varepsilon_1+\varepsilon_2}r^{-\delta_1+\delta_2}) \\ &= -\psi_j(r^{\delta_2-\delta_1}).\end{aligned}$$

○  $\delta_2 - \delta_1 \neq m$

$$\psi_j^{(2)}(s^{\varepsilon_1}r^{\delta_1}, s^{\varepsilon_2}r^{\delta_2}) = -(\zeta^{j(\delta_2-\delta_1)} + \zeta^{-j(\delta_2-\delta_1)}).$$

$$\circ \delta_2 - \delta_1 = m$$

$$\begin{aligned} \psi_j^{(2)}(s^{\varepsilon_1} r^{\delta_1}, s^{\varepsilon_2} r^{\delta_2}) &= -2(-1)^m \\ &= 2(-1)^{m+1}. \end{aligned}$$

**Observation 4.4.** Note that in the case of  $\varepsilon_1 = 1$ ,  $\varepsilon_2 = 1$  and  $\delta_2 - \delta_1 \neq m$ , if we have that in fact  $\delta_2 - \delta_1 = 0$ , then  $\psi_j^{(2)} = -2$ .

Using these results we can produce the factors of multiplicity two in the factorization of the group determinant of  $D_{2n}$  for  $n$  even. Take any  $j$  as above. By Theorem 2.10,  $\psi_j$  is associated with the following factor (we call it  $\phi_j$ ) of  $\Theta_{D_{2n}}$ . We have

$$\begin{aligned} \phi_j &= \sum_{0 \leq \delta_1, \delta_2 \leq n-1} \frac{1}{2} \psi_j^{(2)}(r^{\delta_1}, r^{\delta_2}) x_{r^{\delta_1}} x_{r^{\delta_2}} + \frac{1}{2} \psi_j^{(2)}(sr^{\delta_1}, sr^{\delta_2}) x_{sr^{\delta_1}} x_{sr^{\delta_2}} \\ &= \sum_{\substack{0 \leq \delta_1, \delta_2 \leq n-1 \\ \delta_1, \delta_2 \neq m \\ \delta_1 + \delta_2 \neq m}} \frac{1}{2} (\zeta^{j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 - \delta_2)}) x_{r^{\delta_1}} x_{r^{\delta_2}} + \frac{1}{2} (2(-1)^m) (x_{r^m} x_e + x_e x_{r^m}) + \frac{1}{2} (2x_{r^m}^2) \\ &\quad + \sum_{\substack{\delta_1, \delta_2 \neq m \\ \delta_1 + \delta_2 = m}} \frac{1}{2} (\zeta^{j(\delta_1 + \delta_2)} + \zeta^{j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 + \delta_2)} + 2(-1)^{m+1}) x_{r^{\delta_1}} x_{r^{\delta_2}} \\ &\quad - \sum_{\delta_2 - \delta_1 \neq m} \frac{1}{2} (\zeta^{j(\delta_2 - \delta_1)} + \zeta^{-j(\delta_2 - \delta_1)}) x_{sr^{\delta_1}} x_{sr^{\delta_2}} - \sum_{\delta_2 - \delta_1 = m} \frac{1}{2} (2(-1)^{m+1} x_{sr^{\delta_1}}) x_{sr^{\delta_2}} \\ &= \sum_{\substack{0 \leq \delta_1, \delta_2 \leq n-1 \\ \delta_1, \delta_2 \neq m \\ \delta_1 + \delta_2 \neq m}} \frac{1}{2} (\zeta^{j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 - \delta_2)}) x_{r^{\delta_1}} x_{r^{\delta_2}} + 2(-1)^m x_e x_{r^m} + x_{r^m}^2 \\ &\quad + \sum_{\substack{\delta_1, \delta_2 \neq m \\ \delta_1 + \delta_2 = m}} \frac{1}{2} (\zeta^{j(\delta_1 + \delta_2)} + \zeta^{j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 - \delta_2)} + \zeta^{-j(\delta_1 + \delta_2)} + 2(-1)^{m+1}) x_{r^{\delta_1}} x_{r^{\delta_2}} \\ &\quad - \sum_{\delta_2 - \delta_1 \neq m} \frac{1}{2} (\zeta^{j(\delta_2 - \delta_1)} + \zeta^{-j(\delta_2 - \delta_1)}) x_{sr^{\delta_1}} x_{sr^{\delta_2}} + \sum_{\delta_2 - \delta_1 = m} (-1)^m x_{sr^{\delta_1}} x_{sr^{\delta_2}}, \end{aligned}$$

after combining terms and cancelling coefficients as possible. Thus when  $n = 2m$  is even then for each  $1 \leq j \leq m - 1$  we have a factor  $\phi_j$ , as above, of multiplicity two in the factorization over  $\mathbb{C}$  of the group determinant of  $D_{2n}$ .

This concludes the relevant results on the  $k$ -characters and factorization of the group determinant for the dihedral groups.

## 4.2 THE NON-ABELIAN GROUPS OF ORDER $p^3$

Our next examination deals with non-abelian groups of order  $p^3$  where  $p$  is an odd prime. Up to isomorphism there are two non-abelian groups of order  $p^3$  [8, pp. 179,183–184]. These distinct groups have the following presentations [25, p. 304]:

$$H_1 = \langle a, b \mid a^{p^2} = b^p = e, b^{-1}ab = a^{p+1} \rangle;$$

$$H_2 = \langle a, b, z \mid b^{-1}ab = az, az = za, bz = zb, a^p = b^p = z^p = e \rangle.$$

For  $H_1$  we let  $z = a^p$ , a generator of the center. For either group, a generic element can be written in the form  $a^r b^s z^t$ , where  $0 \leq r, s, t < p$  in either case. Also, for both  $H_1$  and  $H_2$ ,  $z$  generates the center of the group. These groups have identical character tables, with all irreducible characters being distinguished as follows (See [25, p. 302]):

Table 4.3: Character Table for non-abelian groups of order  $p^3$

	$z^t$	$a^r b^s z^t, r, s \neq 0$
$\chi_{v,w}$	$\zeta^{rv+sw}$	$\zeta^{rv+sw}$
$\psi_u$	$p\zeta^{ut}$	0

where  $0 \leq v, w \leq p - 1$  and  $1 \leq u \leq p - 1$  and  $\zeta = e^{2\pi i/p}$ . Hence there are  $p^2$  irreducible characters of degree 1 and  $p - 1$  irreducible characters of degree  $p$ .

**4.2.1 The  $p$ -character of  $\psi_u$ .** Of particular interest is the  $p$ -character of the irreducible character  $\psi_u$  of degree  $p$ . (Here  $u$  satisfies  $1 \leq u \leq p-1$  and is arbitrary but fixed.) In light of the findings presented in Chapter 2, the  $p$ -character of  $\psi_u$  allows us to find a factor (of multiplicity  $p$ ) of the group determinant  $\Theta_G$ , where  $G$  is either  $H_1$  or  $H_2$ . Furthermore, as shown in [29, p. 625], the 1- and 2- characters alone are not sufficient to distinguish between the two groups using character tables only. But, for any odd prime  $p$ , the 3-character of  $\psi_u$  will allow us to uniquely determine which non-abelian group ( $H_1$  or  $H_2$ ) of order  $p^3$  we are working with. This will especially be of use in the case  $p = 3$ .

Let  $p$  be a fixed odd prime. We now examine the irreducible group determinant factors of the group  $G$  of order  $p^3$ , with presentation given as  $H_2$  above.<sup>1</sup>

For  $1 \leq u \leq p-1$ ,  $G$  has irreducible characters  $\psi_u$  of degree  $p$  as given in Table 4.3:

$$\psi_u(a^r b^s z^t) = \begin{cases} p\zeta^{ut}, & \text{if } r = s = 0; \\ 0 & \text{otherwise.} \end{cases}$$

Then  $\psi_u$  is nonzero on the center of  $G$  and is 0 for all noncentral elements.

Given  $g_1, g_2, \dots, g_p \in G$ , write  $g_i = a^{r_i} b^{s_i} z^{t_i}$  for  $0 \leq r_i, s_i, t_i < p$ . Let  $t = \sum t_i$ . We define the following sets.<sup>2</sup> Let  $\mathcal{P}_k$  be the set of all partitions of the set  $\{1, 2, 3, \dots, p\}$  into  $k$  parts such that each block corresponds to a central product of elements among  $g_1, g_2, \dots, g_p$ .<sup>3</sup> We note that if  $g_{i_1} g_{i_2} g_{i_3} \cdots g_{i_r} \in Z(H_i)$  then  $g_{i_{\sigma(1)}} g_{i_{\sigma(2)}} g_{i_{\sigma(3)}} \cdots g_{i_{\sigma(r)}} \in Z(H_i)$  for any  $\sigma \in S_r$ . (This fact is particular to the groups  $H_1$  and  $H_2$  and is not true for general groups.) We denote an element of  $\mathcal{P}_k$  by  $R = \{R_1, R_2, \dots, R_k\}$ . Then the value of the associated  $p$ -character of  $\psi_u$  is given as follows:

---

<sup>1</sup>Many times this group is presented as  $UT(3, p)$ , the unitriangular matrix group of degree three over the prime field  $\mathbb{F}_p$ . For our considerations here, such a presentation will not be of particular utility.

<sup>2</sup>This is done in hopes of eliminating wildly messy notation in the definition of the associated  $p$ -character.

<sup>3</sup>For example, if  $g_1 g_4 g_7, g_2 g_5, g_3 g_6$  are central products in  $G$  (where  $p = 7$ ), then these elements would correspond to the partition  $\{\{1, 4, 7\}, \{2, 5\}, \{3, 6\}\}$ . This partition would be an element of  $\mathcal{P}_3$ .

$$\psi_u^{(p)}(g_1, g_2, \dots, g_p) = \sum_{k=1}^p \sum_{R \in \mathcal{P}_k} \sum_{v=1}^k \sum_{\text{Sym}(R_v)} p^k \zeta^{ut\eta},$$

where

$$\eta = \left( \sum_{\substack{i, j \in R_v \\ \sigma_v(i) < \sigma_v(j)}} s_{\sigma_v(i)} r_{\sigma_v(j)} \right).$$

The proceeding is an example of the 3-character for a group of order 27 (i.e. a group of order  $p^3$  with  $p = 3$ ).

**4.2.2 The 3-Character for SmallGroup(27,3).** Let  $G$  refer to `SmallGroup(27,3)` from GAP's `SmallGroup` library [14]. This group is  $H_2$  from above, with the prime  $p = 3$ . Johnson and Sehgal discuss this group in [29]. Take  $g_1, g_2, g_3 \in G$  with

$$g_1 = a^{r_1} b^{s_1} z^{t_1}, \quad g_2 = a^{r_2} b^{s_2} z^{t_2} \quad \text{and} \quad g_3 = a^{r_3} b^{s_3} z^{t_3}.$$

Also let  $\zeta = e^{2\pi i/3}$ .

Then for  $1 \leq u \leq 2$  we have the irreducible character of degree 3

$$\phi_u(a^r b^s z^t) = \begin{cases} 3\zeta^{ut} & \text{if } r = s = 0 \\ 0 & \text{otherwise} \end{cases}$$

This allows us to construct the 3-character of  $\phi_u$  as defined in Chapter 2:

$$\phi_u^{(3)}(g_1, g_2, g_3) = \phi_u(g_1)\phi_u^{(2)}(g_2g_3) - \phi_u^{(2)}(g_1g_2, g_3) - \phi_u^{(2)}(g_2, g_1g_3).$$

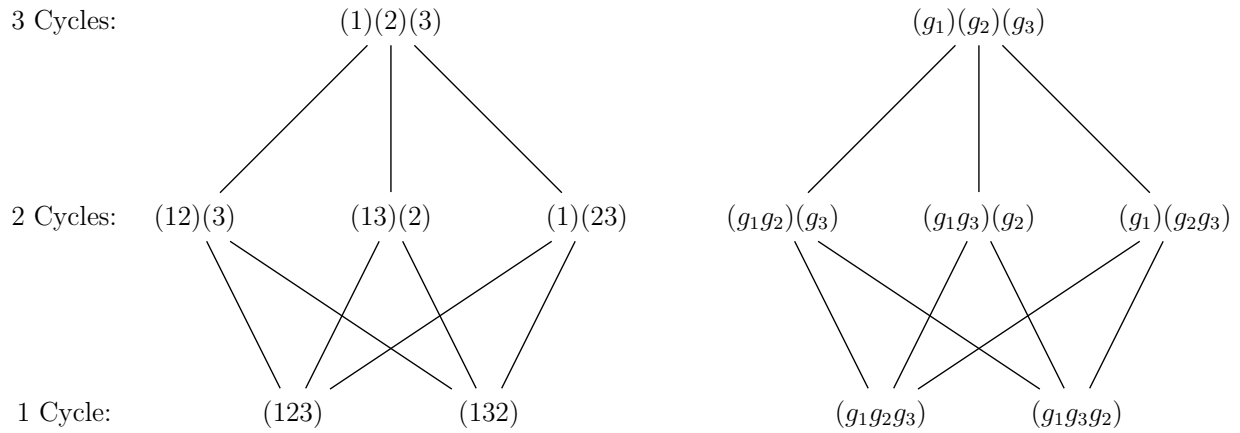
We can expand the 3-character recursively into a sum of products of  $\phi_u$  on different

elements of  $G$ , similar to the proof of Theorem 3.3.

$$\begin{aligned} \phi_u^{(3)}(g_1, g_2, g_3) &= \phi_u(g_1)\phi_u(g_2)\phi_u(g_3) - \phi_u(g_1)\phi_u(g_2g_3) - \phi_u(g_2)\phi_u(g_1g_3) - \phi_u(g_3)\phi_u(g_1g_2). \\ &+ \phi_u(g_1g_2g_3) + \phi_u(g_1g_3g_2) \end{aligned}$$

As we know, this gives rise to using the filigree for  $S_3$ , where here we examine the centrality of  $g_1, g_2, g_3$ , and products of these, as opposed to using the filigree on identity products (e.g.  $(g_1g_3)(g_2)$  means that the product  $g_1g_3$  is in  $Z(G)$ , as well as  $g_2$  itself being central in  $G$ ). See Figure 4.1.

Figure 4.1: The  $S_3$  filigree for  $\phi_u^{(3)}$ : Central Products



$$\begin{aligned}
(g_1)(g_2)(g_3) &\mapsto (p^3 - 3p^2 + 2p)\zeta^{u(t_1+t_2+t_3)} = 6(\zeta^{u(t_1+t_2+t_3)}); \\
(g_1g_2)(g_3) &\mapsto (-p^2 + 2p)(\zeta^{t_1+t_2+t_3+s_1r_2}) = -3(\zeta^{t_1+t_2+t_3+s_1r_2}); \\
(g_1g_3)(g_2) &\mapsto (-p^2 + 2p)(\zeta^{t_1+t_2+t_3+s_1r_3}) = -3(\zeta^{t_1+t_2+t_3+s_1r_3}); \\
(g_2g_3)(g_1) &\mapsto (-p^2 + 2p)(\zeta^{t_1+t_2+t_3+s_2r_3}) = -3(\zeta^{t_1+t_2+t_3+s_2r_3}); \\
(g_1g_2g_3) &\mapsto p(\zeta^{t_1+t_2+t_3+s_1r_2+s_1r_3+s_3r_2}) = 3(\zeta^{t_1+t_2+t_3+s_1r_2+s_1r_3+s_3r_2}); \\
(g_1g_3g_2) &\mapsto p(\zeta^{t_1+t_2+t_3+s_1r_2+s_1r_3+s_2r_3}) = 3(\zeta^{t_1+t_2+t_3+s_1r_2+s_1r_3+s_2r_3}).
\end{aligned}$$

Naturally if no product combination of  $g_1, g_2$  and  $g_3$  is central then  $\phi_u^{(3)}(g_1, g_2, g_3) = 0$ . On the values associated with the transpositions, note that we cannot have two of the transpositions in the center without all three of  $g_1, g_2, g_3$  themselves being central. Note that for  $p = 3$  we were able to directly find the 3-character for  $\phi_u$  without first finding the 2-character.

### 4.3 THE GROUP $AGL(1, p)$

Our next examination will focus on the group  $AGL(1, p)$ , the *affine general linear group* for prime  $p$ . The group  $AGL(1, p)$  is defined as:

$$\left\langle \left( \begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\rangle.$$

The order of  $AGL(1, p)$  is clearly  $p(p - 1)$ . We can define the following cyclic subgroups of  $AGL(1, p)$ , with multiplicative generator as noted:

$$K = \left\langle \left( \begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) \mid b \in \mathbb{F}_p \right\rangle \text{ with generator } \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right);$$



$$H = \left\langle \left( \begin{array}{cc} a & 0 \\ 0 & 1 \end{array} \right) \mid a \in \mathbb{F}_p^\times \right\rangle \text{ with generator } \left( \begin{array}{cc} h & 0 \\ 0 & 1 \end{array} \right), \text{ where } h \text{ generates } \mathbb{F}_p^\times.$$

**Lemma 4.5.** *Every element  $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  of  $AGL(1, p)$  is an invertible matrix with inverse given by the matrix  $\begin{pmatrix} a^{-1} & a^{-1}(-b) \\ 0 & 1 \end{pmatrix}$ . Here  $a^{-1}$  is the multiplicative inverse of  $a$  in  $\mathbb{F}_p^\times$  and  $-b$  is the additive inverse of  $b$  in  $\mathbb{F}_p$ .*

*Proof.* This can be directly verified by matrix multiplication. □

**Lemma 4.6.**  *$K$  is a normal subgroup of  $AGL(1, p)$ .*

*Proof.* Take matrix  $\theta = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$  in  $K$ . Take an arbitrary matrix  $\beta = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$  in  $AGL(1, p)$ . Then

$$\begin{aligned} \beta^{-1}\theta\beta &= \begin{pmatrix} a^{-1} & a^{-1}(-b) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a^{-1} & a^{-1}(t-b) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^{-1}t \\ 0 & 1 \end{pmatrix} \in K. \end{aligned}$$

**Proposition 4.7.** [4, p. 441]  *$AGL(1, p)$  is isomorphic to the semidirect product of  $K$  and  $H$  (where  $H$  acts on  $K$  by matrix multiplication):  $AGL(1, p) \cong K \rtimes H$ .*

The above proposition gives us that  $AGL(1, p)$  is a Frobenius group. As is noted in [17, p. 175],  $G/K \cong H$ , so by Isaacs in [24] we can use the induced characters of  $K$  to find the characters of  $G$ .

**Proposition 4.8.** [25, p. 291] *Let  $H$  be generated by  $\alpha$ . The conjugacy classes of  $AGL(1, p)$  are given as follows.*

$$\{\text{id}\}, K - \{\text{id}\}, K\alpha, K\alpha^2, \dots, K\alpha^{p-2}.$$

Note that the conjugacy classes can be expressed as (right) cosets of  $K$  in the general case, with  $K$  itself splitting into two conjugacy classes in the case of the identity. Using this proposition with the results given in [25, p. 291-292] we can find the character table of  $AGL(1, p)$  for  $p$  an odd prime. There are  $p-1$  irreducible characters of degree 1 and there is a single character of degree  $p-1$ . These results are summarized in Table 4.4 below. (Take  $\zeta = e^{2\pi/p}$ ):

Table 4.4: Character Table for  $AGL(1, p)$ ,  $p$  an odd prime

	id	$K - \{\text{id}\}$	$K\alpha$	$K\alpha^2$	$\dots$	$K\alpha^{p-2}$
$\chi_1$	1	1	1	1	$\dots$	1
$\chi_2$	1	1	$\zeta$	$\zeta^2$	$\dots$	$\zeta^{p-2}$
$\chi_3$	1	1	$\zeta^2$	$\zeta^4$	$\dots$	$\zeta^{2(p-2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$\chi_{p-1}$	1	1	$\zeta^{p-2}$	$\zeta^{2(p-2)}$	$\dots$	$\zeta^{(p-1)(p-2)}$
$\psi$	$p-1$	-1	0	0	$\dots$	0

**Theorem 4.9.** *Let  $\psi^{(p-1)}$  be the  $(p-1)$ -character of  $\psi$ . Take  $g_1, g_2, \dots, g_{p-1} \in AGL(1, p)$ . Then  $\psi^{(p-1)}(g_1, g_2, \dots, g_{p-1})$  is nonzero if and only if there is some permutation  $\sigma \in S_{p-1}$  such that  $g_{\sigma(1)}g_{\sigma(2)} \cdots g_{\sigma(p-1)} \in K$ .*

*Proof.* Once again we can use the filigree for the associated symmetric group. Here the filigree for  $S_{p-1}$  will be employed and we will use the filigree condition of products in  $K$ .

