Invariants of Modular Two-Row Groups

by

Yinglin Wu

A thesis submitted to the
Department of Mathematics and Statistics
in conformity with the requirements for
the degree of Doctor of Philosophy

Queen’s University
Kingston, Ontario, Canada
September 2009

Copyright © Yinglin Wu, 2009
Abstract

It is known that the ring of invariants of any two-row group is Cohen-Macaulay. This result inspired the conjecture that the ring of invariants of any two-row group is a complete intersection. In this thesis, we study this conjecture in the case where the ground field is the prime field \( \mathbb{F}_p \). We prove that all Abelian reflection two-row \( p \)-groups have complete intersection invariant rings. We show that all two-row groups with non-normal Sylow \( p \)-subgroups have polynomial invariant rings. We also show that reflection two-row groups with normal reflection Sylow \( p \)-subgroups have polynomial invariant rings. As an interesting application of a theorem of Nakajima about hypersurface invariant rings, we rework a classical result which says that the invariant rings of subgroups of \( \text{SL}(2, p) \) are all hypersurfaces.

In addition, we obtain a result that characterizes Nakajima \( p \)-groups in characteristic \( p \), namely, if the invariant ring is generated by norms, then the group is a Nakajima \( p \)-group.
Acknowledgments

I would like to thank both of my supervisors Professor Ian Hughes and Professor David Wehlau, whose expertise, understanding, patience, and support, added considerably to my graduate experience. I specially would like to thank Professor Ian Hughes for helping me select this thesis topic and guiding me through the whole research presented in this thesis. I would also like to thank Professor David Wehlau for many interesting and inspiring discussions, for generous support for years, and for devoting a lot time helping me edit my thesis. Finally, I together with my families would like to take this opportunity to show our eternal gratitude to my supervisors for their generous donations to my mother’s medical treatment.

A very special thanks goes out to my previous supervisor Professor Eddy Campbell for his inspiring year-long learning seminar on invariant theory, his support, and his encouragement.

I would also like to thank Ms. Jennifer Read for her great assistance and many valuable suggestions.
Lastly, I thank my parents, my wife and my wife’s family for love, support and patience, and thank my little daughter Jinfei for bringing me laughter everyday.
Statement of Originality

I hereby declare that the results in this thesis, unless accompanied by specific references, are original and have not been published elsewhere.

Yinglin Wu
# Table of Contents

Abstract i

Acknowledgments ii

Statement of Originality iv

Table of Contents v

Chapter 1:

**Introduction** ......................... 1

1.1 Algebraic Structures of Invariant Rings ......................... 3

1.2 $k$-Row Groups and Their Kernels .......................... 6

1.3 What is this Thesis about .................................. 8

Chapter 2:

**Literature Review** ........................ 10
Chapter 3:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Complete Intersections Adjoining an Extra Element</td>
<td>13</td>
</tr>
<tr>
<td>3.2</td>
<td>Abelian Reflection Two-Row $p$-groups</td>
<td>15</td>
</tr>
</tbody>
</table>

Chapter 4:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Abelian Reflection Two-Row $p$-groups with Specific Normalizers</td>
<td>22</td>
</tr>
<tr>
<td>4.2</td>
<td>Two-Row Groups with Non-normal Sylow $p$-Subgroups</td>
<td>30</td>
</tr>
<tr>
<td>4.3</td>
<td>Two-Row Groups with a Normal Sylow $p$-Subgroup</td>
<td>35</td>
</tr>
</tbody>
</table>

Chapter 5:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>A Theorem of Nakajima</td>
<td>40</td>
</tr>
<tr>
<td>5.2</td>
<td>Subgroups of $\text{SL}(2, p)$</td>
<td>41</td>
</tr>
<tr>
<td>5.3</td>
<td>A Counterexample</td>
<td>45</td>
</tr>
</tbody>
</table>

Chapter 6:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Concluding Remarks</td>
<td>46</td>
</tr>
</tbody>
</table>

Bibliography                                           | 48   |
Appendix A:

Characterizing Nakajima $p$-groups . . . . . . . . . . 52
Chapter 1

Introduction

Let $V$ be an $n$-dimensional vector space over an arbitrary field $\mathbb{F}$, $\text{GL}(V)$ the group of invertible linear transformations of $V$, and $S(V)$ the symmetric algebra on $V$. Given a basis of $V$, say $\{x_1, \ldots, x_n\}$, the symmetric algebra $S(V)$ can be identified with the polynomial algebra over $\mathbb{F}$ in $x_1, \ldots, x_n$. Thus the linear transformations in $\text{GL}(V)$ can be naturally regarded as $\mathbb{F}$-algebra automorphisms of $S(V)$ which preserve degree.

Let $G$ be a finite subgroup of $\text{GL}(V)$, we denote by $S(V)^G$ the set of elements of $S(V)$ left fixed by every element of $G$, which is called the ring of invariants of $G$, or the invariant ring of $G$. This is the object of study of the invariant theory of finite groups. Here is a simple example.