Consider the bottom row of the  $S_{p-1}$  filigree. Each entry consists of a single cycle of length  $p-1$  which can be associated with the possible products of the operands  $g_1, \dots, g_{p-1}$ . Hence if there is no  $(p-1)$ -cycle  $\sigma$  in  $S_{p-1}$  such that  $g_{\sigma(1)}g_{\sigma(2)} \cdots g_{\sigma(p-1)} \in K$  then  $\psi^{(p-1)}$  will be zero, as no entry of the filigree satisfies the filigree condition. Note that if there was some permutation in  $S_{p-1}$  such that  $g_{\sigma(1)}g_{\sigma(2)} \cdots g_{\sigma(p-1)}$  was in  $K$ , then it would have as a consequence of coalescence a  $(p-1)$ -cycle in the filigree. So indeed if there is no  $p-1$ -cycle for which the filigree condition is satisfied, there will be no permutation in general that satisfies the filigree condition.

Conversely suppose that there does exist some permutation  $\sigma$  in  $S_{p-1}$  such that  $g_{\sigma(1)}g_{\sigma(2)} \cdots g_{\sigma(p-1)}$  is in  $K$ . Then we will have that  $\psi^{(p-1)}$  is non-zero as the filigree condition will be satisfied for some element of  $S_{p-1}$ .  $\square$

This concludes our examination of  $k$ -characters.

## CHAPTER 5. RANDOM WALKS ON FINITE GROUPS

### 5.1 DEFINITIONS AND PRELIMINARIES

**5.1.1 Introduction.** This subsection is an overview of introductory material found in [15], [20] and [33]. We let  $G$  be a finite group and  $P$  a *probability distribution* on  $G$  ( $P$  is sometimes referred to in the literature as just a *probability*). We specifically designate the *uniform probability distribution* by  $U$ , where  $U(g) = \frac{1}{|G|}$  for all  $g \in G$ . If  $P$  is a probability distribution on  $G$ , it must satisfy

$$\sum_{g \in G} P(g) = 1 \quad \text{as well as} \quad P(g) \geq 0 \quad \forall g \in G.$$

We let  $\Pi(G)$  be the set of all probabilities on a group  $G$ .

**Definition 5.1.** [15, p. 50] We define a *random walk*<sup>1</sup> on  $G$  as a sequence of  $G$ -valued random variables  $Y_1, Y_2, \dots, Y_m$  (for some integer  $m \geq 1$ ) where

$$Y_m = X_1 \circ X_2 \circ \dots \circ X_m,$$

with the  $X_i$ 's being independent, identically distributed  $G$ -valued random variables, and  $\circ$  being the group operation.

When given some  $P \in \Pi(G)$ , we can write  $P(X_i = g)$  as a matter of shorthand  $P(g)$  for any index  $i$ . (Since all the  $X_i$  are identically distributed, this shorthand is well defined.)

**Definition 5.2.** We define a *convolution* of probability distributions  $P$  and  $Q$  by

$$(P * Q)(s) = \sum_{t \in G} P(t)Q(t^{-1}s).$$

---

<sup>1</sup>Hildebrand [20] indicates an alternative definition that always yields identical probability distributions as the definition given here. The associated Markov chains may differ in the case that  $G$  is non-abelian; this topic, however, lies wholly outside the scope of this work and will not be discussed.

Of note is the fact that if  $P$  and  $Q$  are probability distributions associated with  $G$ -valued independent random variables  $X_1$  and  $X_2$  respectively, then  $P * Q$  is the probability distribution of  $X_1 X_2$  as a random variable on  $G$  (see [20]). We further can define for the probability distribution  $P$  the  $k$ -fold convolution  $P^{(k)} = P * P * \dots * P$  ( $k$ -times). Of particular interest in this chapter are those probability distributions for which the sequence  $\{P^{(k)}\}_{k \in \mathbb{N}}$  reaches the limit  $U$  after a finite number of convolutions. That is, there is some  $k \geq 1$  such that

$$P^{(k)} = P^{(k+1)} = P^{(k+2)} = \dots = U.$$

We designate by  $\Omega(G)$  the set of probability distributions on  $G$  satisfying this criterion. As  $U \in \Omega(G)$ , we know that  $\Omega(G)$  is nonempty. One question that arises is as follows: If  $P^{(k)} = U$ , does it follow that  $P^{(k+r)} = U$  for all positive integers  $r$ ? This is in fact true and is demonstrated in the following theorem:

**Theorem 5.1.** *If  $P^{(k)} = U$ , then  $P^{(k+r)} = U$  for all positive integers  $r$ .*

*Proof.* Assume that  $P^{(k)} = U$ . Then for any  $g \in G$

$$\begin{aligned} P^{(k+r)}(g) &= (P^{(r)} * P^{(k)})(g) = (P^{(r)} * U)(g) \\ &= \sum_{t \in G} P^{(r)}(t) U(t^{-1}g) = \frac{1}{|G|} \sum_{t \in G} P^{(r)}(t) \\ &= \frac{1}{|G|}. \end{aligned}$$

This last equality comes from the totalness of  $P^{(r)}$  as a probability. □

Thus the set  $\Omega(G)$  will consist of all random walks on  $G$  whose associated probability distribution converges to the uniform distribution after some finite number of convolutions. The set  $\Omega(G)$  correlates closely with the set of nilpotent elements of the group algebra  $\mathbb{R}G$ . To wit, Vyshnevetskiy and Zhmud' present and prove the following theorem:

**Theorem 5.3.** *[33, pp. 124, 129] For a finite group  $G$ , the following conditions are equivalent:*

(a)  $\Omega(G) = \{U\}$ .

(b)  $G$  is either abelian or a Hamiltonian 2-group. That is, in the case of the latter,

$G \cong E \times Q$  where  $E$  is an elementary abelian 2-group and  $Q$  is the order 8 quaternion group.

(c) Zero is the only nilpotent element of  $\mathbb{R}G$ .

Let  $x = \sum_g x_g \cdot g$  be an element of  $\mathbb{R}G$ . We then define  $|x| = \sum_g x_g$ . If  $P \in \Pi(G)$ , then we will let  $p = \sum_g P(g) \cdot g$ . As  $P$  is a probability,  $|p| = 1$ . Let  $u = \sum_g \frac{1}{|G|} \cdot g$  designate the element of  $\mathbb{R}G$  associated with  $U$ .

The proceeding properties of  $|\cdot|$  are given without proof in [33]. These are direct results of what is called the augmentation map from  $\mathbb{R}G$  to  $\mathbb{R}$ . For any  $x, y$  in  $\mathbb{R}G$

$$|x + y| = |x| + |y|; \quad |x - y| = |x| - |y|; \quad |xy| = |x| \cdot |y|.$$

**Definition 5.4.** Let  $A$  be an arbitrary ring. We then let  $Nil(A)$  designate the set of all nilpotent elements of  $A$ .

**Theorem 5.5.** [33, p. 124] Let  $A$  be as above. For each  $x \in Nil(A)$ ,  $|x| = 0$ .

*Proof.* For some  $k \in \mathbb{N}$ ,  $x^k = 0$ . Thus  $0 = |x^k| = |x|^k$  and hence  $|x| = 0$ .  $\square$

From Proposition 7.2 in [23] we get a theorem pertaining to the relationships between the coefficients of elements of the conjugacy classes of  $G$ . We will employ this theorem at a later point in this chapter.

**Theorem 5.6.** Let  $C_1, C_2, \dots, C_\ell$  be the distinct conjugacy classes of  $G$ . Define  $x = p - u$  where  $p$  is the element of  $\mathbb{R}G$  associated with some  $P \in \Omega(G)$  and let  $\widetilde{C}_j = \sum_{C_j} x_i$  be the sum of the coefficients from  $x$  of the elements in  $C_j$ , for each  $1 \leq j \leq \ell$ . We then have that  $\widetilde{C}_j = 0$  for each  $j$ .

We provide the following easy lemma and corollary without proof.

**Lemma 5.7.** [33, p. 125] *If  $P \in \Pi(G)$  and  $x = p - u$ , with  $p$  and  $u$  as above, then  $p^n = x^n + u$  for any  $n \in \mathbb{N}$ .*

**Corollary 5.8.** [33, p. 125] *Take  $P \in \Pi(G)$ . Define  $x = p - u$  as above. Then  $P \in \Omega(G)$  if and only if  $x \in Nil(\mathbb{R}G)$ .*

This introduces the crux of the remaining pursuits of this chapter, namely the examination of all such  $x \in Nil(\mathbb{R}G)$  in order to in turn determine the elements of  $\Omega(G)$ . A final theorem from [33, Theorem 1.4] aids us in this pursuit.

**Theorem 5.9.** *If  $P \in \Omega(G)$ , then  $P^{(b)} = U$ , where  $b$  is the maximal degree among the irreducible representations of  $G$  over  $\mathbb{C}$ .*

**5.1.2 Use of the Group Matrix in Random Walks.** Let  $G = \{g_1, g_2, \dots, g_n\}$  be a finite group and let  $X_G = [x_k] = [x_{g_i g_j^{-1}}]$  designate the group matrix associated with  $G$  (see Definition 2.1). Here  $x_k = x_{g_i g_j^{-1}}$  is the  $(i, j)$  entry of  $X_G$  with  $g_k = g_i g_j^{-1}$ . The values of each  $x_k$  are found in the proceeding manner.

Take  $P \in \Pi(G)$ . For any  $g_i, g_j \in G$ , let  $p_k = p_{g_i g_j^{-1}}$  designate the probability of “walking” from  $g_i$  to  $g_j$ . In this manner we can say that  $P = (p_1, p_2, \dots, p_n)$  is a probability distribution on  $G$ . Now let  $x = p - u$  as in the previous section, where  $p$  is the element of  $\mathbb{R}G$  associated with  $P$ . Let  $x_k$  be the associated coefficient on each summand of  $x$  in  $\mathbb{R}G$ .

Per the definition of  $x_k$  given above, we can place a condition on the  $x_k$  for all  $k$ :

$$x_k \geq -\frac{1}{|G|}.$$

This follows from the fact that  $p_k \geq 0$  for all  $k$  and that  $u_k = \frac{1}{|G|}$ . We will find that this condition may at times be made even more rigid because of relations among the elements of the group in question.

The following section will contain further work employing the group matrix.

## 5.2 THE DIHEDRAL GROUP $D_{2q}$

**5.2.1 Introduction to the examination of  $D_{2q}$ .** Let  $G = D_{2q}$  with  $q$  an *odd* prime.

Then  $G$  has the following presentation:

$$\langle r, s \mid r^q = s^2 = \text{id}, \quad srs = r^{q-1} \rangle.$$

Now label the elements of  $G$  as follows:

Table 5.1: Labeling the Elements of  $D_{2q}$

$\text{id}$	$\rightarrow$	$g_1$	$s$	$\rightarrow$	$g_{q+1}$
$r$	$\rightarrow$	$g_2$	$sr$	$\rightarrow$	$g_{q+2}$
$r^2$	$\rightarrow$	$g_3$	$sr^2$	$\rightarrow$	$g_{q+3}$
$r^3$	$\rightarrow$	$g_4$	$sr^3$	$\rightarrow$	$g_{q+4}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r^{q-1}$	$\rightarrow$	$g_q$	$sr^{q-1}$	$\rightarrow$	$g_{2q}$

Let  $m = \frac{q-1}{2}$  and let  $p$  be the element in  $\mathbb{R}G$  corresponding to a probability  $P \in \Omega(D_{2q})$ .

We can then let

$$x_i = p_i - u_i = p_i - \frac{1}{2q}$$

where  $p_i$  indicates the coefficient of the  $i^{\text{th}}$  index coefficient of  $p$  as an element in  $\mathbb{R}G$ .

Associate with each  $g_i$  the coefficient  $x_i$ . Define the element  $e = \sum_G x_i g_i$  in  $\mathbb{R}G$ . Since  $e$  was constructed using a probability  $P$  in  $\Omega(D_{2q})$ , Theorem 5.9 gives that  $e^2 = 0$  (as an irreducible representation of  $D_{2q}$  has degree at most 2). The remaining pursuit of this chapter is to establish what values of the coefficients  $x_i$  of  $e$  can be when we know  $e^2 = 0$ . We have the following relations on the coefficients by Theorem 5.6:

$$x_1 = 0, x_2 = -x_q, x_3 = -x_{q-1}, \dots, x_{m+1} = -x_{m+2},$$

$$x_{q+1} = -(x_{q+2} + x_{q+3} + \dots + x_{2q}).$$

We will refer to  $x_1, x_2, \dots, x_{m+1}, x_{m+2}, \dots, x_q$  as the *lower index variables* and

$x_{q+2}, x_{q+3}, \dots, x_{2q}$  as the *higher index variables*.

We can rewrite  $e$  as follows:

$$\begin{aligned} e = 0 \cdot \mathbf{id} &+ x_q(r^{q-1} - r) + x_{q-1}(r^{q-2} + r^2) + \dots + x_{m+2}(r^{m+2} - r^{m+1}) \\ &+ (-x_{q+2} - x_{q+3} - \dots - x_{2q})s + x_{q+2}sr + \dots + x_{2q}sr^{q-1}. \end{aligned}$$

We now examine the coefficient of the identity element of  $e^2$ .

**Lemma 5.10.** *The coefficient of  $g_1 = \mathbf{id}$  in  $e^2$  is given as follows:*

$$-2 \sum_{j=m+2}^q x_j^2 + 2 \sum_{i=q+2}^{2q} x_i^2 + 2 \sum_{\substack{i,j=q+2 \\ i < j}}^{2q} x_i x_j.$$

*Proof.* The only terms in the product  $e^2$  that contribute to the coefficient of  $\mathbf{id}$  are those products between coefficients  $x_g$  and  $x_{g^{-1}}$  where  $g$  cycles through the elements of  $G$ . For  $2 \leq i \leq m+1$ ,  $x_{g_i}$  can be expressed as the negative of the coefficient on  $g_i^{-1}$ , as given by the above relations. Hence indeed we have a contribution of  $-2x_j^2$  to the coefficient of  $\mathbf{id}$  for  $m+2 \leq j \leq q$ . Each of  $s, sr, sr^2, \dots, sr^{q-1}$  is its own inverse. Hence the square of each of the coefficients of these elements give the remaining contributions to the coefficient of  $\mathbf{id}$  in  $e^2$ . To wit, we have the following contribution from the coefficient of  $s$ :

$$(-x_{q+2} - x_{q+3} - \dots - x_{2q})^2 = \sum_{i=q+2}^{2q} x_i^2 + 2 \sum_{\substack{i,j=q+2 \\ i < j}}^{2q} x_i x_j.$$

The coefficients of each of  $sr, sr^2, \dots, sr^{q-1}$  contribute the remaining square terms, yielding en totale

$$-2 \sum_{j=m+2}^q x_j^2 + 2 \sum_{i=q+2}^{2q} x_i^2 + 2 \sum_{\substack{i,j=q+2 \\ i < j}}^{2q} x_i x_j.$$

This was the desired result. □



**Corollary 5.11.** *The previous lemma, along with Theorem 5.6 gives us the following:*

$$-2 \sum_{j=m+2}^q x_j^2 + 2 \sum_{i=q+2}^{2q} x_i^2 + 2 \sum_{\substack{i,j=q+2 \\ i < j}}^{2q} x_i x_j = 0.$$

**5.2.2 Results of diagonalization of  $X_G$ .** Let  $T : D_{2q} \rightarrow GL_{2q}(\mathbb{C})$  be the regular representation of  $D_{2q}$ . The group matrix  $X_G$  can be associated under the regular representation of  $D_{2q}$  with the element  $e$  from above in the following manner [18, p. 143], [26, p. 300]:

- We can write  $e = \sum_G x_i g_i$  in  $\mathbb{C}G$ .
- Replacing each  $g_i$  with the associated matrix given by  $T(g_i)$ , we then have  $X_G = \sum_G x_i T(g_i)$ .

**Definition 5.12.** [2, p. 25] [7, p. 7] Let  $G$  be any group. Let  $\varrho$  be a representation of  $G$ . The *Fourier Transform at  $\varrho$*  of a function  $f : G \rightarrow \mathbb{C}$  is given by

$$\widehat{f}(\varrho) = \sum_G f(g) \varrho(g).$$

Hence we can say that  $X_{D_{2q}} = \widehat{\Xi}(T)$ , where  $\Xi : D_{2q} \rightarrow \mathbb{C}$  is defined by  $\Xi(g_i) = x_i$ .

We can block diagonalize  $X_{D_{2q}}$ , with blocks corresponding to the irreducible representations of  $D_{2q}$  [7, p. 48-49].

$$X_{D_{2q}} \sim B_1 \oplus B_2 \oplus \Psi_1 \oplus \Psi_1 \oplus \cdots \oplus \Psi_m \oplus \Psi_m,$$

where  $B_1$  and  $B_2$  are the matrices associated with the two characters of  $D_{2q}$  of degree one and the  $\Psi_j$  ( $1 \leq j \leq m$ ) are the  $2 \times 2$  blocks associated with the  $m$  degree 2 irreducible representations of  $D_{2q}$ . Note that each  $\Psi_j$  occurs with multiplicity two. That is to say, given any irreducible representation  $\varrho$  of  $D_{2q}$ , we have a corresponding block in the diagonalization of  $X_{D_{2q}}$  given by  $\widehat{\Xi}(\varrho)$ . Each such block occurs with multiplicity equal to the degree of the associated representation.

We further specify the entries of  $\Psi_j$ :

$$\Psi_j = \begin{pmatrix} m_{11}^{(j)} & m_{12}^{(j)} \\ m_{21}^{(j)} & m_{22}^{(j)} \end{pmatrix}.$$

When the index  $(j)$  is either implied or irrelevant, we will commonly suppress such and denote the entries of  $\Psi_j$  as merely  $m_{11}, m_{12}, m_{21}$ , and  $m_{22}$ .

**Theorem 5.13.** *For any  $1 \leq j \leq m$ , the matrix  $\Psi_j$  has determinant equal to 0. Furthermore, both eigenvalues of  $\Psi_j$  are 0.*

*Proof.* As  $X_{D_{2q}}$  corresponds to  $e$  under the regular representation of  $D_{2q}$  and  $e^2 = 0$  is known from [33], we get  $(X_{D_{2q}})^2 = 0$ . The block diagonalization of  $X_{D_{2q}}$  gives us that each block of  $X_{D_{2q}}$  must be nilpotent of degree less than or equal to 2. Any nilpotent matrix must have determinant equal to 0. Thus  $\det \Psi_j = 0$  for each  $j$ . Moreover, as each eigenvalue of a nilpotent matrix must be 0, the only element of the spectrum of  $\Psi_j$  will be 0.  $\square$

**Corollary 5.14.** *Since the spectrum of  $\Psi_j$  only contains 0, this also tells us that the trace of  $\Psi_j$  is equal to 0.*

Let  $\varrho_j$  designate the  $j^{\text{th}}$  irreducible 2-dimensional representation of  $D_{2q}$ . There are  $m = \frac{q-1}{2}$  such representations. Furthermore,  $\varrho_j$  maps the generators  $r, s$  of  $D_{2q}$  to elements of  $GL_2(\mathbb{C})$  as given in [25, p. 181] and below:

$$\varrho_j(r) = \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix}, \quad \varrho_j(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where  $\zeta = e^{2\pi i/q}$ . We can hence write general elements of  $D_{2q}$  under the representation  $\varrho_j$  in the following manner ( $0 \leq k \leq q-1$ ):

$$\varrho_j(r^k) = \begin{pmatrix} \zeta^{kj} & 0 \\ 0 & \zeta^{-kj} \end{pmatrix}, \quad \varrho_j(sr^k) = \begin{pmatrix} 0 & \zeta^{-kj} \\ \zeta^{kj} & 0 \end{pmatrix}.$$

We now have the following decomposition of  $\Psi_j$ :

$$\begin{aligned} \Psi_j &= \sum_{k=0}^{q-1} \varrho_j(r^k)x_{k+1} + \sum_{k=0}^{q-1} \varrho_j(sr^k)x_{q+k+1} \\ &= \begin{pmatrix} \sum_{k=0}^{q-1} \zeta^{kj}x_{k+1} & 0 \\ 0 & \sum_{k=0}^{q-1} \zeta^{-kj}x_{k+1} \end{pmatrix} + \begin{pmatrix} 0 & \sum_{k=0}^{q-1} \zeta^{-kj}x_{q+k+1} \\ \sum_{k=0}^{q-1} \zeta^{kj}x_{q+k+1} & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sum_{k=1}^m (\zeta^{kj} - \zeta^{-kj})x_{k+1} & \sum_{k=0}^{q-1} \zeta^{-kj}x_{q+k+1} \\ \sum_{k=0}^{q-1} \zeta^{kj}x_{q+k+1} & \sum_{k=1}^m (\zeta^{-kj} - \zeta^{kj})x_{k+1} \end{pmatrix} \end{aligned}$$

where the diagonal entries of the final matrix can be confirmed by observing first that  $x_1 = 0$  (by Theorem 5.6) and also that  $x_{2+k} = -x_{q-k}$  for  $0 \leq k < q-2$ .

**Observation 5.15.** As each of the  $x_i$  are real, the above decomposition shows us that the off-diagonal entries of  $\Psi_j$  are complex conjugates of one another. That is,  $m_{12} = \overline{m_{21}}$ . Furthermore, note that  $m_{11} = \overline{m_{22}}$  and  $m_{11} = -m_{22}$  (this latter fact follows from  $\text{Tr } \Psi_j = 0$ ). This allows us to conclude that the real part of  $m_{11}$  and  $m_{22}$  is zero.

Let  $\lambda_{kj} = \zeta^{kj} - \zeta^{-kj}$  and let  $\Lambda = [\lambda_{kj}]$ , an  $m \times m$  matrix. We know that  $\Psi_j$  has determinant 0 from Theorem 5.13. Hence we know that  $m_{11}m_{22} = m_{12}m_{21}$ . Furthermore,

since  $\text{Tr } \Psi_j = 0$  implies  $m_{11} = -m_{22}$ , we have that  $(m_{11})^2 = -m_{12}m_{21}$ . Indeed, in a sufficient ring extension, we have  $m_{11} = \sqrt{-m_{12}m_{21}} = -i|m_{12}|$ . This final equality follows from the fact that  $m_{12} = \overline{m_{21}}$ .

In Table 4.1 we gave a general form of the character table for  $D_{2q}$  ( $q$  being odd). Here we provide this character table again, this time in an expanded rendering. This version of the character table can be confirmed by use of [14]. The utility of such an exposition will become apparent in the theorem that follows.

Table 5.2: Character Table of  $D_{2q}$

	id	$s$	$r$	$r^2$	$\dots$	$r^m$
$\chi_1$	1	1	1	1	$\dots$	1
$\chi_2$	1	-1	1	1	$\dots$	1
$\psi_1$	2	0	$\zeta - \zeta^{-1}$	$\zeta^2 - \zeta^{-2}$	$\dots$	$\zeta^m - \zeta^{-m}$
$\psi_2$	2	0	$\zeta^2 - \zeta^{-2}$	$\zeta^4 - \zeta^{-4}$	$\dots$	$\zeta^{2m} - \zeta^{-2m}$
$\psi_3$	2	0	$\zeta^3 - \zeta^{-3}$	$\zeta^6 - \zeta^{-6}$	$\dots$	$\zeta^{3m} - \zeta^{-3m}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$\psi_m$	2	0	$\zeta^m - \zeta^{-m}$	$\zeta^{2m} - \zeta^{-2m}$	$\dots$	$\zeta^{m^2} - \zeta^{-m^2}$

**Theorem 5.16.** *The matrix  $\Lambda$  is invertible.*

*Proof.* The first order of business is to notice that  $\Lambda$  appears in the lower right corner of Table 5.2. Treating the entries of Table 5.2 as entries of a matrix, we get an invertible  $(m+2) \times (m+2)$  matrix (a character table is always an invertible matrix). Call this matrix  $C$ .

Suppose that  $\Lambda$  has rank less than or equal to  $m-2$ . This would then imply that  $C$  is not an invertible matrix. Hence  $\Lambda$  has rank greater than or equal to  $m-1$ .

Suppose that  $\Lambda$  has rank  $m-1$ . Let  $C_1, C_2, \dots, C_{m+2}$  be the columns of  $C$ . Since  $\Lambda$  is supposed to have rank  $m-1$ , there exists scalars  $\beta_3, \beta_4, \dots, \beta_{m+2}$  not all zero such that

$$\sum_{i=3}^{m+2} \beta_i C_i = (k, k, 0, \dots, 0)^T.$$

Since the  $C_3, C_4, \dots, C_{m+2}$  are linearly dependent,  $k \neq 0$ . This means that in fact  $(1, 1, 0, \dots, 0)^T$  is in the span of the columns containing  $\Lambda$ . So we have that in fact  $C$  is row equivalent to the following matrix:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & -1 & 0 & 0 & \dots & 0 \\ 2 & 0 & \zeta - \zeta^{-1} & \zeta^2 - \zeta^{-2} & \dots & \zeta^m - \zeta^{-m} \\ 2 & 0 & \zeta^2 - \zeta^{-2} & \zeta^4 - \zeta^{-4} & \dots & \zeta^{2m} - \zeta^{-2m} \\ 2 & 0 & \zeta^3 - \zeta^{-3} & \zeta^6 - \zeta^{-6} & \dots & \zeta^{3m} - \zeta^{-3m} \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 2 & 0 & \zeta^m - \zeta^{-m} & \zeta^{2m} - \zeta^{-2m} & \dots & \zeta^{m^2} - \zeta^{-m^2} \end{pmatrix}.$$

Since we have a zero block in the upper right hand corner, we know that the determinant of  $M$  is  $-2 \det \Lambda = \det C \neq 0$ . But this implies that  $\det \Lambda \neq 0$  (while we assumed otherwise). So in fact  $\Lambda$  cannot have rank less than  $m$ . Since  $\Lambda$  has rank  $m$ , then  $\Lambda$  is invertible.  $\square$

We will let  $\Lambda^{-1} = [\mu_{ij}]$ . The above theorem allows us to state a subsequent corollary.

**Corollary 5.17.** *We can write  $x_1, x_2, \dots, x_q$  in terms of  $x_{q+1}, x_{q+2}, \dots, x_{2q}$ .*

*Proof.* For the lower index variables, we have the following aforementioned pairings from Theorem 5.6. We now write  $x_2, x_3, \dots, x_{m+1}$  in terms of the higher index variables. Let  $v = (x_2, x_3, \dots, x_{m+1})$  be a vector of length  $m$  as depicted. Then

$$\Lambda v^T = \begin{pmatrix} \sum_{j=1}^m \lambda_{1j} x_j \\ \sum_{j=1}^m \lambda_{2j} x_j \\ \vdots \\ \sum_{j=1}^m \lambda_{mj} x_j \end{pmatrix} = \begin{pmatrix} -|m_{12}^{(1)}| \\ -|m_{12}^{(2)}| \\ \vdots \\ -|m_{12}^{(m)}| \end{pmatrix}.$$

Remember that each  $m_{12}^{(k)}$  is a polynomial only in terms of the higher index variables. Since  $\Lambda$  is invertible, this allows us to write the vector  $v$  as follows:

$$\Lambda^{-1}\Lambda v^T = v^T = \Lambda^{-1} \begin{pmatrix} -|m_{12}^{(1)}| \\ -|m_{12}^{(2)}| \\ \vdots \\ -|m_{12}^{(m)}| \end{pmatrix} = \begin{pmatrix} -\sum_{j=1}^m \mu_{1j} |m_{12}^{(1)}| \\ -\sum_{j=1}^m \mu_{2j} |m_{12}^{(2)}| \\ \vdots \\ -\sum_{j=1}^m \mu_{mj} |m_{12}^{(m)}| \end{pmatrix}.$$

We have now written the lower index variables in terms of the higher index variables.  $\square$

Hence the lower index variables are dependent on the higher index variables.

**5.2.3 Finding solutions to the equation  $e^2 = 0$ .** Our main pursuit is now to obtain results relevant to the set of solutions satisfying  $e^2 = 0$ , where  $e$  is as defined above in Section 5.2.1. We have already seen some efforts in this regard in Corollary 5.17. Let  $\text{Coeff}(e^2)$  be the set of nonzero coefficients of  $e^2$ . We will consider the dihedral groups  $D_{2q}$  for the primes  $q = 3, 5, 7$ .

**Observation 5.18.** As  $x_i \geq -\frac{1}{2q}$  for each  $i$ , it follows from Section 5.2.1 that

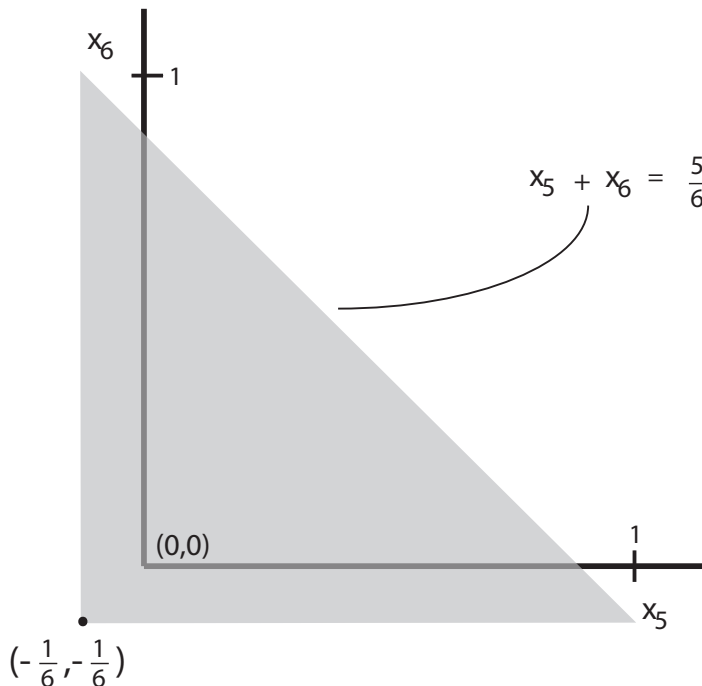
$$x_{q+1} \leq -\left(-\frac{1}{2q} - \frac{1}{2q} - \dots - \frac{1}{2q}\right) = \frac{q-1}{2q}.$$

**5.2.3.1 The case  $q = 3$ .** We first inspect  $D_6$ , the dihedral group of order 6. We know that each of  $x_2, x_3, x_4, x_5, x_6$  are greater than or equal to  $-\frac{1}{6}$  (and  $x_1 = 0$ ). Furthermore we have the following relationships between the variables:

$$x_2 = -x_3, \quad x_4 = -(x_5 + x_6).$$

By Observation 5.18, we have  $x_4 \leq \frac{1}{3}$ . Moreover, we have  $-\frac{1}{6} \leq x_2, x_3 \leq \frac{1}{6}$ . We have a 2-simplex in the variables  $x_5$  and  $x_6$  since  $x_5, x_6 \geq -\frac{1}{6}$  and  $x_5 + x_6 \leq \frac{5}{6}$ . (See Figure 5.1.)

Figure 5.1: The 2-simplex for  $x_5$  and  $x_6$



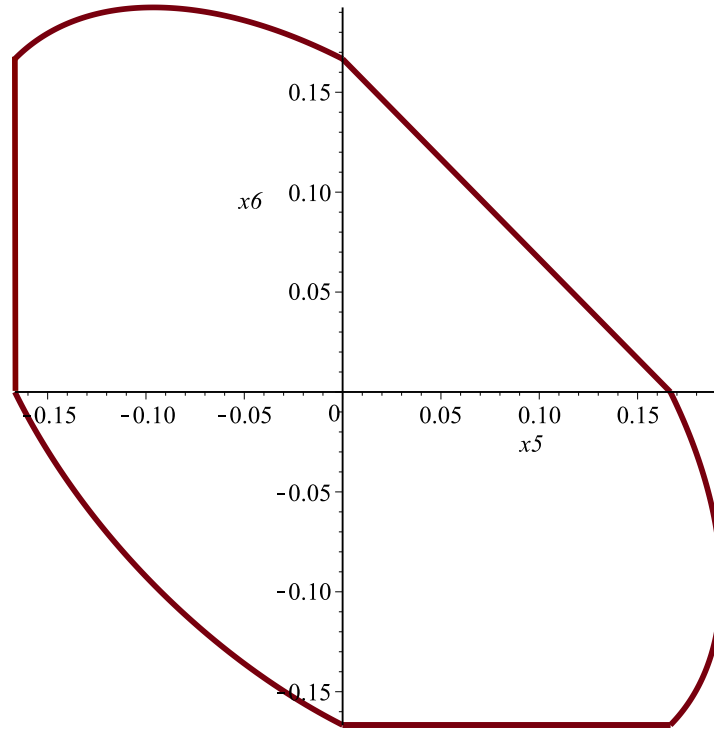
The variables  $x_5$  and  $x_6$  comprise the independent variables and the lower index variables  $x_2$  and  $x_3$  comprise the dependent variables in the solutions to  $e^2 = 0$ . All solutions will lie above this simplex. Finding a Gröbner basis for the ideal generated by the coefficients of  $e^2$  and the equations given by Theorem 5.6 gives us the previously found relationships between the coefficients of  $e$ , as well as the following additional relationship:

$$x_3^2 - x_5^2 - x_5x_6 - x_6^2 = 0.$$

This allows us to relate  $x_3$  to  $x_5$  and  $x_6$ , which in turn allows us to determine  $x_2$ .

The 2-simplex above can be improved upon by observing the constraint on the lower bound of the  $x_i$  (to wit,  $x_i \geq -\frac{1}{6}$ ) and solving explicitly for a 2-simplex for the solutions. The resulting 2-simplex is given in Figure 5.2 below.

Figure 5.2: Explicit 2-simplex for  $x_5$  and  $x_6$  under constraint  $x_i \geq -\frac{1}{6}$



The rounded curve on the top of the figure is given by the equation

$$x_6 = -\frac{x_5}{2} + \frac{1}{6}\sqrt{1 - 27x_5^2} \quad \text{for } -\frac{1}{6} \leq x_5 \leq 0.$$

The rounded curve on the bottom left corner of the figure is given by the equation

$$x_6 = -\frac{x_5}{2} - \frac{1}{6}\sqrt{1 - 27x_5^2} \quad \text{for } -\frac{1}{6} \leq x_5 \leq 0.$$

The rounded curve on the bottom right corner of the figure is given by two equations:

$$x_6 = -\frac{x_5}{2} \pm \frac{1}{6}\sqrt{1 - 27x_5^2} \quad \text{for } \frac{1}{6} \leq x_5 \leq \frac{1}{3\sqrt{3}}.$$



The line of negative slope in the first quadrant is given by

$$x_6 = \frac{1}{6} - x_5,$$

and the horizontal and vertical lines are given by  $x_5 = -\frac{1}{6}$  and  $x_6 = -\frac{1}{6}$  respectively.

**5.2.3.2 The case  $q = 5$ .** Our examination turns now to  $q = 5$ , the group in question being  $D_{10}$ . We desire here to determine, under certain conditions, the values for the coefficients on  $e$  which yield solutions to  $e^2 = 0$ . The basic approach which we employ is to set some of the coefficients of  $e$  equal to 0, then seek to find a solution to  $e^2 = 0$  among the remaining variables. An example of this process is described below. But first we provide a relevant definition.

**Definition 5.19.** Let  $\mathcal{I}$  be an ideal in  $\mathbb{C}[x_1, x_2, \dots, x_n]$ , where  $n$  is a positive integer. Take a subset  $S$  of  $\{1, 2, \dots, n\}$  consisting of  $m$  elements  $s_1, s_2, \dots, s_m$ . We can then associate with  $S$  an *elimination ideal*  $\mathcal{I}_S$  given by

$$\mathcal{I}_S = \mathcal{I} \cap \mathbb{C}[x_{s_1}, x_{s_2}, \dots, x_{s_m}].$$

Elimination ideals are commonly used in conjunction with a Gröbner basis.

**Example.** Here we demonstrate a process for finding a set containing solutions to  $e^2$ . We first create the ideal  $\mathcal{C}$  in the polynomial algebra  $\mathbb{C}[x_1, x_2, \dots, x_{10}]$ :

$$\mathcal{C} = \left\langle \text{Coeff}(e^2), x_4^2 + x_5^2 + x_7^2 + x_8^2 + x_9^2 - 1 + \frac{1}{10}, x_{10} \right\rangle$$

Recall that  $\text{Coeff}(e^2)$  is the set of nonzero coefficients of  $e^2$ . The creation of  $\mathcal{C}$  allows us to seek for solutions to  $e^2 = 0$  in the quotient ring  $\mathbb{C}[x_1, x_2, \dots, x_{10}]/\mathcal{C}$ . Seeking for solutions to  $e^2 = 0$  in this quotient ring is equivalent to setting  $x_{10}$  to 0 and finding solutions among the remaining variables. Furthermore, in order to produce a compact space containing solutions

to the equation, we intersect the variety of  $e^2$  with a 4-sphere of radius  $1 - \frac{1}{10}$  in the variables  $x_4, x_5, x_7, x_8, x_9$ . By including  $x_{10}$  itself as a generator  $\mathcal{C}$  we are effectively setting  $x_{10}$  equal to 0. This is done to give us a solution space that can be plotted over three variables.<sup>2</sup> Overall, we obtain a compact space which contains as a subset a set of solutions to  $e^2 = 0$  whose coefficients are at most  $1 - \frac{1}{10}$  and are determined by the values of  $x_4, x_5, x_7, x_8$ , and  $x_9$ . We calculate a Gröbner basis for  $\mathcal{C}$ , then find the associated elimination ideal for the variables  $x_4, x_8, x_9$ . This elimination ideal is generated by a single element, as given below:

$$\begin{aligned}
& x_4^8 + \frac{9}{10}x_4^6x_8^2 + \frac{4}{5}x_4^6x_8x_9 + \frac{11}{10}x_4^6x_9^2 - \frac{6}{5}x_4^6 + \frac{181}{400}x_4^4x_8^4 + \frac{9}{5}x_4^4x_8^3x_9 + \frac{539}{200}x_4^4x_8^2x_9^2 - \frac{43}{50}x_4^4x_8^2 \\
& + \frac{23}{10}x_4^4x_8x_9^3 - \frac{13}{10}x_4^4x_8x_9 + \frac{421}{400}x_4^4x_9^4 - \frac{31}{25}x_4^4x_9^2 + \frac{23}{50}x_4^4 + \frac{3}{100}x_4^2x_8^6 + \frac{71}{200}x_4^2x_8^5x_9 \\
& + \frac{103}{100}x_4^2x_8^4x_9^2 - \frac{19}{100}x_4^2x_8^4 + \frac{369}{200}x_4^2x_8^3x_9^3 - \frac{187}{200}x_4^2x_8^3x_9 + \frac{93}{50}x_4^2x_8^2x_9^4 - \frac{311}{200}x_4^2x_8^2x_9^2 \\
& + \frac{41}{200}x_4^2x_8^2 + \frac{63}{50}x_4^2x_8x_9^5 - \frac{301}{200}x_4^2x_8x_9^3 + \frac{21}{50}x_4^2x_8x_9 + \frac{12}{25}x_4^2x_9^6 - \frac{143}{200}x_4^2x_9^4 \\
& + \frac{71}{200}x_4^2x_9^2 + \frac{3}{50}x_4^2 + \frac{1}{25}x_8^8 + \frac{9}{50}x_8^7x_9 + \frac{9}{16}x_8^6x_9^2 - \frac{2}{25}x_8^6 + \frac{21}{20}x_8^5x_9^3 - \frac{7}{25}x_8^5x_9 \\
& + \frac{147}{100}x_8^4x_9^4 - \frac{137}{200}x_8^4x_9^2 + \frac{3}{50}x_8^4 + \frac{27}{20}x_8^3x_9^5 - \frac{183}{200}x_8^3x_9^3 + \frac{29}{200}x_8^3x_9 + \frac{9}{10}x_8^2x_9^6 \\
& - \frac{87}{100}x_8^2x_9^4 + \frac{101}{400}x_8^2x_9^2 - \frac{1}{50}x_8^2 + \frac{9}{25}x_8x_9^7 - \frac{9}{20}x_8x_9^5 + \frac{37}{200}x_8x_9^3 - \frac{1}{40}x_8x_9 \\
& + \frac{9}{100}x_9^8 - \frac{3}{20}x_9^6 + \frac{37}{400}x_9^4 - \frac{1}{40}x_9^2 + \frac{1}{400}.
\end{aligned}$$