Example. Let $\mathbb{C}$ be the complex numbers, and $V = \mathbb{C}^2$ with a basis $\{x_1, x_2\}$. Let
CHAPTER 1. INTRODUCTION

$G$ be a subgroup of $\text{GL}(V)$ given by

$$G = \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle.$$  

Then ring of invariants $S(V)^G = \mathbb{C}[x_1^2, x_2^3]$.

In general, the invariant ring $S(V)^G$ has many nice properties. Perhaps the most important one, due to Hilbert and Noether, is that $S(V)^G$ is a finitely generated $F$-algebra. It is also important to know that $S(V)$ is integral over $S(V)^G$, namely, every element of $S(V)$ satisfies a monic polynomial with coefficients in $S(V)^G$. We refer the reader to Neusel [23] for proofs of these properties.

It is important to note that the invariant theory of finite groups divides sharply between the non-modular case and the modular case. By the non-modular case we mean the case where the characteristic of the ground field does not divide the order of the finite group (we call such a group a non-modular group). By the modular case we mean the case where the characteristic of the ground field divides the order of the finite group (we call such a finite group a modular group). In general, the invariant theory of modular groups is not so well developed as that of non-modular groups.

There are several modern references available on invariant theory of finite groups, such as Benson [2], Campbell and Wehlau [6], Derksen and Kemper [9], Kane [17], Neusel and Smith [24], and Smith [28].
1.1 Algebraic Structures of Invariant Rings

One of the major interests in the invariant theory of finite groups lies in studying the relationship between the algebraic structure of the invariant ring $S(V)^G$ and properties of the finite linear group $G$. Here we discuss five important structures that rings of invariants might have, which form the following hierarchy:

- polynomial ring $\Rightarrow$ hypersurface $\Rightarrow$ complete intersection
- $\Rightarrow$ Gorenstein $\Rightarrow$ Cohen-Macaulay.

Recall that an element $g \in \text{GL}(V)$ is called a reflection (on $V$) if the subspace $(g - 1)V$ is one-dimensional. A reflection group is just a finite subgroup of $\text{GL}(V)$ which is generated by reflections. One of the most celebrated results about rings of invariants is the following.

**Theorem 1.1.1** (Shephard and Todd [27], Chevalley [7], Serre [26]). Let $G$ be a finite subgroup of $\text{GL}(V)$. If $S(V)^G$ is polynomial, then $G$ is a reflection group. Conversely, if $G$ is a non-modular reflection group, then $S(V)^G$ is polynomial.

This result does not answer the question of whether or not $S(V)^G$ is polynomial when $G$ is a modular reflection group. In fact, there are modular reflection $p$-groups whose invariant rings are not even Cohen-Macaulay (c.f. Campbell, Geramita, Hughes, Shank, and Wehlau [4]), whereas the invariant rings of all non-modular finite groups are Cohen-Macaulay (see Hochster and Eagan [13]). Recall that an $F$-algebra
is called **Cohen-Macaulay** if it is a finitely generated free module over a polynomial \( \mathbb{F} \)-subalgebra.

**Definition.** Assuming that the ground field \( \mathbb{F} \) is of positive characteristic \( p \), a \( p \)-subgroup \( G \) of \( \text{GL}(V) \) is called a **Nakajima \( p \)-group** (on \( V \)) if there is a basis \( \{x_1, \ldots, x_n\} \) of \( V \) such that under this basis \( G \) is upper triangular and such that \( G = G_1 \cdots G_n \), where each subgroup \( G_i := \{g \in G \mid gx_j = x_j \text{ for } j \neq i\} \). We sometimes refer to \( \{x_1, \ldots, x_n\} \) as a Nakajima basis and refer to \( G = G_1 \cdots G_n \) as a Nakajima decomposition.

Obviously Nakajima \( p \)-groups are modular reflection \( p \)-groups. But a reflection \( p \)-group may not be a Nakajima \( p \)-group. Here is an example.

**Example.** Let \( V \) be a 4-dimensional vector space over the prime field \( \mathbb{F}_p \). Let \( G \) be a subgroup of \( \text{GL}(V) \) given by

\[
G = \left\langle \begin{bmatrix} I_2 & 0 & 0 \\ 0 & I_{n-2} \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} I_2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & I_{n-2} \end{bmatrix}, \begin{bmatrix} I_2 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & I_{n-2} \end{bmatrix} \right\rangle.
\]

Now \( G \) is a reflection subgroup of order \( p^3 \) in the obvious Nakajima \( p \)-group of order \( p^4 \). By applying Theorem 4.4 and Corollary 4.5 of Campbell and Hughes [5], we see that the invariant ring of \( G \) is a hypersurface, but not a polynomial ring. So \( G \) is not a Nakajima \( p \)-group.

The following important result concerns Nakajima \( p \)-groups.
Theorem 1.1.2 (Nakajima [20]). Let $V$ be a finite-dimensional vector space over the prime field $\mathbb{F}_p$, and $G$ a $p$-subgroup of $\text{GL}(V)$. Then $G$ is a Nakajima $p$-group if and only if $S(V)^G$ is polynomial.

Unfortunately, this result stated above does not extend to other fields of characteristic $p$ as is shown by an example due to Stong (c.f. Neusel and Smith [24, Example 2, p. 164]). In contrast, we obtain a result which permits us to say this: Assume the ground field is of characteristic $p$. Then a $p$-subgroup of $\text{GL}(V)$ is a Nakajima $p$-group if and only if its ring of invariants is a polynomial algebra generated by norms. In fact, the sufficiency is well-known and not hard to see. We will prove the necessity in the Appendix of this thesis.

An invariant ring $S(V)^G$ is called a hypersurface algebra if it is generated as an $\mathbb{F}$-algebra by at most $\dim(V) + 1$ elements. Nakajima [21] made an extensive study of non-modular subgroups of $\text{GL}(V)$ whose rings of invariants are hypersurfaces. As for modular groups, Campbell and Hughes [5, Theorem 4.4] showed that rings of invariants of maximal proper subgroups of a Nakajima $p$-group over the prime field $\mathbb{F}_p$ are hypersurfaces. Later Broer [3] found that this result can be extended to the other fields of characteristic $p$.

Definition. A finitely generated graded algebra $A$ over a field $\mathbb{F}$ of Krull dimension $m$ is called a complete intersection if there is a polynomial algebra $B$ over $\mathbb{F}$ in $m + s$ indeterminates and a homogeneous ideal $I$ of $B$ generated by $s$ elements such
that $B/I \cong A$.

Recall that an non-identity element $g \in \text{GL}(V)$ is called a bireflection if the subspace $(g - 1)V$ is at most two-dimensional. A necessary condition on $G$ for $S(V)^G$ to be a complete intersection is given by the following result.

**Theorem 1.1.3 (Kac and Watanabe [16, Theorem A])**. If $S(V)^G$ is a complete intersection, then $G$ is generated by bireflections.

As for Gorenstein rings of invariants, we refer the reader to Bass [1] for the definition. For our application, we mention the following result.

**Theorem 1.1.4 (Watanabe [29, Theorem 1])**. Let $G$ be a non-modular subgroup of $\text{GL}(V)$ which contains no reflections. Then $S(V)^G$ is Gorenstein if and only if $G \subset \text{SL}(V)$.

### 1.2 $k$-Row Groups and Their Kernels

Given a finite subgroup $G$ of $\text{GL}(V)$, we define a subspace of $V$ by

$$V_G := \text{span}_F \{(g - 1)v \mid g \in G, v \in V\}.$$ 

If $V_G$ is $k$-dimensional, then we call $G$ a $k$-row group. By this definition, every subgroup of $\text{GL}(V)$ is a $k$-row group for some non-negative integer $k$. For each subgroup $G$ of $\text{GL}(V)$, we define a group homomorphism given by the restriction of
$G$ to $V_G$:

$$- : G \ni g \mapsto g|_{V_G} \in \text{GL}(V_G).$$

Obviously, the kernel of this homomorphism, denoted $K_G$, is the set of all the elements of $G$ which acts trivially on $V_G$. We sometimes refer to $K_G$ as the kernel of the group $G$. We note $K_G$ is a normal subgroup of $G$.

On the other hand, given a $k$-dimensional subspace $U$ of $V$, we may define two subgroups of $\text{GL}(V)$ as follows:

$$T(U) := \{ g \in \text{GL}(V) \mid (g - 1)V \subset U \},$$

$$E(U) := \{ g \in \text{GL}(V) \mid (g - 1)V \subset U \subset V^g \},$$

where $V^g$ is the set of elements of $V$ left fixed by an element $g \in G$. Since $V_{T(U)} = U = V_{E(U)}$, it follows that both $T(U)$ and $E(U)$ are $k$-row groups. In fact, $T(U)$ contains all the $k$-row subgroups $G$ of $\text{GL}(V)$ with $V_G = U$, and $E(U)$ contains all the $k$-row subgroups of $\text{GL}(V)$ which act trivially on $U$. Therefore we refer to $T(U)$ as the largest $k$-row subgroup of $\text{GL}(V)$ with respect to $U$, and $E(U)$ as the largest $k$-row subgroup of $\text{GL}(V)$ which acts trivially on $U$. We note that $E(U)$ is the kernel of $T(U)$, namely, $E(U) = K_{T(U)}$, and that the kernel of $E(U)$ is itself. Given a basis $X$ of $V$ which is enlarged from a basis of $U$, we may identify the $k$-row multiplicative group $E(U)$ with the additive group $M_{k \times (n - 2)}(\mathbb{F})$ via the following isomorphism:

$$t_X : E(U) \ni g \mapsto A \in M_{k \times (n - 2)}(\mathbb{F}),$$
CHAPTER 1. INTRODUCTION

where $A$ is the $2 \times (n - 2)$ matrix such that

$$[g]_X = \begin{bmatrix} I_k & A \\ 0 & I_{n-k} \end{bmatrix}_{n \times n}.$$ 

For $g \in E(U)$, we refer to $t_X(g)$ as the tail matrix of $g$ under $X$. Sometimes we write $t(g)$ for $t_X(g)$ when no confusion arises. By this identification, we see that $E(U)$ is Abelian.