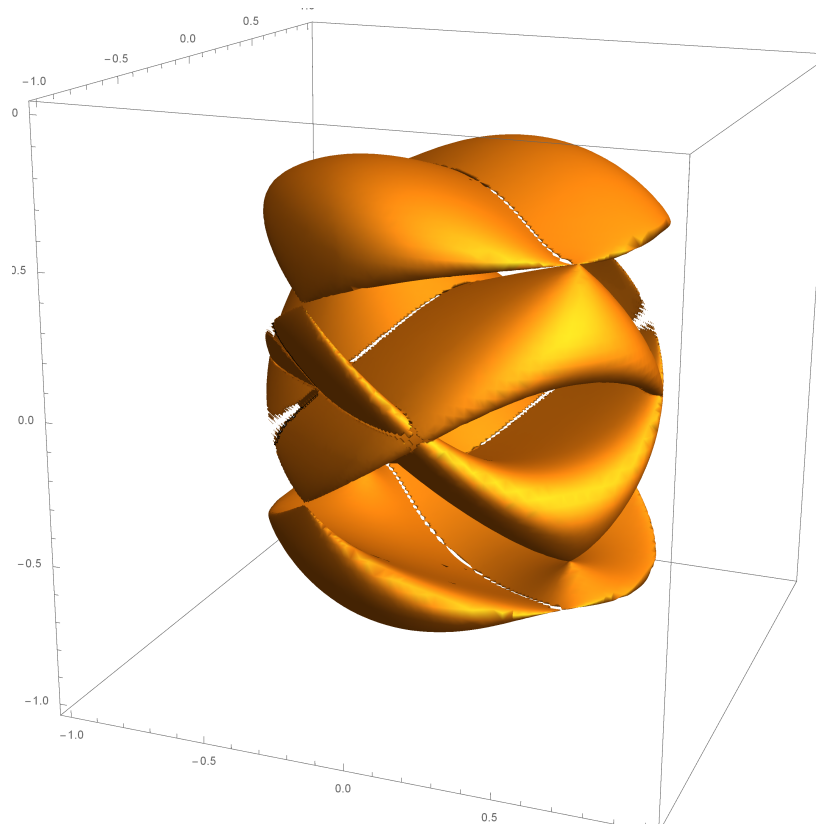
This polynomial produces a space of solutions as shown in Figures 5.3a and 5.3b (alternate views of the same space):

---

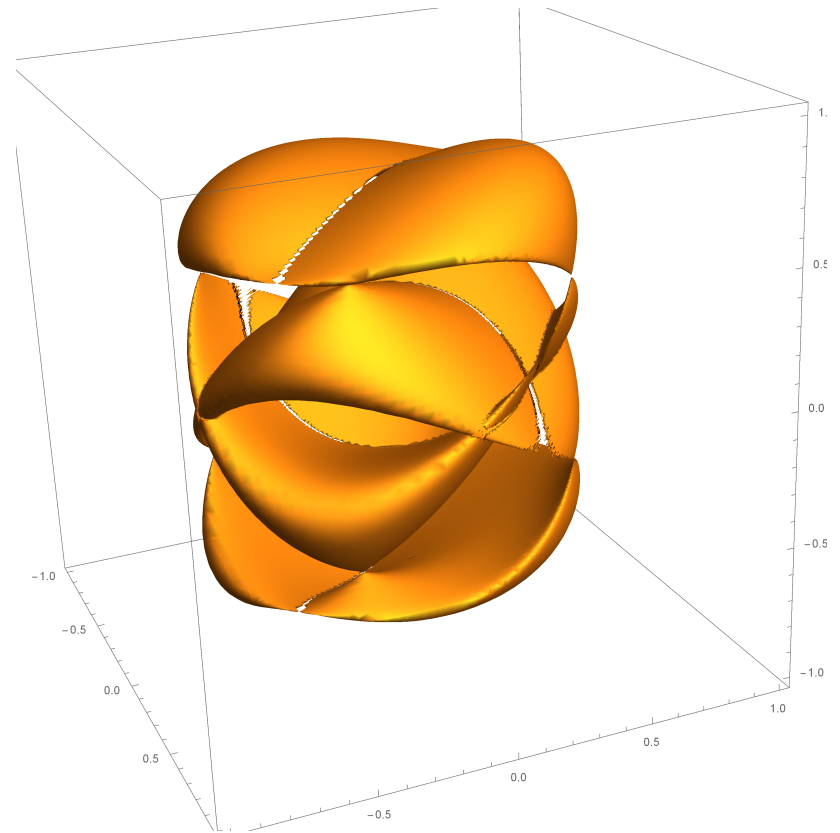
<sup>2</sup>When all of the larger index variables were allowed to take on non-zero values, solution spaces were described by three or more free variables, making even an implicit plot impossible in only three dimensions. Further work on  $D_{10}$  should focus on describing these more robust solution sets.

Figure 5.3: Subspace of solutions to  $e^2 = 0$  ( $D_{10}$ )

(a) Elimination ideal for  $x_4, x_8,$  and  $x_9$  view I



(b) Elimination ideal for  $x_4, x_8,$  and  $x_9$  view II



It is again important to note that this space is not the *only* set of solutions to  $e^2 = 0$ . These results are only one sliver of a considerable set of solutions.

The preceding example can be repeated for the following triples of variables:

$$(x_4, x_7, x_8), (x_4, x_7, x_9), (x_4, x_7, x_{10}), (x_4, x_8, x_{10}), (x_4, x_9, x_{10})$$

$$(x_5, x_7, x_8), (x_5, x_7, x_9), (x_5, x_7, x_{10}), (x_5, x_8, x_9), (x_5, x_8, x_{10}), (x_5, x_9, x_{10})$$

Each triple produces results very similar (in terms of geometric considerations) to the triple  $(x_4, x_8, x_9)$  given in the example, although no two spaces are identical.

**5.2.3.3 The case  $q = 7$ .** We now examine the group  $D_{14}$ . We can perform a similar method of examination here as we did with  $D_{10}$ . Again we seek to determine, under certain conditions, the values for the higher index variables which yield solutions to  $e^2 = 0$ . To simplify the situation,<sup>3</sup> we will set some of the higher index variables to 0, then find solutions to  $e^2 = 0$  among the remaining higher index variables. This is demonstrated below.

**Example.** Here we will be looking at solutions to  $e^2 = 0$  comprised only of the variables  $x_9, x_{10}, x_{11}$ . We create the ideal

$$\mathcal{D} = \langle \text{Coeff}(e^2), x_{12}, x_{13}, x_{14} \rangle$$

in  $\mathbb{C}[x_1, \dots, x_{14}]$ . This sets the variables  $x_{12}, x_{13}, x_{14}$  equal to zero. We next calculate a Gröbner basis for  $\mathcal{D}$ , then find the associated elimination ideal for the variables  $x_7, x_9, x_{10}, x_{11}$ . In order to produce a compact space containing solutions of  $e^2 = 0$ , we intersect the variety of  $e^2$  over the variables  $x_7, x_9, x_{10}, x_{11}$  with a 3-sphere of radius  $1 - \frac{1}{14}$  in the variables  $x_7, x_9, x_{10}, x_{11}$ . This allows us to obtain a compact set of solutions to  $e^2 = 0$  for which none of the coordinates exceeds  $1 - \frac{1}{14}$ . This is important due to the fact that  $e = p - u$  restricts the size of the coefficients of  $e$ . Finding a Gröbner basis for the resulting ideal, yields

---

<sup>3</sup>When all of the higher index variables were allowed to be non-zero, MAGMA was unable to find a Gröbner basis in any reasonable ( $\sim 24$  hours) amount of time.

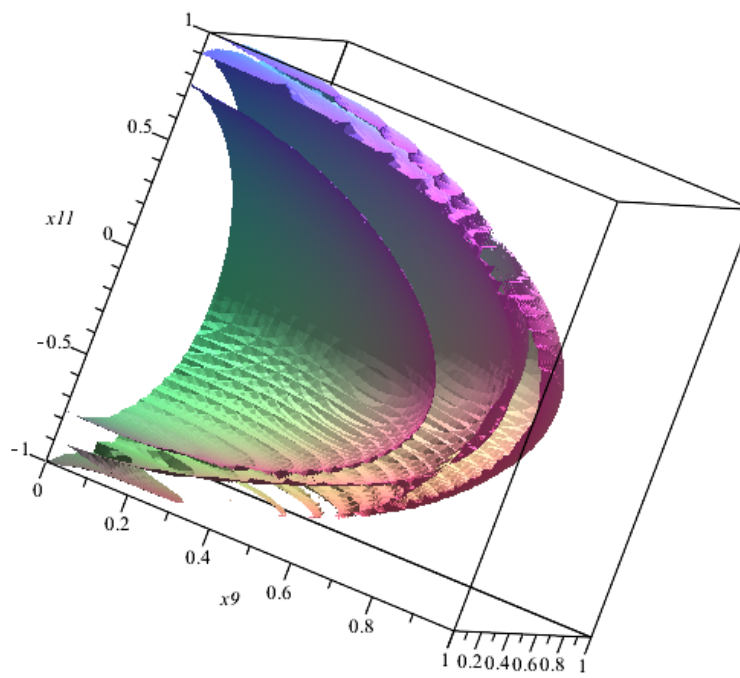
two polynomials in  $\mathbb{C}[x_7, x_9, x_{10}, x_{11}]$ . The first of these corresponds to the aforementioned 3-sphere. The second of these is given as follows:

$$\begin{aligned}
& x_9^8 + \frac{6788}{5993}x_7x_{10} + \frac{1796}{5993}x_7x_{11} + \frac{28558}{5993}x_9^6x_{10}^2 + \frac{6984}{5993}x_9^6x_{10}x_{11} + \frac{23994}{5993}x_9^6x_{11}^2 - \frac{9734}{3227}x_9^6 + \frac{22124}{5993}x_9^5x_{10}^3 \\
& + \frac{9424}{5993}x_9^5x_{10}^2x_{11} + \frac{21108}{5993}x_9^5x_{10}x_{11}^2 - \frac{8686}{3227}x_9^5x_{10} + \frac{5944}{5993}x_9^5x_{11}^3 - \frac{2466}{3227}x_9^5x_{11} \\
& + \frac{47705}{5993}x_9^4x_{10}^4 + \frac{21688}{5993}x_9^4x_{10}^3x_{11} + \frac{6536}{461}x_9^4x_{10}^2x_{11}^2 - \frac{34190}{3227}x_9^4x_{10}^2 + \frac{20972}{5993}x_9^4x_{10}x_{11}^3 \\
& - \frac{8882}{3227}x_9^4x_{10}x_{11} + \frac{35771}{5993}x_9^4x_{11}^4 - \frac{29156}{3227}x_9^4x_{11}^2 + \frac{3107}{922}x_9^4 + \frac{23624}{5993}x_9^3x_{10}^5 + \frac{12988}{5993}x_9^3x_{10}^4x_{11} \\
& + \frac{45108}{5993}x_9^3x_{10}^3x_{11}^2 - \frac{18938}{3227}x_9^3x_{10}^3 + \frac{20476}{5993}x_9^3x_{10}^2x_{11}^3 - \frac{8718}{3227}x_9^3x_{10}^2x_{11} + \frac{22020}{5993}x_9^3x_{10}x_{11}^4 \\
& - \frac{17998}{3227}x_9^3x_{10}x_{11}^2 + \frac{975}{461}x_9^3x_{10} + \frac{6408}{5993}x_9^3x_{11}^5 - \frac{5394}{3227}x_9^3x_{11}^3 + \frac{299}{461}x_9^3x_{11} + \frac{33672}{5993}x_9^2x_{10}^6 \\
& + \frac{22176}{5993}x_9^2x_{10}^5x_{11} + \frac{93222}{5993}x_9^2x_{10}^4x_{11}^2 - \frac{37388}{3227}x_9^2x_{10}^4 + \frac{42852}{5993}x_9^2x_{10}^3x_{11}^3 - \frac{18542}{3227}x_9^2x_{10}^3x_{11} \\
& + \frac{83912}{5993}x_9^2x_{10}^2x_{11}^4 - \frac{67700}{3227}x_9^2x_{10}^2x_{11}^2 + \frac{7111}{922}x_9^2x_{10}^2 + \frac{20604}{5993}x_9^2x_{10}x_{11}^5 - \frac{17622}{3227}x_9^2x_{10}x_{11}^3 \\
& + \frac{988}{461}x_9^2x_{10}x_{11} + \frac{23770}{5993}x_9^2x_{11}^6 - \frac{29052}{3227}x_9^2x_{11}^4 + \frac{6201}{922}x_9^2x_{11}^2 - \frac{1521}{922}x_9^2 + \frac{8288}{5993}x_9x_{10}^7 \\
& + \frac{5392}{5993}x_9x_{10}^6x_{11} + \frac{23672}{5993}x_9x_{10}^5x_{11}^2 - \frac{10120}{3227}x_9x_{10}^5 + \frac{14012}{5993}x_9x_{10}^4x_{11}^3 - \frac{6040}{3227}x_9x_{10}^4x_{11} \\
& + \frac{23160}{5993}x_9x_{10}^3x_{11}^4 - \frac{19254}{3227}x_9x_{10}^3x_{11}^2 + \frac{1066}{461}x_9x_{10}^3 + \frac{10808}{5993}x_9x_{10}^2x_{11}^5 - \frac{9358}{3227}x_9x_{10}^2x_{11}^3 \\
& + \frac{533}{461}x_9x_{10}^2x_{11} + \frac{7744}{5993}x_9x_{10}x_{11}^6 - \frac{9458}{3227}x_9x_{10}x_{11}^4 + \frac{1014}{461}x_9x_{10}x_{11}^2 - \frac{507}{922}x_9x_{10} \\
& + \frac{2284}{5993}x_9x_{11}^7 - \frac{2906}{3227}x_9x_{11}^5 + \frac{325}{461}x_9x_{11}^3 - \frac{169}{922}x_9x_{11} + \frac{656}{461}x_{10}^8 + \frac{576}{461}x_{10}^7x_{11} + \frac{32280}{5993}x_{10}^6x_{11}^2 \\
& - \frac{12912}{3227}x_{10}^6 + \frac{21568}{5993}x_{10}^5x_{11}^3 - \frac{9528}{3227}x_{10}^5x_{11} + \frac{45585}{5993}x_{10}^4x_{11}^4 - \frac{36500}{3227}x_{10}^4x_{11}^2 + \frac{1898}{461}x_{10}^4 \\
& + \frac{20788}{5993}x_{10}^3x_{11}^5 - \frac{18106}{3227}x_{10}^3x_{11}^3 + \frac{1040}{461}x_{10}^3x_{11} + \frac{27814}{5993}x_{10}^2x_{11}^6 - \frac{33622}{3227}x_{10}^2x_{11}^4 \\
& + \frac{7059}{922}x_{10}^2x_{11}^2 - \frac{845}{461}x_{10}^2 + \frac{6724}{5993}x_{10}x_{11}^7 - \frac{8654}{3227}x_{10}x_{11}^5 + \frac{975}{461}x_{10}x_{11}^3 - \frac{507}{922}x_{10}x_{11} \\
& + x_{11}^8 - \frac{9734}{3227}x_{11}^6 + \frac{3107}{922}x_{11}^4 - \frac{1521}{922}x_{11}^2 + \frac{2197}{7376}.
\end{aligned}$$

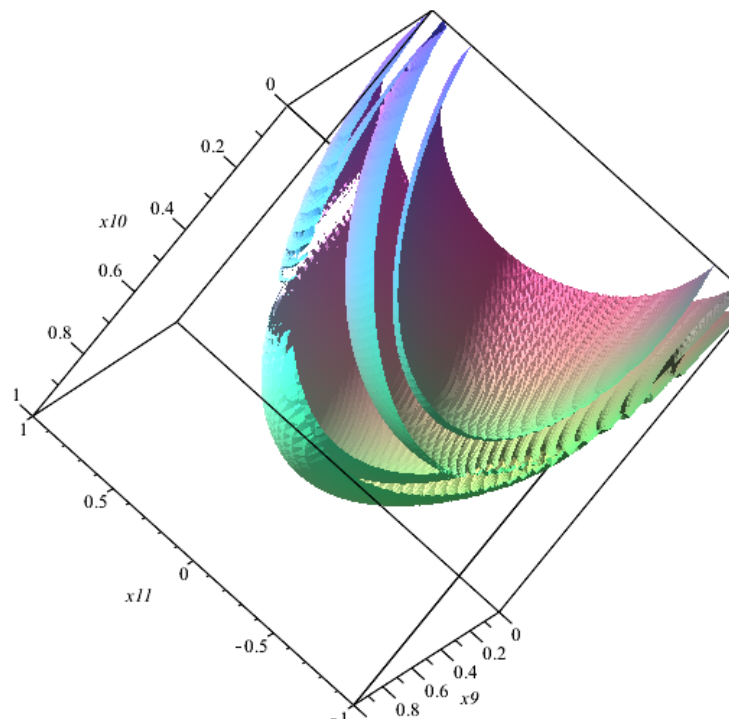
Solutions to this polynomial produce a 4-fold cover of a 2-sphere. Figures 5.4a and 5.4b provide two views of a cut-away of a quarter of this 4-fold cover.

Figure 5.4: Space containing solutions to  $e^2 = 0$  ( $D_{14}$ )

(a) 4-fold cover of a 2-sphere (I)



(b) 4-fold cover of a 2-sphere (II)



As with the example given for  $D_{10}$ , this space represents a compact space containing solutions to  $e^2 = 0$ . In order to further inspect this 4-fold cover (and keeping in mind that 3-dimensional depictions of it, such as above, are ultimately insufficient), we perform several examinations of its properties.

One of the simplest investigations we can make is that of taking 2-dimensional cross sections of the 4-fold cover, much as if we were slicing an onion. See Figures A.1a through A.1q in Appendix A for an example of such a process. This exercise of examining cross sections allows us to confirm that indeed the cover in general has four distinct sheets, as well as verify that the 4-fold cover is symmetric with respect to the plane  $x_9 + x_{10} + x_{11} = 0$ .

We can also examine topological aspects of this 4-fold cover. First we provide some definitions.

**Definition 5.20.** [10, p. 175] Let  $S$  and  $T$  be compact Riemann surfaces. Let

$$\gamma : S \rightarrow T$$

be a nonconstant holomorphic map. For each point  $p$  of  $S$ , there is a natural number  $k$ , and local coordinates  $s \in S$  around  $p$  and  $t \in T$  around  $\gamma(p)$  such that  $\gamma$  is given by

$$s \mapsto t = s^k.$$

We call  $\text{ord}_p(\gamma)$  the *order of  $\gamma$  at  $p$*  and define

$$v_p(\gamma) := \text{ord}_p(\gamma) - 1$$

to be the *branching order* of  $\gamma$  at  $p$ .

**Definition 5.21.** [10, p. 175] Let  $\gamma, p, S$ , and  $T$  be as in the previous definition. We say that  $p \in S$  is a *branch point* if

$$v_p(\gamma) \geq 1.$$

**Definition 5.22.** [10, p. 189] Let  $\varphi : W \rightarrow Y$  be a continuous map. Then  $\varphi$  is called a *covering* of  $Y$  if for every point  $q \in Y$ , there exists an open neighborhood  $V$  with the following property: if we let

$$\varphi^{-1}(V) = \bigcup_{i \in I} U_i$$

be the decomposition of  $\varphi^{-1}(V)$  into connected components, then for every  $i$  in indexing set  $I$ , the map

$$\varphi|_{U_i} : U_i \rightarrow V$$

is a homeomorphism.

Fischer [10] provides the following lemma without proof.

**Lemma 5.23.** [10, p. 176] *Let  $M$  be the set of all branch points (many times called the branch set) of  $\gamma$ , where  $\gamma$  and its domain and codomain are again as in the first two definitions. Let  $S' = S - \gamma^{-1}(M)$  and  $T' = T - M$ . Then the restriction of  $\gamma$  to  $S'$  is a covering in the sense of Definition 5.22.*

We many times speak of the map  $\gamma$  as a *branched cover*, although such a term is, strictly speaking, nonuniform. For our specific purposes here, we inspect the 4-fold cover as a branched cover of a 2-sphere. As above, let  $M$  denote the branch set of the 4-fold cover. We note that at a branch point we do not in general have a tangent plane, and so

$$\frac{\partial h}{\partial x_9} = \frac{\partial h}{\partial x_{10}} = \frac{\partial h}{\partial x_{11}} = 0,$$

where  $h$  denotes the previously given function yielding the 4-fold cover. Let  $\mathcal{H}$  be the following ideal in  $\mathbb{C}[x_1, \dots, x_{14}]$ ,

$$\mathcal{H} = \left\langle h, \frac{\partial h}{\partial x_9}, \frac{\partial h}{\partial x_{10}}, \frac{\partial h}{\partial x_{11}} \right\rangle.$$

The ideal  $\mathcal{H}$  effectively allows us to find where the gradient of  $h$  is zero, which in turn allows us to locate points where two or more sheets of the 4-fold cover intersect. Such points



constitute the branch set  $M$  of the 4-fold cover. Using MAGMA [1] we find a Gröbner basis for  $\mathcal{H}$ . Selecting the final element of the basis calculated by MAGMA we can look at one subset of  $M$ .<sup>4</sup>

We factor the final basis element over the cyclotomic field  $\mathbb{Q}(\zeta_{42})$  where  $\zeta_{42}$  is a 42nd root of unity. (Note that 42 is 3 times 14. This was the smallest multiple of 14 for which  $h$  factored over the associated cyclotomic field). This gave three factors of degree 4 which we discuss in further detail below. We also have 30 quadratic factors of the form  $x_{11}^2 - \alpha^2$  where  $\alpha$  is a real number in  $\mathbb{Q}(\zeta_{42})$ . Hence each of these 30 quadratic factors will have two real roots (viz.  $x_{11} = \pm\alpha$ ). As  $h$  is never constant on  $x_{11}$ , this means that each of these quadratics in the basis of  $\mathcal{H}$  will only give us finitely many branch points. These points can be associated with tangential contact between two sheets of the 4-fold cover.

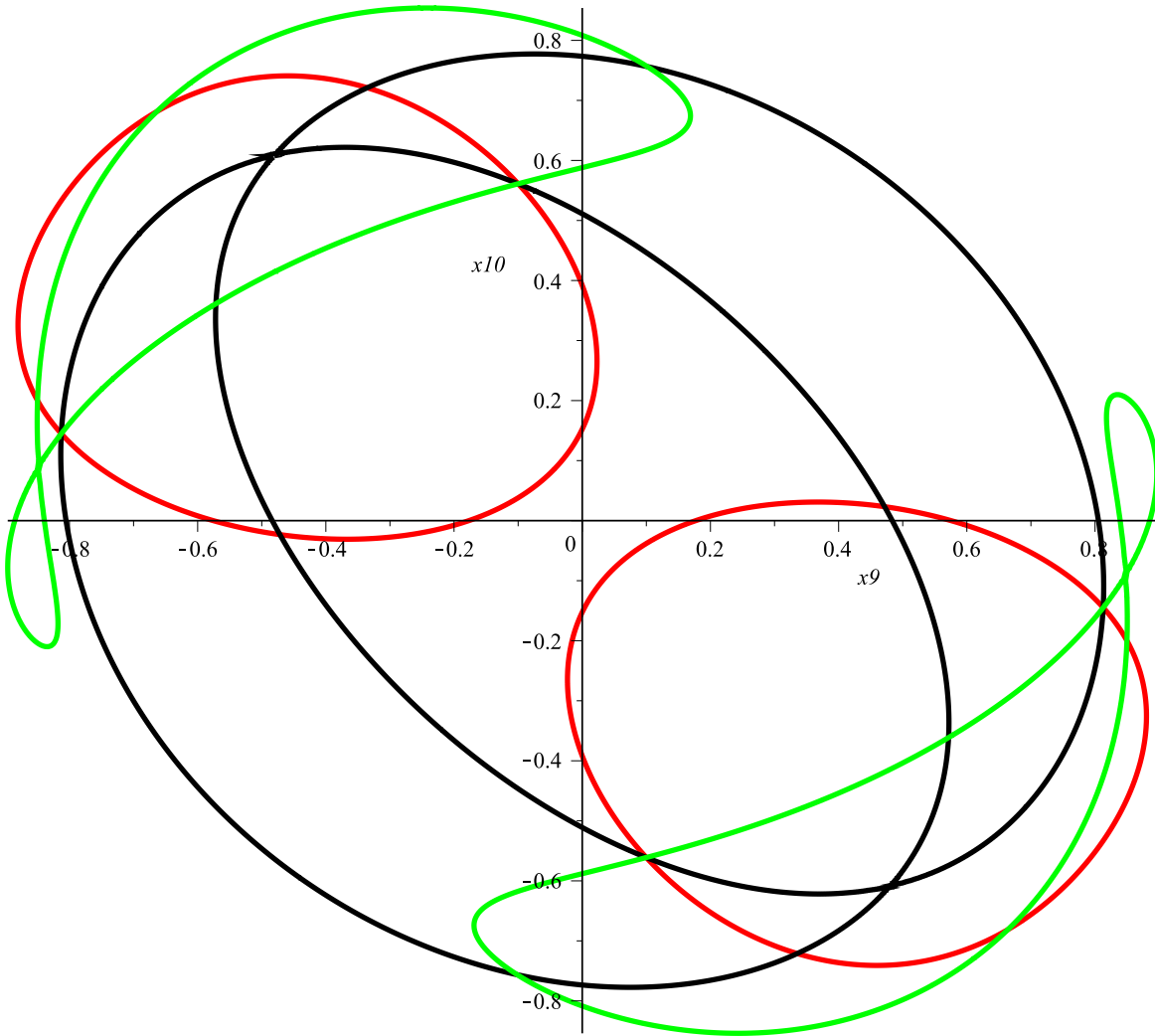
The quartic factors of the final basis element of  $\mathcal{H}$  give us a subset of  $M$ . Figures 5.7a, 5.7b, and 5.7c show the projections of this subset of  $M$  respectively onto the  $x_9x_{10}$ -,  $x_9x_{11}$ -, and  $x_{10}x_{11}$ -planes in 2-space.

---

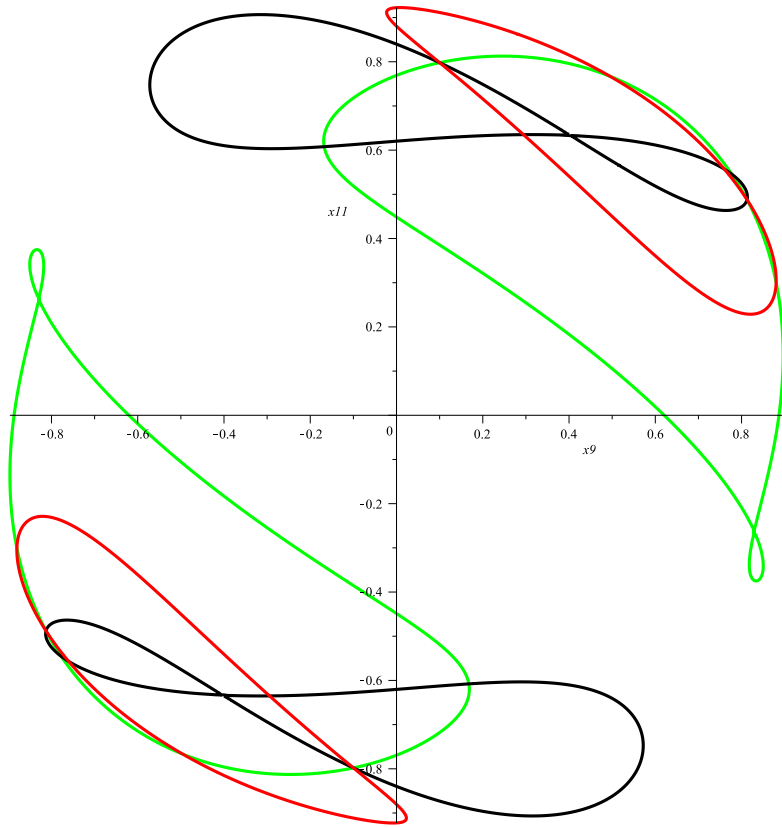
<sup>4</sup>For this specific example, MAGMA finds six basis elements. The sixth and final element was by far the simplest to work with from a computational standpoint. All other basis elements proved too computationally difficult to factor.

Figure 5.5: Projections of subset of branch points  $(x_9, x_{10}, x_{11})$

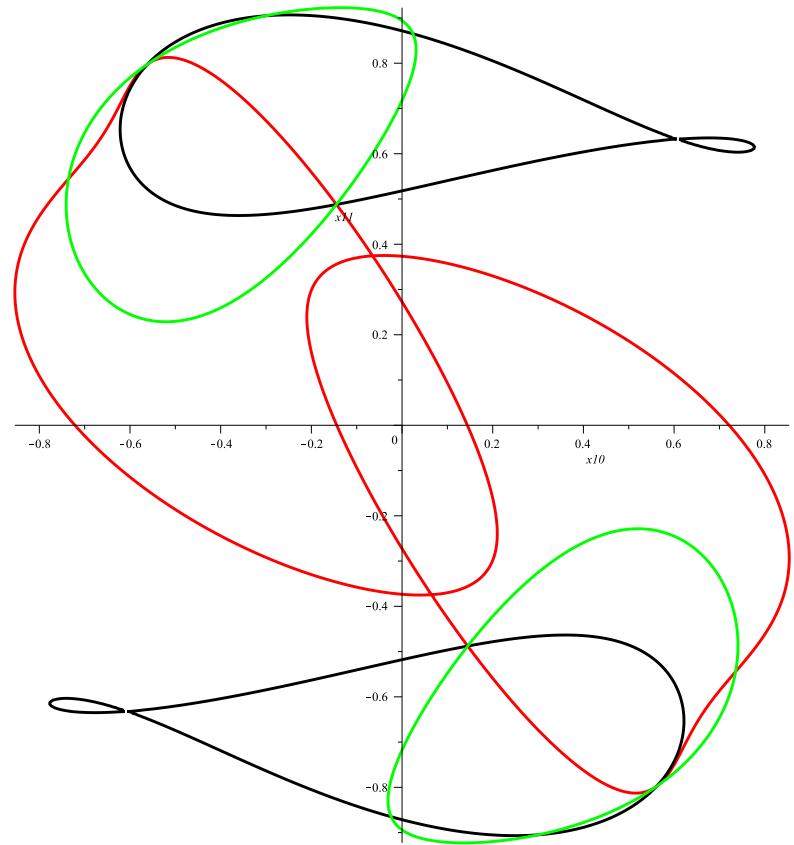
(a) Projection of a subset of  $M$  onto  $x_9x_{10}$  plane



(b) Projection of a subset of  $M$  onto  $x_9x_{11}$  plane



(c) Projection of a subset of  $M$  onto  $x_{10}x_{11}$  plane



As depicted in the above figures, this subset of  $M$  can actually be “factored” as the union of six distinct closed curves, each of the three quartics giving a symmetric pair of such curves. These pairs of curves are indicated by the red, green, and black curves in the figure. These colors are consistent across the images (i.e. green always corresponds to the same quartic, viewed in various projections). Although there are six distinct closed curves, when we refer to the “branch curves,” we are speaking of the three pairs of branch curves. Hence the red curves will be taken as one branch curve, the green pair of curves another branch curve, and the black pair of curves completing the count of branch curves.

One aspect of these projections that is of interest is what we term the *triple points*. We define a triple point to be a point in 3-space where all three of our branch curves intersect. Triple points are best viewed through the medium of the projections of the branch curves. Here we will specifically look at the  $x_{10}, x_{11}$  projection of the branch points for this space. Our aim is to determine where all three branch curves intersect at a single point. In order to do this, we construct an ideal in MAGMA whose generators are the three branch curves (i.e. the quartics generating such). Finding a Gröbner basis of this ideal yields two polynomials. The first of these polynomials is

$$x_{10} + \frac{340298005940}{5664298913}x_{11}^7 - \frac{104180396701}{2427556677}x_{11}^5 + \frac{587502029}{346793811}x_{11}^3 + \frac{75025487}{49541973}x_{11}.$$

The second of these two polynomials is a degree 8 polynomial over only the variable  $x_{11}$ :

$$x_{11}^8 - \frac{217861}{405385}x_{11}^6 - \frac{42336}{405385}x_{11}^4 + \frac{1372}{81077}x_{11}^2 + \frac{2401}{405385}.$$

Thus if we can find all real roots of this second polynomial, we can use the first polynomial to solve for corresponding values of  $x_{10}$ . Using Descartes’ Rule of Signs [32, p. 366], we can in fact find that this second polynomial has exactly four real roots, two positive and two negative. We use Maple to find these roots and obtain the following four points in  $x_9, x_{10}, x_{11}$

space. (The  $x_9$  slot will momentarily be left unfilled):

$$(\bullet, 0.5611253609, -0.7979665209); \quad (\bullet, 0.1447894706, -0.4878254662);$$

$$(\bullet, -0.1447894706, 0.4878254662); \quad (\bullet, -0.5611253609, 0.7979665209).$$

Performing a similar analysis with the  $x_9, x_{11}$  projection of the branch points, we obtain the  $x_9$  values for the four points given above. The four triple points of this space are as follows:

$$(-0.0999664959, 0.5611253609, -0.7979665209);$$

$$(-.8127227366, 0.1447894706, -0.4878254662);$$

$$(.8127227366, -0.1447894706, 0.4878254662);$$

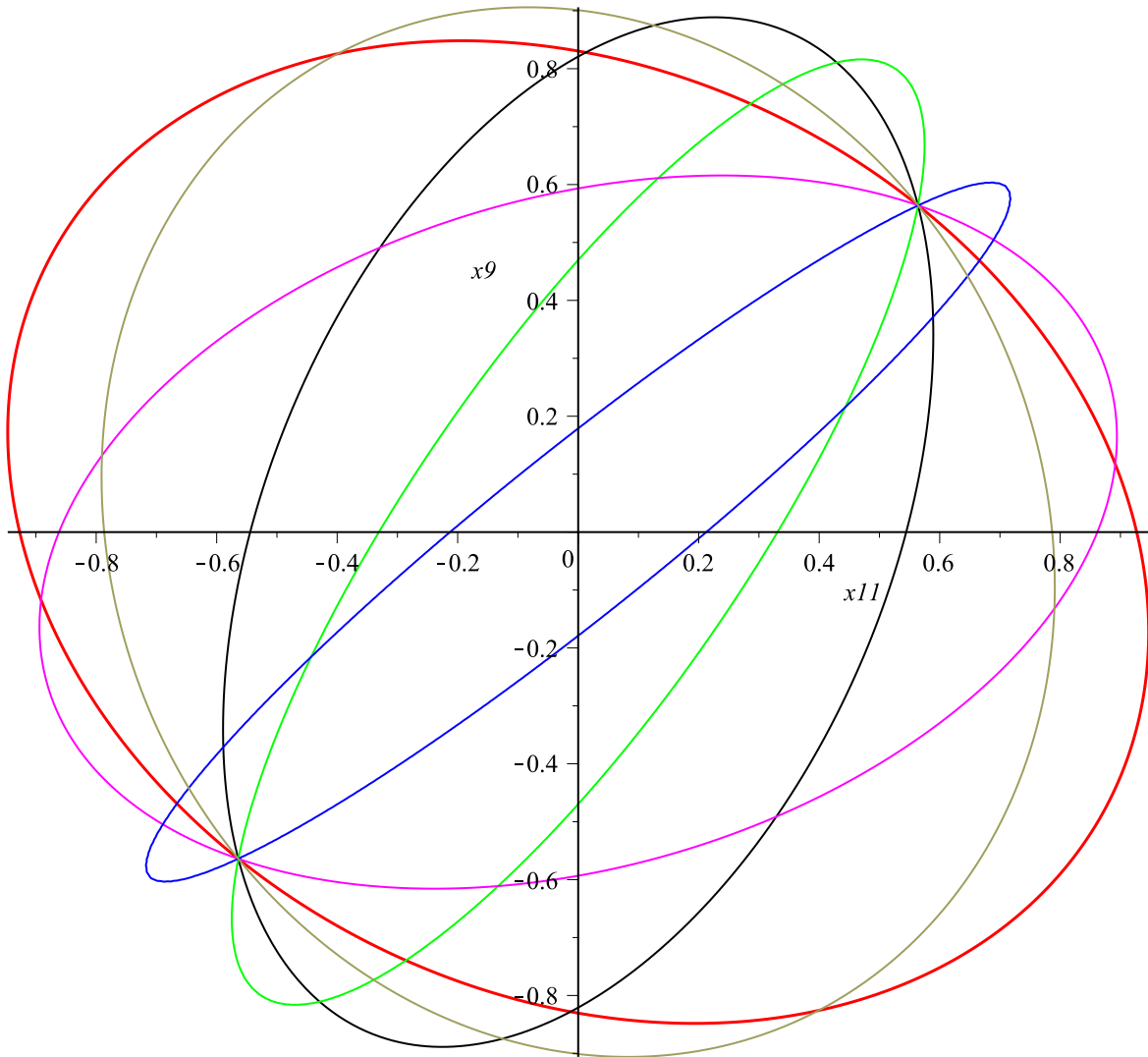
$$(0.0999664959, -0.5611253609, 0.7979665209).$$

These triple points can be visually confirmed by looking at the images of the projections of the branch points.

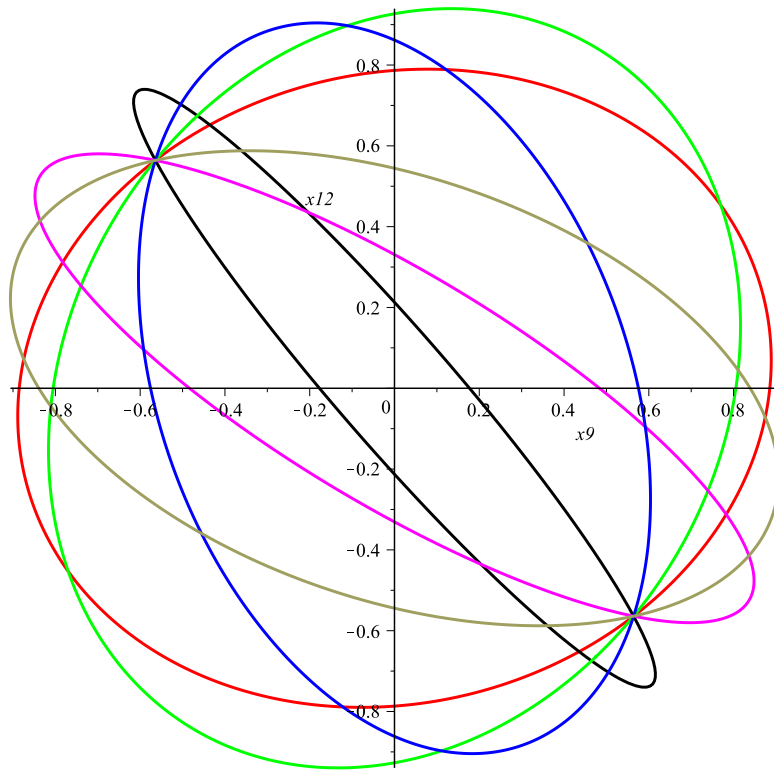
**Example.** We now examine a solution space to  $e^2 = 0$  whose associated branch curves all intersect at two points. In a process very similar to the one previously described for  $x_9, x_{10}$ , and  $x_{11}$  above, we can produce another 4-fold cover of the sphere that represents a solution space for  $e^2 = 0$  only over the variables  $x_9, x_{11}$ , and  $x_{12}$ . Three dimensional depictions of this space appear to be very similar to the 4-fold cover previously described. However, its set of branch points is intriguing in that instead of obtaining three quartics describing three pairs as we previously had, we now obtain six quadratics describing six individual curves. Furthermore, these six components all intersect at exactly two points. The projections of the branch curves onto the  $x_9x_{11}$ -,  $x_9x_{12}$ -, and  $x_{11}x_{12}$ -planes are as follows:

Figure 5.6: Projections of subset of branch points  $(x_9, x_{11}, x_{12})$

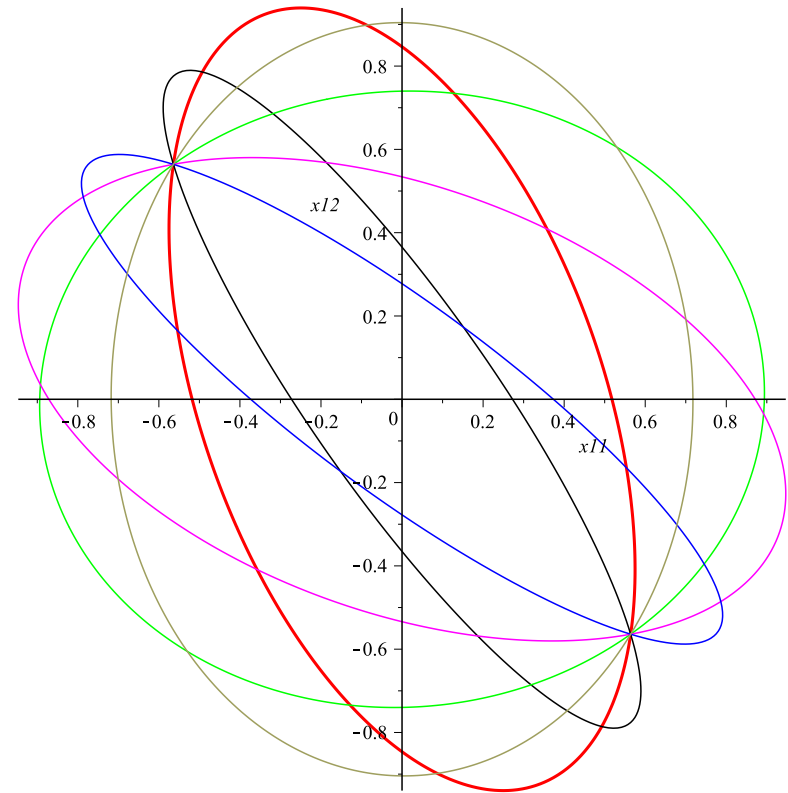
(a) Projection of a subset of branch points onto  $x_9x_{11}$  plane