Let $G$ be a $k$-row subgroup of $GL(V)$. Then $V_G$ is a $k$-dimensional subspace. It is routine to verify that $K_G = G \cap E(V_G)$. It follows that $K_G$ is elementary Abelian.

1.3 What is this Thesis about

When Bram Broer spoke in the Invariant Theory seminar at Queen’s University in 2005, he gave a proof of the result that the ring of invariants of an arbitrary two-row group is Cohen-Macaulay. This result had inspired the conjecture that the invariant ring of any two-row group is a complete intersection. I found this conjecture very interesting and decided that it would be my thesis topic.

In this thesis, we consider several cases where the conjecture holds and we find a counterexample showing that the conjecture does not hold for all non-modular groups.

In Chapter 3, we deal with two-row groups whose rings of invariants are complete intersections.
In Chapter 4, we deal with two-row groups whose rings of invariants are polynomial.

In Chapter 5, we give a direct simpler proof to the classical result which says the subgroups of $\text{SL}(2, p)$ all have hypersurface rings of invariants.

In Appendix, we prove a sufficient condition for Nakajima $p$-groups.
Chapter 2

Literature Review

Invariant rings of $k$-row groups, where $k$ is small, behave quite interestingly. Landweber and Stong [19] showed invariant rings of one-row groups are polynomial. It is known that invariant rings of two-row groups are Cohen-Macaulay (For a proof, see Campbell and Wehlau [6, Theorem 4.17]). As mentioned before, there are 3-row groups whose invariant rings are not Cohen-Macaulay ([4]). There are reflection 4-row groups whose invariant rings are not Cohen-Macaulay (c.f. Kemper [18]).

There is work showing some particular two-row groups are actually complete intersections. For example, Neusel [22] showed invariant rings of modular cyclic two-row groups of order a power of a prime are complete intersections.

In this thesis, we focus on the conjecture that invariant rings of two-row groups
are complete intersections. We show that invariant rings of Abelian reflection two-row $p$-groups are complete intersections. In the proof of this result, both Proposition 3.1 and Theorem 4.4 of Campbell and Hughes [5] play crucial roles. We also show a quite general result that invariant rings of two-row groups with non-normal Sylow $p$-subgroups are polynomial.

Nakajima $p$-groups play an important role in our study of two-row groups. The formal definition of a Nakajima $p$-group is given in Shank and Wehlau[23] inspired by the study in Nakajima[20], which gave an intensive study of such groups.

The main theorem in Nakajima[21] about hypersurfaces inspired the new proof for the classical result that subgroups of $\text{SL}(2, p)$ all have hypersurface rings of invariants.

The proof of Theorem 8.1 in Gorenstein [12] inspired the proof of Proposition 4.2.1 in this thesis.
Chapter 3

Complete Intersection Invariant Rings

Let $V$ be a finite-dimensional vector space over the prime field $\mathbb{F}_p$. In this chapter, we study those reflection two-row subgroups $G$ of $\text{GL}(V)$ which are equal to their kernels $K_G$. By a result due to Nakajima (c.f. Chuai [8, Proposition 5.1.1]), such two-row groups of $\text{GL}(V)$ are exactly those Abelian reflection two-row $p$-subgroups of $\text{GL}(V)$. We show that their invariant rings are complete intersections.
3.1 Complete Intersections Adjoining an Extra Element

The following result says, roughly speaking, that often adjoining an extra element to a complete intersection yields another complete intersection. This result is at the core of our proof of the main theorem of this chapter.

**Proposition 3.1.1.** Let $V$ be an $n$-dimensional vector space over a field $\mathbb{F}$ of positive characteristic $p$. Let $K$ be a finite $p$-subgroup of $\text{GL}(V)$, and $H$ a maximal proper subgroup of $K$ whose index in $K$ is $p$. If $S(V)^K$ is a complete intersection and $S(V)^H = S(V)^K[a]$ for some homogeneous element $a \in S(V)^H$, then $S(V)^H$ is a complete intersection.

**Proof.** By Galois Theory, we have

$$a^p + \omega_{p-1}a^{p-1} + \cdots + \omega_1a + \omega_0 = 0,$$

where each $\omega_i$ is an element of $S(V)^K$.