(b) Projection of a subset of branch points onto  $x_9x_{12}$  plane



(c) Projection of a subset of branch points onto  $x_{11}x_{12}$  plane



Using an ideal in MAGMA as we did before, we can find the two points where these six curves intersect:

$$(\alpha, \alpha, -\alpha) \quad \text{and} \quad (-\alpha, -\alpha, \alpha) \quad \text{where} \quad \alpha = \sqrt{\frac{7}{22}}.$$

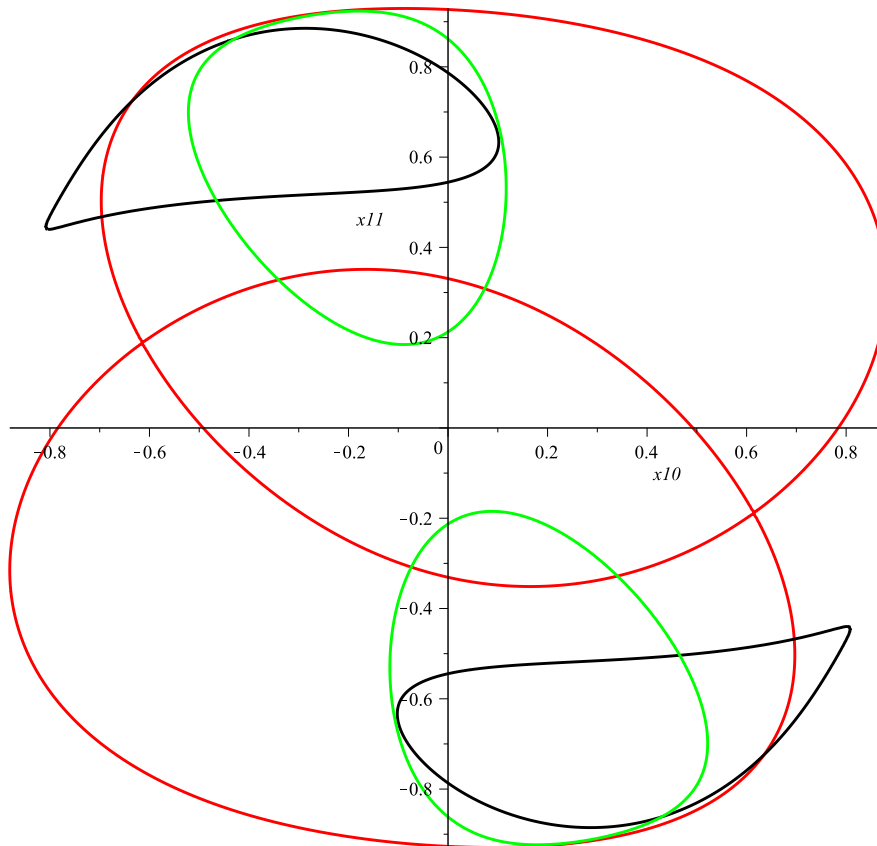
Once again, this can visually be confirmed.

**Example.** The final example that we will look at is the solution set to  $e^2 = 0$  over only the variables  $x_{10}, x_{11}$  and  $x_{12}$ . As with the previous two examples, this solution set is topologically a 4-fold cover. However, distinct from the other examples, the branch curves never intersect.

The projections of the branch curves are given below:

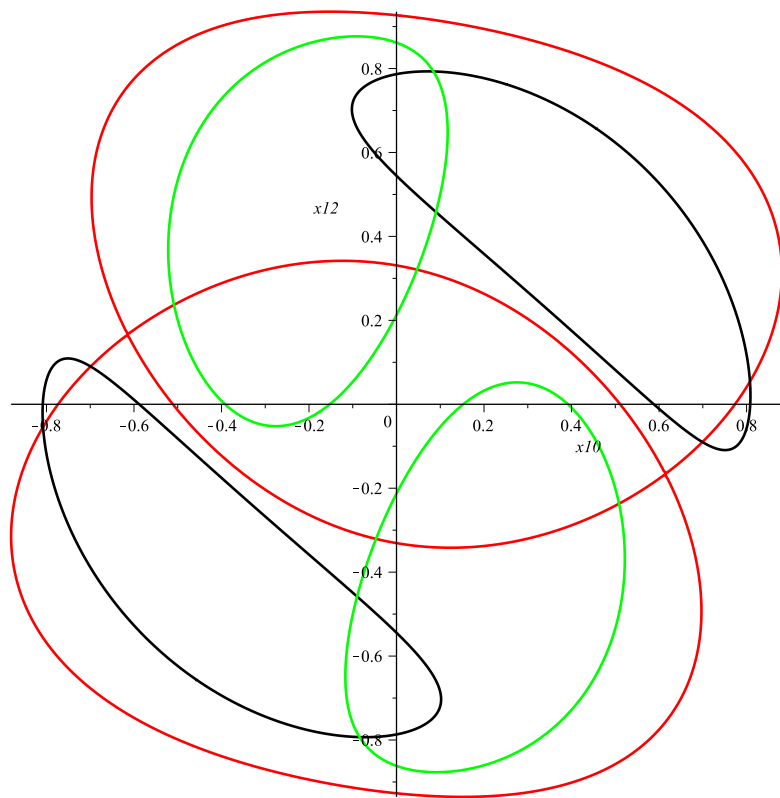
Figure 5.7: Projections of subset of branch points  $(x_{10}, x_{11}, x_{12})$

(a) Projection of a subset of branch points onto  $x_{10}x_{11}$  plane

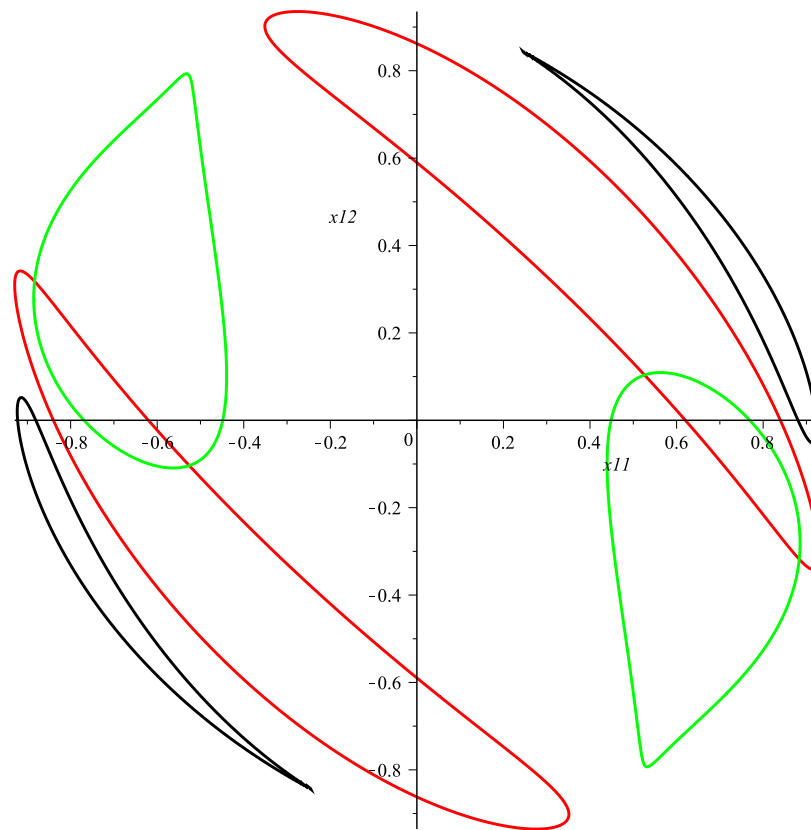




(b) Projection of a subset of branch points onto  $x_{10}x_{12}$  plane



(c) Projection of a subset of branch points onto  $x_{11}x_{12}$  plane



For every combination of three variables chosen from the higher index variables, we have examined the branch set for the associated space of solutions to  $e^2 = 0$  over only these three given variables. The branch sets can be classified into three categories, based on the intersection of their components. These results are summarized in the following table.

Table 5.3: Branch Curve types for  $D_{14}$

Branch Curve Intersections	Solutions to $e^2 = 0$ over $\{x_i, x_j, x_k\}$
Three Distinct Branch Curves with Four Triple Points	$(x_9, x_{10}, x_{11}), (x_9, x_{10}, x_{14})$ $(x_9, x_{13}, x_{14}), (x_{12}, x_{13}, x_{14})$
Six Distinct Branch Curves with Two Points in Common	$(x_9, x_{11}, x_{12}), (x_9, x_{12}, x_{13})$ $(x_{10}, x_{11}, x_{14}), (x_{11}, x_{12}, x_{14})$
Three Distinct Branch Curves with No Intersections	$(x_9, x_{10}, x_{12}), (x_9, x_{10}, x_{13})$ $(x_9, x_{11}, x_{13}), (x_9, x_{11}, x_{14})$ $(x_9, x_{12}, x_{14}), (x_{10}, x_{11}, x_{12})$ $(x_{10}, x_{11}, x_{13}), (x_{10}, x_{12}, x_{13})$ $(x_{10}, x_{12}, x_{14}), (x_{10}, x_{13}, x_{14})$ $(x_{11}, x_{12}, x_{13}), (x_{11}, x_{13}, x_{14})$

## CHAPTER 6. FURTHER QUESTIONS FOR FUTURE EXAMINATION

One question worth consideration was brought up in Section 3.1:

- While the converse of 3.1 does not hold in general, are there nevertheless classes of groups (e.g. Dihedral groups,  $p$ -groups, etc.) for which the conjecture does hold?

We can ask several questions pertaining to the admissible polynomials of  $\pi^{(k)}$  for  $k \geq 6$ :

- For every  $k \geq 6$  are there admissible polynomials which do not factor into linear terms over  $\mathbb{Z}$ ?
- Can we develop an algorithm for determining the number of distinct admissible polynomials for  $\pi^{(k)}$ ?
- In Chapter 3 we established that for  $k = 6$  there are admissible polynomials with irreducible (over  $\mathbb{Z}$ ) factors of degree 2. Are there values of  $k \geq 6$  for which there exists admissible polynomials with irreducible factors of degree strictly larger than 2?

Pertinent questions arise in relation to finding the solution space to  $e^2 = 0$  in Chapter 5:

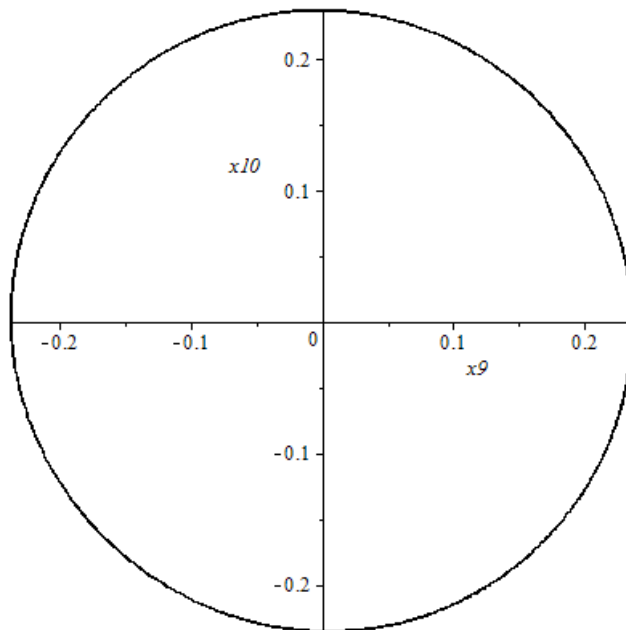
- While we intersect with a sphere to create a compact space containing solutions to  $e^2 = 0$ , what are the topological properties of the solution space itself? Is it connected? Is it open?
- The results that we present on solutions to  $e^2 = 0$  only represent a small fraction of all possible solutions. Further inquiries (viz. those resulting from factoring other basis elements for the branch set) may yield additional results. Computational limitations for  $D_{14}$  played a factor in obtaining a complete examination of the solution set to  $e^2 = 0$ .
- Computational shortcomings also prevented a sufficient examination for primes larger than  $q = 7$ . Further work could focus on developing results for larger primes.

APPENDIX A. CROSS SECTIONS OF 4-FOLD COVER OVER THE  
 VARIABLES  $x_9, x_{10}$ , AND  $x_{11}$

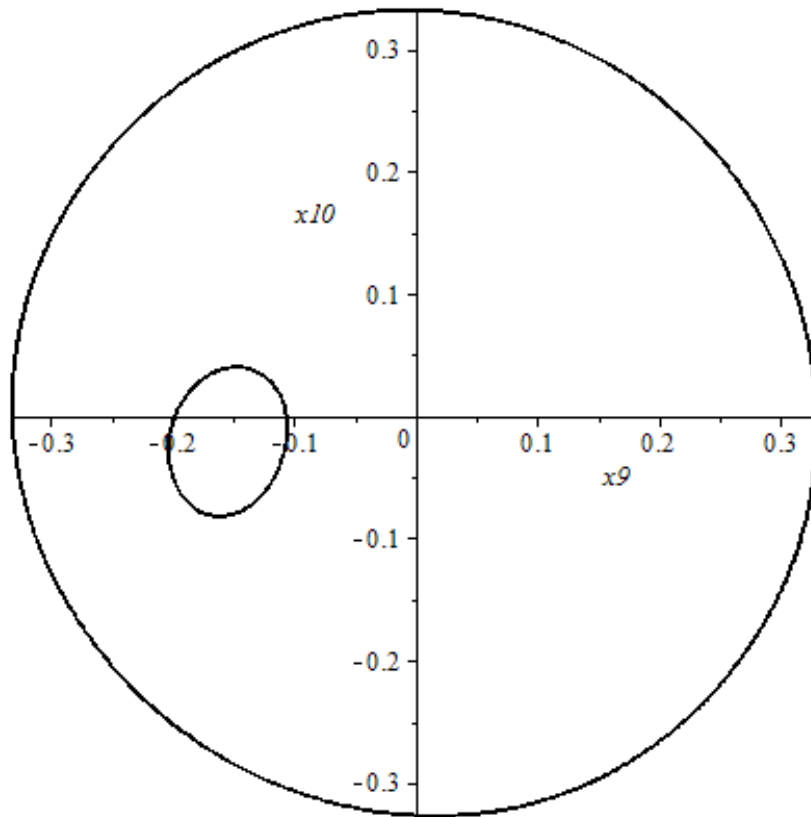
The following is a sequence of cross sections of the 4-fold cover discussed in Subsection 5.2.3.3. We take cross sections along the  $x_{11}$ -axis. There are 17 figures in all. The first figure begins with  $x_{11} = \frac{34}{35}$  and travels along the  $x_{11}$ -axis in decreasing increments of  $\frac{1}{35}$ , ending with  $x_{11} = \frac{18}{35}$ . This allows us to see cross sections of half of the 4-fold cover. Due to symmetry, the other half of the 4-fold cover will have cross sections that, when inverted, are identical to the ones depicted below. Because of the tangential nature of the intersection of some of the sheets of the cover, renderings of these cross sections will have fragmentation on some of the boundaries. This indicates that two distinct sheets are so close to one another that they cannot be properly rendered on any reasonable scale.

Figure A.1: Cross sections of 4-fold cover in  $x_9, x_{10}, x_{11}$

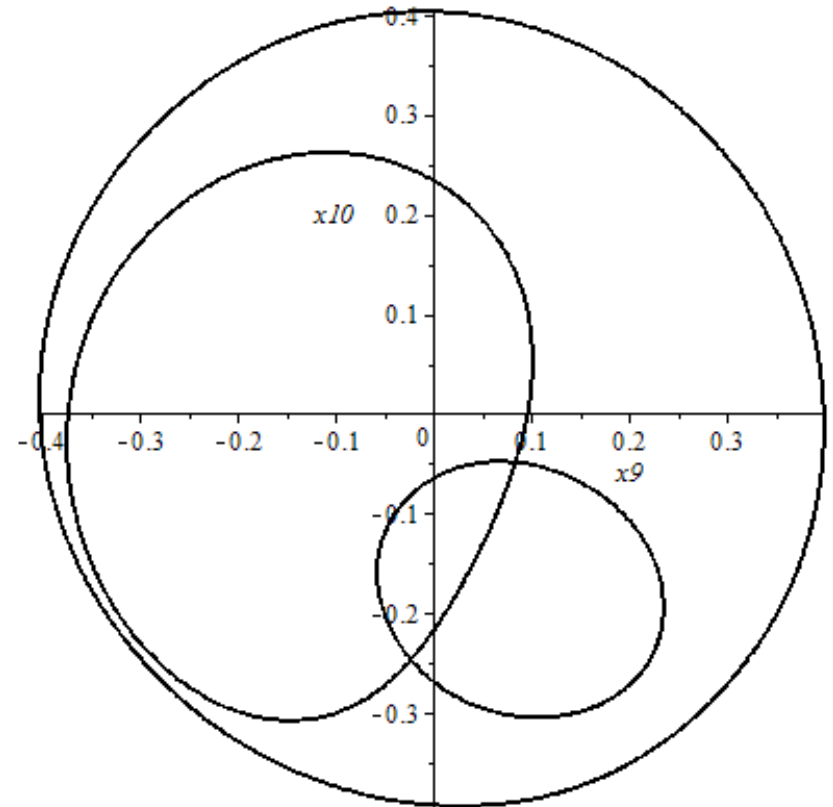
(a) Cross Section: 4-fold Cover of a 2-sphere (I)



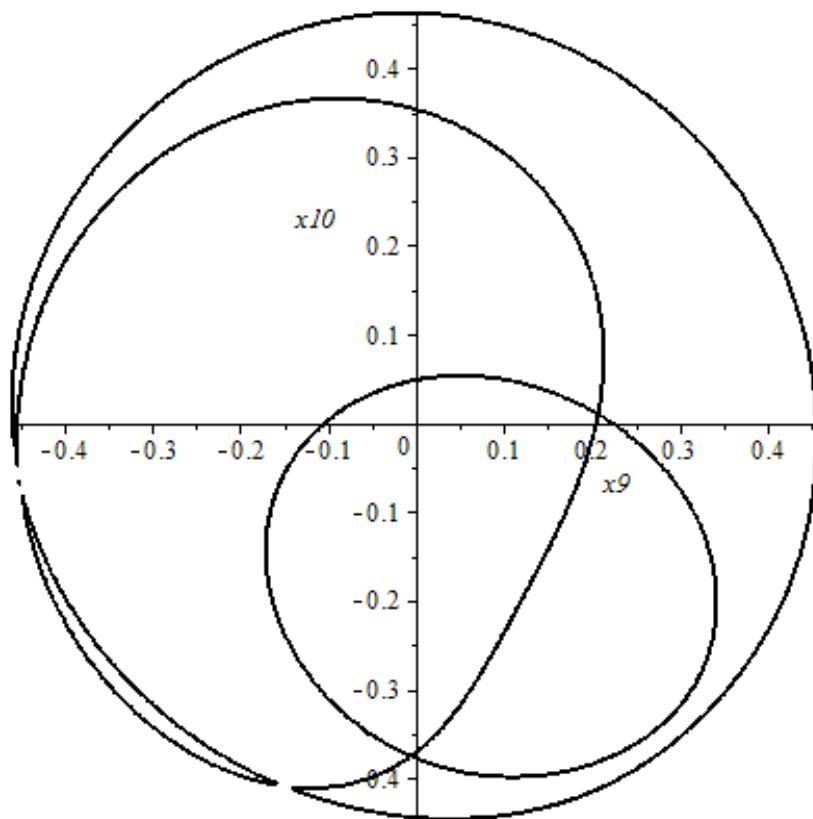
(b) Cross Section: 4-fold Cover of a 2-sphere (II)