Since $S(V)^K$ is a complete intersection of Krull dimension $n$, it follows that there is a polynomial ring $R$ over $\mathbb{F}$ in $n + s$ indeterminates, and a homogeneous ideal $I$ of $R$ which is generated by $s$ homogeneous polynomials $f_1, \ldots, f_s$ in $R$, such that

$$R/I \cong S(V)^K,$$

where $\phi$ is an isomorphism.
This induces an epimorphism

\[ \Phi: R[X] \ni rX^k \mapsto \phi(r + I)a^k \in S(V)^K[a], \]

where \( R[X] \) is a polynomial ring over \( R \) in indeterminate \( X \) and \( r \in R \). Since we have

\[ R[X]/\ker(\Phi) \cong S(V)^K[a] = S(V)^H, \]

in order to show that \( S(V)^H \) is a complete intersection algebra, we only need to prove that \( \ker \Phi \) is generated by \( s + 1 \) homogeneous elements.

Since \( \Phi \) is epimorphic, for each \( \omega_i \) there exists an \( r_i \in R \) such that we have \( \Phi(r_i) = \omega_i \). Put

\[ f_{s+1} := X^p + r_{p-1}X^{p-1} + \cdots + r_1X + r_0. \]

We claim that

\[ \ker(\Phi) = (f_1, \ldots, f_s, f_{s+1})R[X]. \]

It is easily seen that \( \ker(\Phi) \supseteq (f_1, \ldots, f_s, f_{s+1})R[X] \). To show that the inverse inclusion holds, consider an element \( q \in R[X] \) such that \( \Phi(q) = 0 \). Note that \( f_{s+1} \) is a monic polynomial. It follows that \( q = hf_{s+1} + t \), where both \( h \) and \( t \) are some polynomials in \( R[X] \), and either \( t = 0 \) or \( t \) has degree strictly less than \( p \), the degree of \( f_{s+1} \). Write

\[ t = b_uX^u + \cdots + b_1X + b_0, \]
where \( u < p \), and each \( b_i \in R \). Since \( \Phi(t) = 0 \), we have

\[
\phi(b_u + I) a^u + \cdots + \phi(b_1 + I) a + \phi(b_0 + I) = 0.
\]

Since \( \{1, a, \ldots, a^{p-1}\} \) is a basis for the field extension \( Q(S(V)^H)/Q(S(V)^G) \), it follows that all \( \phi(b_i + I) = 0 \). Thus all \( b_i \in I \). This implies that \( t \in (f_1, \ldots, f_s) R[X] \).

Therefore \( q \in (f_1, \ldots, f_s, f_{s+1}) R[X] \). \( \Box \)

## 3.2 Abelian Reflection Two-Row \( p \)-groups

Let \( V \) be an \( n \)-dimensional vector space over the prime field \( \mathbb{F}_p \), where \( n \geq 2 \). As mentioned before, the reflection two-row subgroups \( G \) of \( \text{GL}(V) \) with \( G = K_G \) are exactly the Abelian reflection two-row \( p \)-subgroups of \( \text{GL}(V) \), and each such group \( G \) is a subgroup of \( E(V_G) \). So \( G \) can be identified with the additive group consisting of the tail matrices of elements of \( G \). We now show that their rings of invariants are complete intersections.

**Theorem 3.2.1.** Let \( G \) be an Abelian reflection two-row \( p \)-subgroup of \( \text{GL}(V) \). Then \( S(V)^G \) is a complete intersection.

**Proof.** By induction on \( n \). If \( n = 2 \), then \( G \) is the identity group, whose invariant ring is the polynomial algebra \( S(V) \) itself. We now assume \( n \geq 3 \).

Note that the tail matrix of any reflection in \( G \), under a given basis of \( V \) enlarged from a basis of \( V_G \), is of rank one, namely, its columns are pairwise linearly dependent.
Considering this, it is easily seen that there exists \( m \) reflections \( g_1', \ldots, g_m' \in G \) such that we can say the following:

1. For each \( i \in \{1, \ldots, m\} \), the \( i \)-th column of the tail matrix \( t(g_i') \) of \( g_i' \) is the only non-zero column of \( t(g_i') \), denoted \( \binom{\alpha_i}{\beta_i} \). To indicate this, we write \( t(g_i') = \begin{bmatrix} \binom{\alpha_i}{\beta_i} \\ \vdots \end{bmatrix} \).

2. For any other element in \( G \), the non-zero columns of its tail matrix only occur in the first \( m \) columns.

It follows that we may assume \( m = n - 2 \).

Consider the group generated by \( g_1', \ldots, g_{n-2}' \). If \( G = \langle g_1', \ldots, g_{n-2}' \rangle \), then clearly \( G \) is a Nakajima \( p \)-group, whose invariant ring is polynomial. We now proceed assuming \( G \neq \langle g_1', \ldots, g_{n-2}' \rangle \). Take an element \( g' \in G \setminus \langle g_1', \ldots, g_{n-2}' \rangle \), write

\[
t(g') = \begin{bmatrix} \binom{\eta_1}{\delta_1} \\ \vdots \\ \binom{\eta_{n-2}}{\delta_{n-2}} \end{bmatrix}.
\]