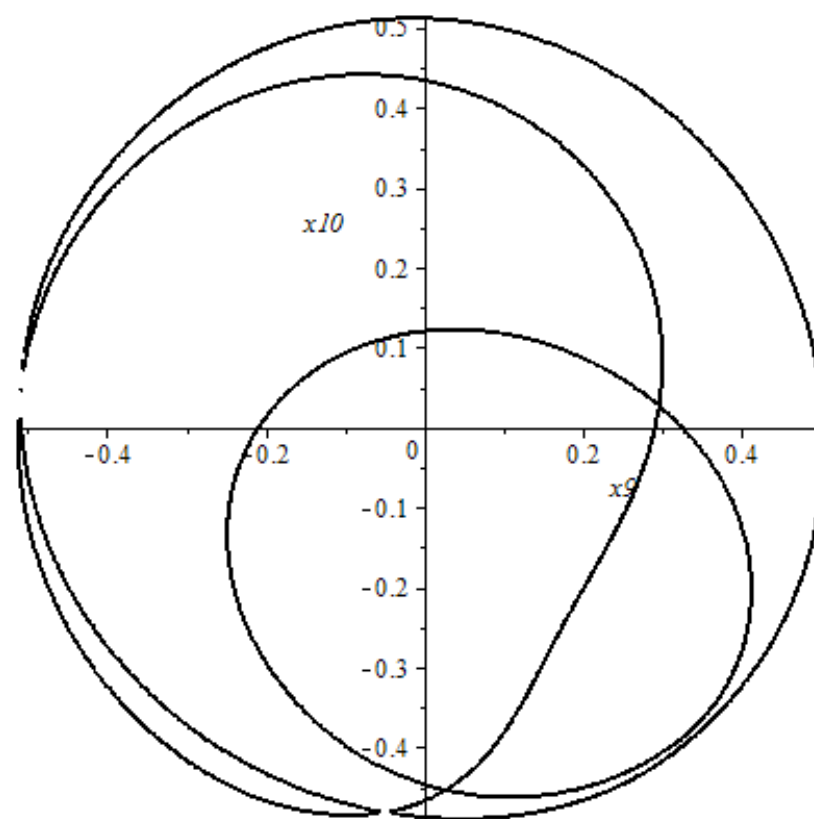
(c) Cross Section: 4-fold Cover of a 2-sphere (III)



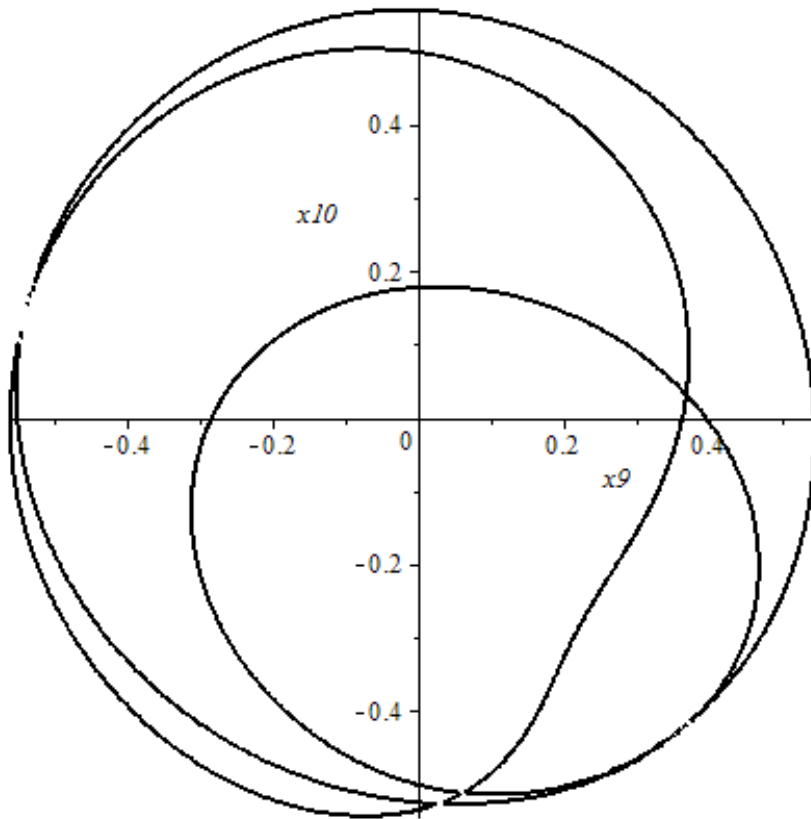
(d) Cross Section: 4-fold Cover of a 2-sphere (IV)



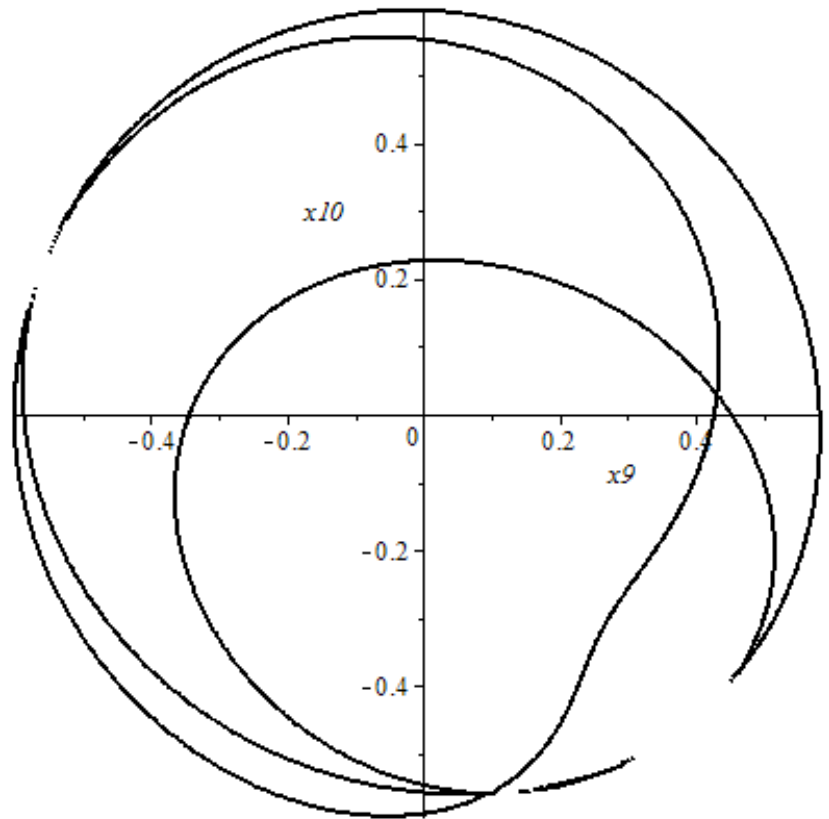
(e) Cross Section: 4-fold Cover of a 2-sphere (V)



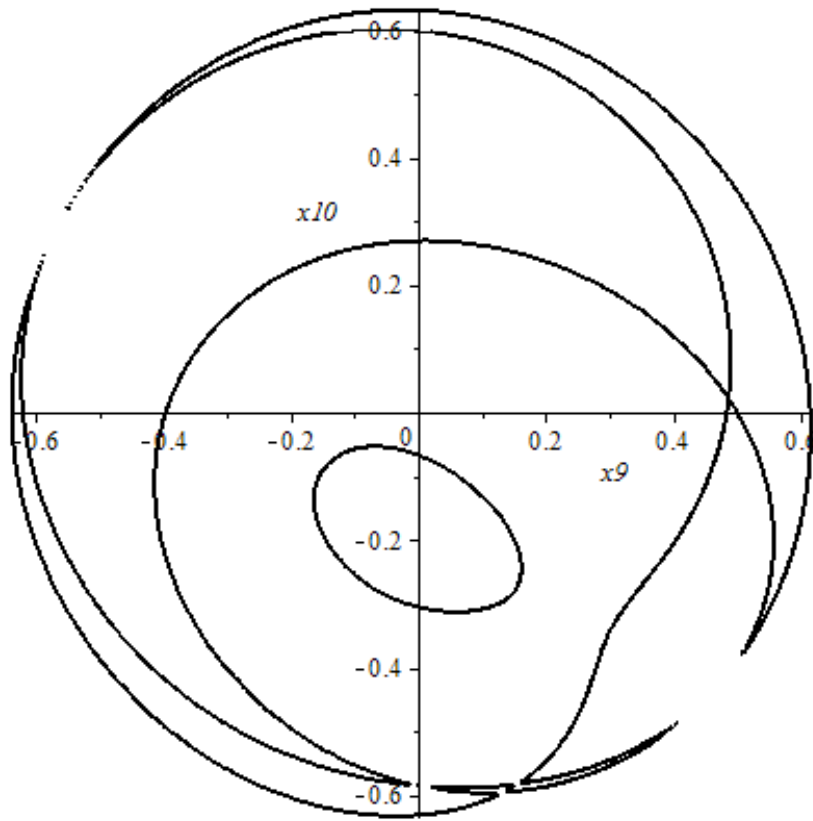
(f) Cross Section: 4-fold Cover of a 2-sphere (VI)



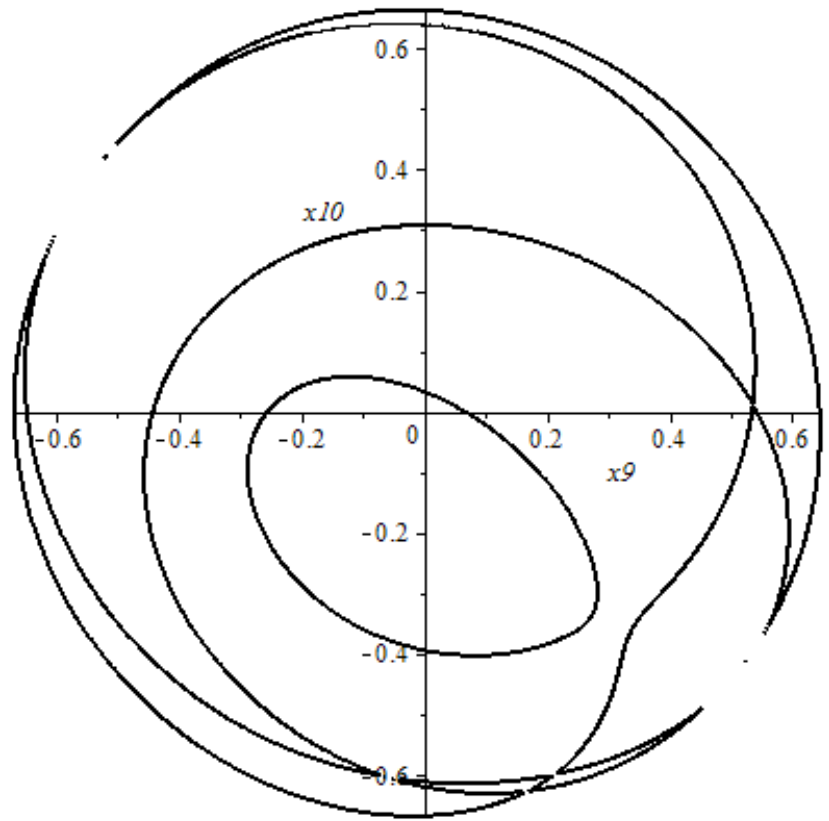
(g) Cross Section: 4-fold Cover of a 2-sphere (VII)



(h) Cross Section: 4-fold Cover of a 2-sphere (VIII)

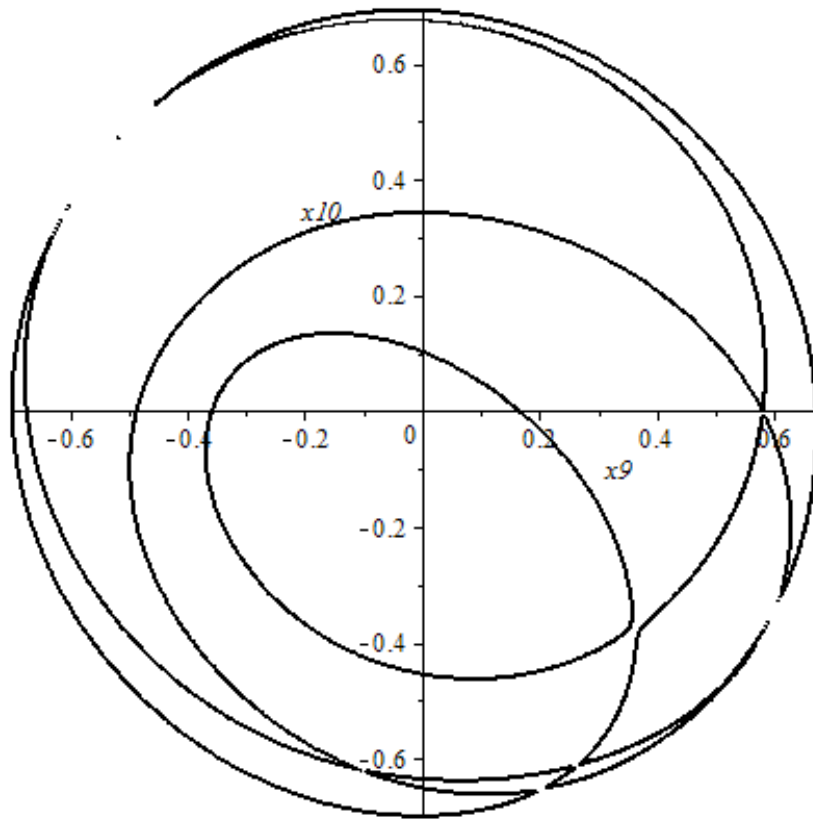


(i) Cross Section: 4-fold Cover of a 2-sphere (IX)

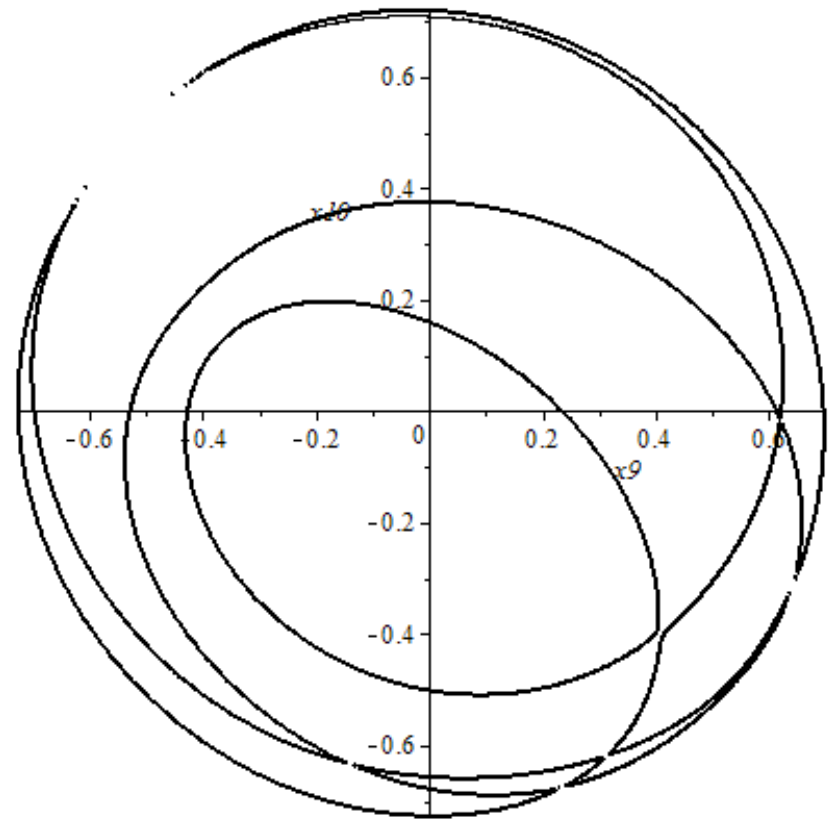




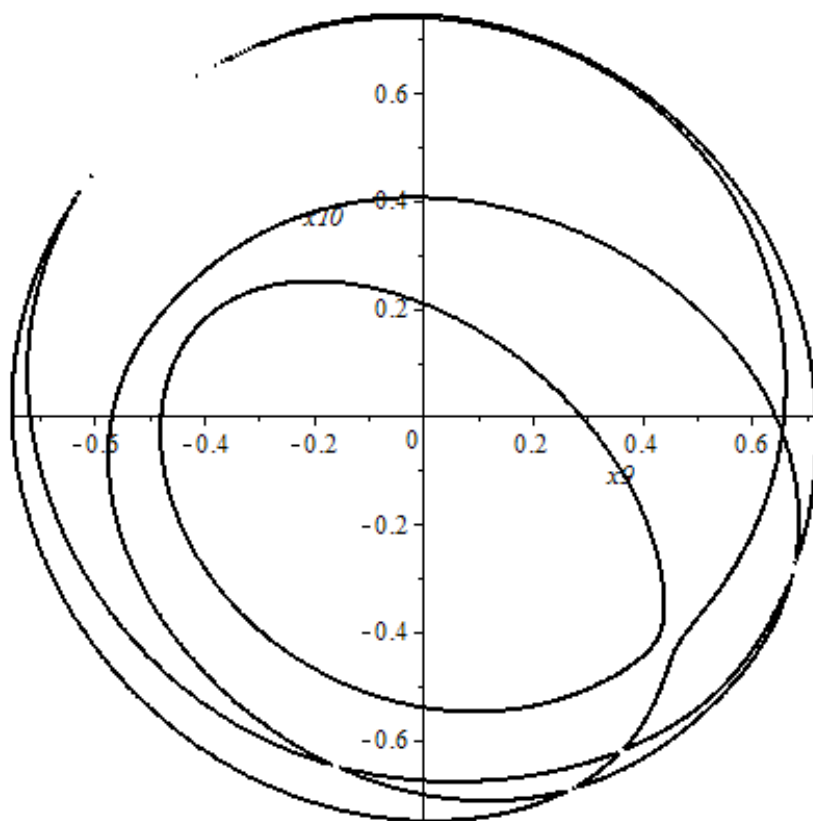
(j) Cross Section: 4-fold Cover of a 2-sphere (X)



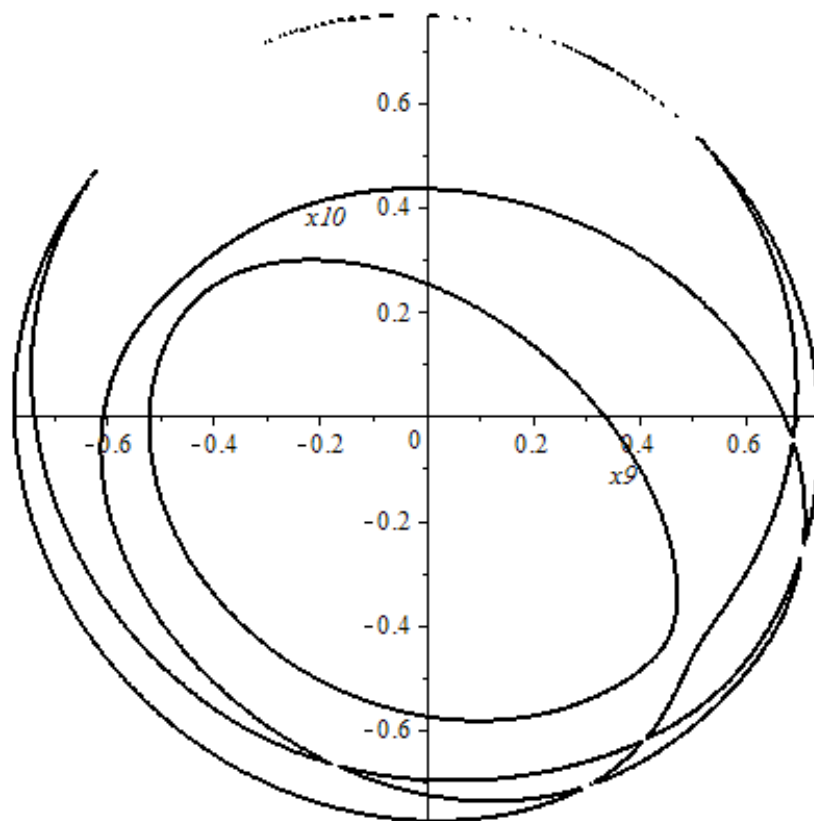
(k) Cross Section: 4-fold Cover of a 2-sphere (XI)