For the purpose of visualization, we arrange the \( n - 1 \) tail matrices obtained so far into the following picture:

\[
\begin{bmatrix}
\binom{\alpha_1}{\beta_1} \\
\vdots \\
\binom{\alpha_{n-2}}{\beta_{n-2}}
\end{bmatrix}, \quad
\begin{bmatrix}
\binom{\eta_1}{\delta_1} \\
\vdots \\
\binom{\eta_{n-2}}{\delta_{n-2}}
\end{bmatrix}
\]

Consider the pairs

\[
\left( \binom{\alpha_i}{\beta_i}, \binom{\eta_i}{\delta_i} \right), \text{ for } i = 1, \ldots, n - 2.
\]

If each such pair was linearly dependent, then \( g' \) would be a product of the appropriate powers of \( g_1', \ldots, g_{n-2}' \), a contradiction. Thus there exists at least one such pair
which is linearly independent. We may suppose that the first $s$ pairs are linearly independent and the others are linearly dependent. Then, for each linearly dependent pair $\left( \left( \alpha_j \right)_j, \left( \eta_j \right)_j \right)$, where $j = s + 1, \ldots, n - 2$, we may add the appropriate multiple of $\left( \left( \alpha_j \right)_j \right)$ to the second row of the above picture to cancel the corresponding column. Thus we have a new picture:

$$
\begin{bmatrix}
\left( \alpha_1 \right)_1, & \cdots, & \left( \alpha_s \right)_s, & \left( \alpha_{s+1} \right)_{s+1}, & \cdots, & \left( \alpha_{n-2} \right)_{n-2} \\
\left( \eta_1 \right)_{d_1}, & \cdots, & \left( \eta_s \right)_{d_s}, & 0, & \cdots, & 0 \\
\end{bmatrix},
$$

where, the pairs $\left( \left( \alpha_i \right)_i, \left( \eta_i \right)_{d_i} \right)$, for $i = 1, \ldots, s$, are linearly independent. Since the last $n - 2 - s$ tail matrices on the first row of the picture above will not play roles in our argument any more, we ignore them by considering this picture:

$$
\begin{bmatrix}
\left( \alpha_1 \right)_1, & \cdots, & \left( \alpha_s \right)_s, & \left( \ast \right)_1, & \cdots, & \left( \ast \right) \\
\left( \eta_1 \right)_{d_1}, & \cdots, & \left( \eta_s \right)_{d_s}, & 0, & \cdots, & 0 \\
\end{bmatrix}.
$$

In the picture above, it is not hard to see that we may simply put $\left( \left( \alpha_i \right)_i \right) = \left( \left( 1 \right)_i \right)$. For each $i \in \{2, \ldots, s\}$, up to multiplying $\left( \left( \alpha_i \right)_i \right)$ by the appropriate scalar, we may put $\left( \left( \alpha_i \right)_i \right) = \left( \left( 0 \right)_i \right)$ if $\beta_i = 0$, and put $\left( \left( \alpha_i \right)_i \right) = \left( \left( 1 \right)_i \right)$ if $\beta_i \neq 0$. Thus we may proceed assuming the following picture:

$$
\begin{bmatrix}
\left( \left( 1 \right)_i \right)_1, & \cdots, & \left( \left( 1 \right)_{t+1} \right)_{t+1}, & \left( \ast \right)_1, & \cdots, & \left( \ast \right) \\
\left( \eta_1 \right)_{d_1}, & \cdots, & \left( \eta_{t+1} \right)_{d_{t+1}}, & \left( \eta_s \right)_{d_s}, & 0, & \cdots, & 0 \\
\end{bmatrix},
$$

where $t$ is some integer with $1 \leq t \leq s$, and the pairs $\left( \left( 1 \right)_i, \left( \eta_i \right)_{d_i} \right)$ ($1 \leq i \leq t$) and $\left( \left( \alpha_j \right)_j, \left( \eta_j \right)_{d_j} \right)$ ($t + 1 \leq j \leq s$) are all linearly independent.
We now add the appropriate multiples of the first \( s \) tail matrices on the first row of the picture above to the second row of the picture and obtain:

\[
\begin{bmatrix}
(1_0)_1, & \ldots, & (1_0)_t, & \left(\frac{\alpha t+1}{1}\right)_{t+1}, & \ldots, & \left(\frac{\alpha s}{1}\right), & (\ast), & \ldots, & (\ast) \\
(0), & \ldots, & 0, & \left(\frac{\alpha t+1}{0}\right), & \ldots, & (\frac{\alpha s}{0}), & 0, & \ldots, & 0
\end{bmatrix}
\]

where all \( \lambda_i \)'s have to be non-zero.

Finally, it is not hard to see that we may derive this picture:

\[
\begin{bmatrix}
(1_0)_1, & \ldots, & (1_0)_t, & \left(\frac{\alpha t+1}{1}\right)_{t+1}, & \ldots, & \left(\frac{\alpha s}{1}\right), & (\ast), & \ldots, & (\ast) \\
(0), & \ldots, & 0, & \left(\frac{\alpha t+1}{0}\right), & \ldots, & (\frac{\alpha s}{0}), & 0, & \ldots, & 0
\end{bmatrix}
\]

From now on we suppose that \( X := \{x_1, x_2, y_1, \ldots, y_{n-2}\} \) is the basis associated with this picture above, where \( \{x_1, x_2\} \) is a basis of \( V_G \). We note, from the picture above, that there exist \( g_1, g \in G \) such that

\[
t_X(g_1) = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)},
\]

\[
t_X(g) = \begin{bmatrix} 0 & 0 & \ldots & 0 & \lambda_{t+1} & \ldots & \lambda_s & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)}.
\]

Now consider an element \( g_2 \in \text{GL}(V) \) with

\[
t_X(g_2) = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)}.
\]

If \( g_2 \in G \), then it is easily seen that \( G = \langle g_1, g_2, G' \rangle \), where \( G' \) is some reflection subgroup of \( G \) which fixes \( \{x_1, x_2, y_1\} \) point-wise. If \( G' \) is a one-row group, then it is not hard to see that \( G' \) is a Nakajima \( p \)-group with respect to \( X \). And it follows that \( G \) is a Nakajima \( p \)-group, whose invariant ring is polynomial. If \( G' \) is a two-row
group, then it is an Abelian reflection two-row $p$-group. It follows that there is a natural faithful representation $\rho: G' \to \text{GL}(V')$, where $V'$ is the subspace spanned by \{ $x_1$, $x_2$, $y_2$, $\ldots$, $y_{n-2}$ \}, such that $\rho(G')$ is an Abelian reflection two-row $p$-subgroup of $\text{GL}(V')$. By the induction hypothesis, we see that $S(V)\rho(G')$ is an Abelian reflection two-row $p$-subgroup of $\text{GL}(V')$. By the induction hypothesis, we see that $S(V')\rho(G')$ is a complete intersection.

Since $S(V)^{G'} \cong S(V')^{\rho(G')}[y_1]$, it follows that $S(V)^G \cong S(V')^{\rho(G')}[N]$, where $N$ is the norm of $y_1$ under $G$. By Proposition 3.1.1, we see that $S(V)^G$ is a complete intersection.

Thus we may assume $g_2 \notin G$. Note that this assumption forces $t \neq s$ in the picture above. Let $E$ be the largest Abelian reflection two-row $p$-group containing $G$. We know that $E$ is a Nakajima $p$-group. It is easily seen that we may have a maximal subgroup $L$ of $E$ which contains $G$ and satisfies the condition $g_2 \notin L$. Thus, by Campbell and Hughes [5, Theorem 4.4], we have $S(V)^L = S(V)^E[a]$ for some homogeneous element $a \in S(V)^L$ which has these properties:

1. $(g_2 - 1)a \in S(V)^E$.

2. $(g_2 - 1)a$ divides the product $x_1 \prod_{\alpha \in \mathbb{F}_p} (x_2 + \alpha x_1)$. (See Campbell and Hughes [5, Section 4], or c.f. Hughes and Kechagias [14, Proposition 9].)

Let $K = \langle g_2, G \rangle$. We claim that $S(V)^G = S(V)^K[a]$. By Campbell and Hughes [5, Proposition 3.1], in order to show this we may prove that $(g_2 - 1)a$ divides $(g_2 - 1)c$ for any $c \in S(V)^G$, which can be achieved by showing that $x_1 \prod_{\alpha \in \mathbb{F}_p} (x_2 + \alpha x_1)$ divides $(g_2 - 1)c$ for any $c \in S(V)^G$. Now let $c$ be in $S(V)^G$. Since $g_1$ and $g$ are elements of
$G$, then for all $\alpha \in \mathbb{F}_p$ we have

$$(g_2 - 1)c = (g_2g^{-1} - 1)c = (g_2g_1^\alpha - 1)c.$$

It is easily seen that $g_2g^{-1}$ and all $g_2g_1^\alpha$ are reflections, whose root vectors are exactly the distinct linear factors (up to scalars) of the product $x_1 \prod_{\alpha \in \mathbb{F}_p} (x_2 + \alpha x_1)$. (Note: a root vector of a reflection $g \in \text{GL}(V)$ is just a nonzero element of the 1-dimensional vector space $(g - 1)V$.) Because of the equalities above, it follows that all the root vectors divide $(g_2 - 1)c$, and thus so does the product, as desired.

Since $K$ contains both $g_1$ and $g_2$, by an analogue of the argument for the situation where $g_2 \in G$, we see that $S(V)^K$ is a complete intersection. It follows from Proposition 3.1.1 that $S(V)^G$ is a complete intersection. \qed
Chapter 4

Polynomial Invariant Rings

Throughout this chapter, unless otherwise stated, let $V$ be an $n$-dimensional vector space over the prime field $\mathbb{F}_p$, where $p$ is an odd prime number.