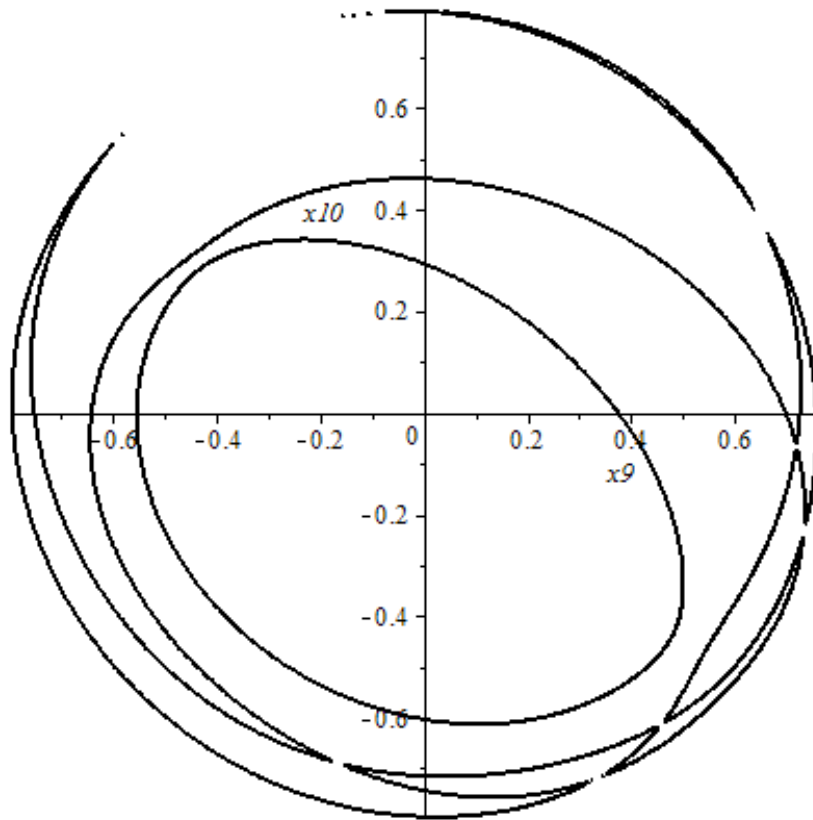
(l) Cross Section: 4-fold Cover of a 2-sphere (XII)



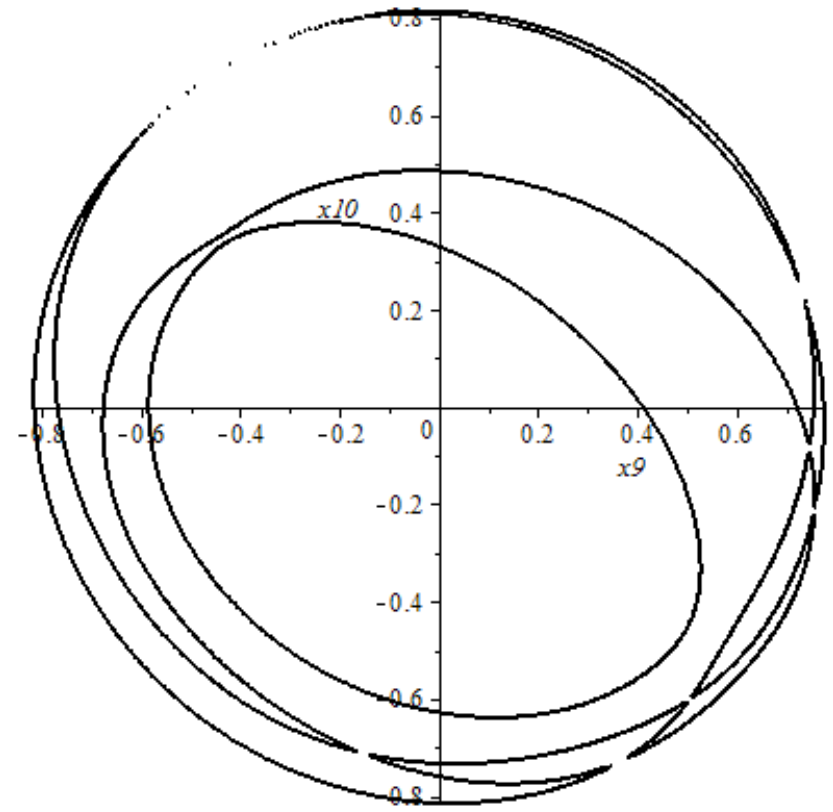
(m) Cross Section: 4-fold Cover of a 2-sphere (XIII)



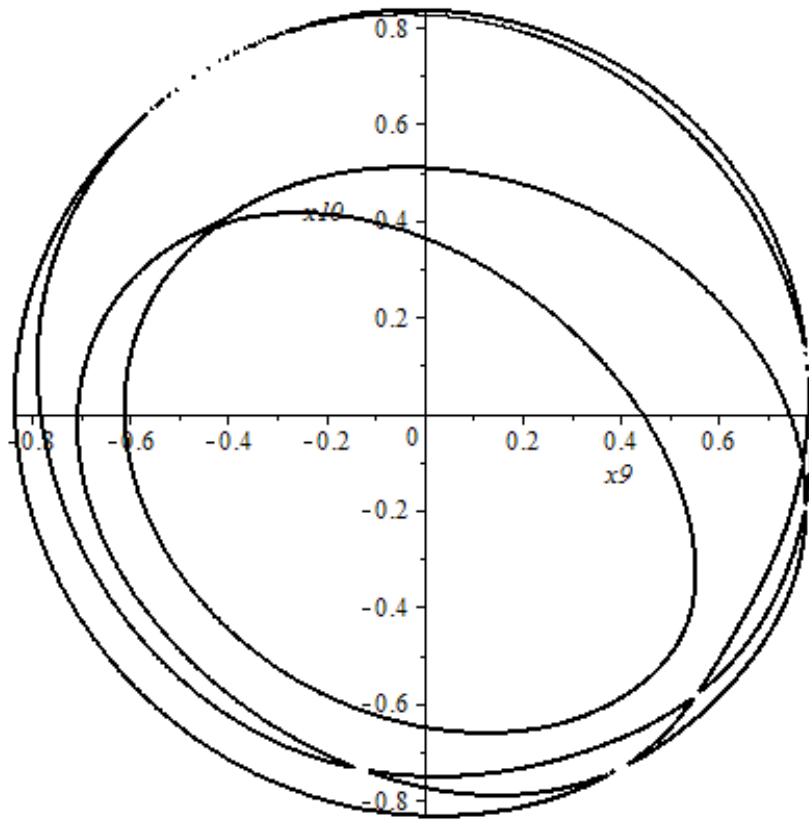
(n) Cross Section: 4-fold Cover of a 2-sphere (XIV)



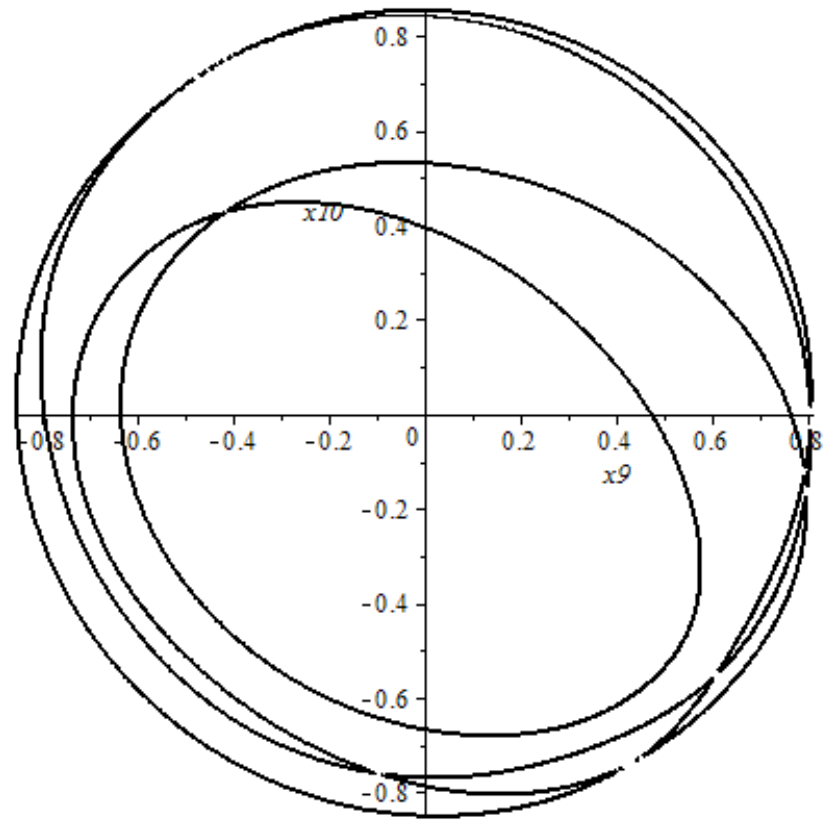
(o) Cross Section: 4-fold Cover of a 2-sphere (XV)



(p) Cross Section: 4-fold Cover of a 2-sphere (XVI)



(q) Cross Section: 4-fold Cover of a 2-sphere (XVII)



## APPENDIX B. MAGMA CODE

Here we provide the MAGMA[1] code used to perform the calculations included in this thesis:

### B.1 CODE FOR SOLVING $e^2 = 0$ IN $D_{2q}$

#### B.1.1 The case $q = 3$ .

```
g:=SmallGroup(6,1);
F:=RationalField();
P<x1,x2,x3,x4,x5,x6>:=PolynomialAlgebra(F,#g);
ga:=GroupAlgebra(P,g);
e:={P.i*ga.i:i in [1..#g]};
J:=ideal<P|Coefficients(e^2), x1, x2+x3, x4+x5+x6>;
Groebner(J);
```

#### B.1.2 The case $q = 5$ .

```
G:=SmallGroup(10,1);
F:=CyclotomicField(#G);
P<x1,x2,x3,x4,x5,x6,x7,x8,x9,x10>:=PolynomialAlgebra(F,#G);
ga:=GroupAlgebra(P,G);
e:={P.i*ga.i:i in [1..#G]};

eg:={x:x in G};
PH:=hom<P -> P| [0, -x5, -x4,x4,x5, -x7-x8-x9-x10,x7, x8, x9, x10]>;
co:=Coefficients(e^2);
co1:=PH(co);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);
co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);

co2:=Setseq(Set(co1));
co2:=Exclude(co2, 0);

C:=ideal<P|co2>;
Groebner(C);
bb:=Basis(C);

CS:=ideal<P|C,{P.i^2:i in {4..10} diff {6}}-1>;
Groebner(CS);
CS1:=ideal<P|CS, x10>;//Setting x10 to 0.
Groebner(CS1);
ee:=EliminationIdeal(CS1,{4,8,9});
//Other cases: x4810, x4910, x589, x5810, x5910, x478, x479, x4710, x578, x579, x5710.
//All the other cases produce bullfrogs of some fashion.
```

#### B.1.3 The case $q = 7$ .

```
G:=SmallGroup(14,1);
F:=CyclotomicField(#G);
P<x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12,x13,x14>:=PolynomialAlgebra(F,#G);
groupAlg:=GroupAlgebra(P,G);
```

```

e:={P.i*groupAlg.i:i in [1..#G]};

elementsG:={x:x in G};
Phom:=hom<P->P|[0,-x7,-x6,-x5,x5,x6,x7,-x9-x10-x11-x12-x13-x14,x9,x10,x11,x12,x13,x14]>;
//No x8.
co:=Coefficients(e^2);
co1:=Phom(co);
co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);

co2:=Setseq(Set(co1));
co2:=Exclude(co2, 0);

//This is the actual 4-fold cover code.
D:=ideal<P|co2,x14,x13,x12>;
//Set x14, x13, x12 to zero. Other cases would look at setting other variables to 0.
Groebner(D);
Elim791011:=EliminationIdeal(D,{7,9,10,11});//

E:=ideal<P|Elim791011,x7^2+x9^2+x10^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//Setting x11, x13, x14 to 0.
D:=ideal<P|co2,x14,x13,x11>;//Set x14, x13, x11 to zero.
Groebner(D);
Elim791012:=EliminationIdeal(D,{7,9,10,12});//

E:=ideal<P|Elim791012,x7^2+x9^2+x10^2+x12^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//Setting x14, x13, x10 to 0.
D:=ideal<P|co2,x14,x13,x10>;
Groebner(D);
Elim791112:=EliminationIdeal(D,{7,9,12,11});//

E:=ideal<P|Elim791112,x7^2+x9^2+x12^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//Setting x14, x13, x9 to 0.
D:=ideal<P|co2,x14,x13,x9>;
Groebner(D);
Elim7101112:=EliminationIdeal(D,{7,10,12,11});//

E:=ideal<P|Elim7101112,x7^2+x10^2+x12^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//Further cases can be considered similarly.

```

## B.2 CODE FOR FINDING BRANCH CURVE PROJECTIONS

The following code finds the branch curve projections for the solutions over the variables  $x_9$ ,  $x_{10}$ , and  $x_{11}$  to  $e^2 = 0$  when  $q = 7$ . The branch curve projections for other variable triples are found in the same way, the necessary changes being made.

```
G:=SmallGroup(14,1);
//F:=RationalField();
F<zz>:=CyclotomicField(3*#G);
P<x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12,x13,x14>:=PolynomialAlgebra(F,#G);
groupAlg:=GroupAlgebra(P,G);
e:=&+[P.i*groupAlg.i:i in [1..#G]];

elementsG:=[x:x in G];
Phom:=hom<P -> P| [0, -x7, -x6,-x5, x5,x6,x7,-x9-x10-x11-x12-x13-x14,x9, x10, x11, x12, x
13,x14]>;//No x8.
co:=Coefficients(e^2);
co1:=Phom(co);
co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);

co2:=Setseq(Set(co1));
co2:=Exclude(co2, 0);

//This is the actual 4-fold cover code.
D:=ideal<P|co2,x14,x13,x12>;
Groebner(D);
Elim791011:=EliminationIdeal(D,{7,9,10,11});//

E:=ideal<P|Elim791011,x7^2+x9^2+x10^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//The 10,11 case.
hh:=Basis(E)[2];
deriv9:=Derivative(hh,x9);
deriv10:=Derivative(hh,x10);
deriv11:=Derivative(hh,x11);
H:=ideal<P|deriv9,deriv10,deriv11,hh>;Groebner(H);
basisH:=Basis(H);
pr:=basisH[6];
factor6:=Factorization(pr);

Phom:=hom<P -> P| [0, -x7, -x6,-x5, x5,x6,x7,-x9-x10-x11-x12-x13-x14,x10, x9, x11, x12, x
13,x14]>;//No x8.
co:=Coefficients(e^2);
co1:=Phom(co);
co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);

co2:=Setseq(Set(co1));
co2:=Exclude(co2, 0);

D:=ideal<P|co2,x14,x13,x12>;
Groebner(D);
```

```

Elim791011:=EliminationIdeal(D,{7,9,10,11});//

E:=ideal<P|Elim791011,x7^2+x9^2+x10^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//The 9,11 case.
hh:=Basis(E)[2];
deriv9:=Derivative(hh,x9);
deriv10:=Derivative(hh,x10);
deriv11:=Derivative(hh,x11);
H:=ideal<P|deriv9,deriv10,deriv11,hh>;Groebner(H);//
basisH:=Basis(H);
pr:=basisH[6];//
factor6:=Factorization(pr);//

G:=SmallGroup(14,1);
//F:=RationalField();
F<zz>:=CyclotomicField(3*#G);
P<x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12,x13,x14>:=PolynomialAlgebra(F,#G);
groupAlg:=GroupAlgebra(P,G);
e:={P.i*groupAlg.i:i in [1..#G]};

elementsG:={x:x in G};
Phom:=hom<P -> P| [0, -x7, -x6,-x5, x5,x6,x7,-x9-x10-x11-x12-x13-x14,x11, x10, x9, x12, x
13,x14]>;//No x8.
co:=Coefficients(e^2);
co1:=Phom(co);
co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);co1:=Exclude(co1, 0);

co2:=Setseq(Set(co1));
co2:=Exclude(co2, 0);

D:=ideal<P|co2,x14,x13,x12>;//Set x14, x13, x12 to zero. Other cases would look at
setting other variables to 0.
Groebner(D);
Elim791011:=EliminationIdeal(D,{7,9,10,11});//

E:=ideal<P|Elim791011,x7^2+x9^2+x10^2+x11^2-1>;
Groebner(E);
hh:=Basis(E)[2];

//The 9,10 case.
hh:=Basis(E)[2];
deriv9:=Derivative(hh,x9);
deriv10:=Derivative(hh,x10);
deriv11:=Derivative(hh,x11);
H:=ideal<P|deriv9,deriv10,deriv11,hh>;Groebner(H);
basisH:=Basis(H);
pr:=basisH[6];//
factor6:=Factorization(pr);

```



## BIBLIOGRAPHY

- [1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
- [2] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli. *Representation Theory of the Symmetric Groups*. Number 121 in Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2010.
- [3] Keith Conrad. The origin of representation theory. *Enseign. Math. (2)*, 44(3-4):361–392, 1998.
- [4] David A. Cox. *Galois Theory*. John Wiley & Sons, 2nd edition, 2012.
- [5] Charles W. Curtis. *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Baruer*, volume 15 of *History of Mathematics*. American Mathematical Society, 1999.
- [6] Richard Dedekind. *Gesammelte mathematische Werke*, volume II. Chelsea Publishing Company, 1969. From original correspondence between D. and F.G. Frobenius, 1896.
- [7] Persi Diaconis. *Group Representations in Probability and Statistics*, volume 11 of *Lecture Notes–Monograph Series*. Institute of Mathematical Statistics, 1988.
- [8] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3rd edition, 2004.
- [9] Pavel I. Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to Representation Theory*, volume 59 of *Student Mathematical Library*. American Mathematical Society, 2011.
- [10] Gerd Fischer. *Plane Algebraic Curves*, volume 15 of *Student Mathematical Library*. American Mathematical Society, 2001.
- [11] F.G. Frobenius. Über die primfactoren der gruppendedeterminante. *Sitzungsberichte der Preußischen Akademie der Wissenschaften zu Berlin*, pages 1343–1382, 1896.
- [12] F.G. Frobenius. Über gruppencharaktere. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, pages 985–1021, 1896.
- [13] F.G. Frobenius. Über vertauschbare matrizen. *Sitzungsberichte der Preußischen Akademie der Wissenschaften zu Berlin*, pages 705–718, 1896.
- [14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.6*, 2014.
- [15] Andrew S. Greenhalgh. A model for random random-walks on finite groups. *Combinatorics, Probability and Computing*, 6:49–56, 1997.
- [16] Johnathan L. Gross and Jay Yellen. *Graph Theory and its Applications*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2nd edition, 2006.

- [17] Larry C. Grove. *Groups and Characters*. John Wiley & Sons, Inc., 1997.
- [18] Thomas Hawkins. The origins of the theory of group characters. *Archive for History of Exact Sciences*, 7(2):pp. 142–170, 1971.
- [19] Michiel Hazewinkel (ed.). Character group. In *Encyclopaedia of Mathematics*, pages 100–101. Kluwer Academic Publishers, 1988.
- [20] Martin Hildebrand. A survey of results on random random-walks on finite groups. *Probability Surveys*, 2:33–63, 2005.
- [21] Hans-Jürgen Hoehnke and Kenneth W. Johnson. The 1-, 2-, and 3-characters determine a group. *Bulletin (New Series) of the American Mathematical Society*, 27(2):243–245, 1992.
- [22] Hans-Jürgen Hoehnke and Kenneth W. Johnson. *3-Characters are sufficient for the group determinant*, volume 184 of *Contemporary Mathematics*. American Mathematical Society, 1995. Proceedings from the Second International Conference on Algebra, August 20-25, 1991.
- [23] Stephen P. Humphries. Generalized cogrowth series, random walks, and the group determinant. Preprint (2012).
- [24] I. Martin Isaacs. *Character Theory of Finite Groups*. AMS Chelsea Publishing Series. AMS Chelsea Pub., 1976.
- [25] Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, Cambridge, 3rd edition, 2001.
- [26] Kenneth W. Johnson. On the group determinant. *Math. Proc. Camb. Phil. Soc.*, 109:299–311, 1991.
- [27] Kenneth W. Johnson. Old and new developments in group matrices. In *Slides: Groups St. Andrews 2013*, August 2013.
- [28] Kenneth W. Johnson and Surinder K. Sehgal. The 2-character table does not determine a group. *Proceedings of the American Mathematical Society*, 119(4):pp. 1021–1027, 1993.
- [29] Kenneth W. Johnson and Surinder K. Sehgal. The 2-characters of a group and the group determinant. *Eurp. J. of Combinatorics*, 16:623–631, 1995.
- [30] Pierre-Guy Plamondon. Personal communication (2015-05-11).
- [31] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Number 42 in Graduate Texts in Mathematics. Springer, 1977.
- [32] Michael Sullivan. *College Algebra*. Prentice-Hall Inc., 7th edition, 2005.
- [33] A.L. Vyshnevetskiy and E.M. Zhmud'. Random walks on finite groups converging after finite number of steps. *Algebra and Discrete Mathematics*, (2):123–129, 2008.