From the preceding chapter, we know the invariant rings of Abelian reflection two-row $p$-subgroups of $\text{GL}(V)$ are complete intersections. As mentioned before, the Abelian reflection two-row $p$-subgroups are exactly the two-row subgroups which are equal to their kernels. In this chapter, we deal with two-row groups which are \textit{not} equal to their kernels. We show “almost” all these groups have polynomial invariant rings. More precisely speaking, if a two-row subgroup of $\text{GL}(V)$ has non-normal Sylow $p$-subgroups, then the invariant rings are polynomial; if a two-row subgroup of $\text{GL}(V)$ has normal Sylow $p$-subgroups, then its invariant ring is polynomial if we further assume both the two-row group and its Sylow $p$-subgroups are generated by
CHAPTER 4. POLYNOMIAL INVARIANT RINGS

reflections.

4.1 Abelian Reflection Two-Row $p$-groups

with Specific Normalizers

In proving that the invariant rings of some two-row groups which are not equal to their kernels are polynomial, an essential step is to show their kernels are Nakajima $p$-groups. The following results will tell us that the kernels are Nakajima $p$-groups if the two-row groups contain some specific elements.

Lemma 4.1.1. Let $U$ be a two-dimensional subspace of $V$ with a basis $X_0 = \{x_1, x_2\}$. Let $M$ be a subgroup of $E(U)$.

Then we have the following conclusions.

1. Let $a$ and $b$ be elements in $T(U)$ whose actions on $U$ under $X_0$ are given by the following:

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. $$

If $M$ is normalized by $a$ and $b$, then $M$ is a Nakajima $p$-group with respect to a basis $X$ of $V$ which is enlarged from the basis $X_0$ of $U$, and the Nakajima decomposition $M = M_1 \cdots M_n$ satisfies the conditions: $M_1 = M_2 = 1$, and $M_i = 1$ or $p^2$ for $i = 3, \ldots, n$. We refer to such a Nakajima $p$-group as a full Nakajima $p$-group.
2. If $M$ is normalized by one of the two elements $c$ and $d$ in $T(U)$ whose actions on $U$ under $X_0$ are given by the following:

$$
\bar{c} = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}, \quad \bar{d} = \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix},
$$

where $\zeta$ and $\xi$ are non-zero and non-identity scalars, then $M$ is a Nakajima $p$-group with respect to a basis $X$ of $V$ which is enlarged from the basis $X_0$ of $U$.

3. Let $a$ and $b$ be elements in $T(U)$ whose actions on $U$ under $X_0$ are given by the following:

$$
\bar{a} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \bar{b} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.
$$

If $M$ is a reflection group and $M$ is normalized by either $a$ or $b$, then $M$ is a Nakajima $p$-group with respect to a basis $X$ of $V$ which is enlarged from the basis $X_0$ of $U$.

Proof. We note that $M$ is an elementary Abelian $p$-group consisting of elements of order $p$.

1. Let $X$ be a basis of $V$ which is enlarged from $X_0$. Take a non-identity element $g \in M$, whose tail matrix under $X$ can be expressed as

$$
g = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},
$$

where $\alpha$ and $\beta$ are row vectors of $\mathbb{F}_p^{n-2}$, at least one of which is non-zero. Without loss of generality, suppose that $\beta$ is non-zero. Since both $a$ and $b$ normalize $M$, then both
$g_1 := aga^{-1}g^{-1}$ and $g_2 := bg_1b^{-1}g_1^{-1}$ are elements of $M$, whose tail matrices under $X$ can be expressed as

$$g_1 = \begin{bmatrix} \beta \\ \vdots \\ 0 \end{bmatrix} \text{ and } g_2 = \begin{bmatrix} 0 \\ \vdots \\ \beta \end{bmatrix}.$$  

Up to a change of the basis $X$ on the elements not in $X_0$ and up to raising $g_1$ and $g_2$ to appropriate powers, we may assume that the tail matrices of $g_1$ and $g_2$ under $X$ can be expressed as  

$$g_1 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{2 \times (n-2)} \quad \text{and} \quad g_2 = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix}_{2 \times (n-2)}.$$  

Putting $X = \{x_1, x_2, \ldots, x_n\}$, let $E'$ be the subgroup of $E(U)$ which consists of the elements whose tail matrices under $X$ form this set

$$\left\{ \begin{bmatrix} 0 & \lambda_1 & \cdots & \lambda_{n-3} \\ 0 & \mu_1 & \cdots & \mu_{n-3} \end{bmatrix} \bigg| \lambda_i, \mu_i \in \mathbb{F}_p, i = 1, \ldots, n-3 \right\}.$$  

It is not hard to see that $M = \langle g_1, g_2, M' \rangle$, where $M' = E' \cap M$. Note that $E'$ acts trivially on $\{x_1, x_2, x_3\}$. Let $V'$ be the subspace of $V$ which is spanned by $\{x_1, x_2, x_4, \ldots, x_n\}$. Then there is a natural faithful representation $\rho: E' \to \text{GL}(V')$ such that $\rho(E')$ is the largest two-row subgroup of $\text{GL}(V')$ which acts trivially on $U$. Clearly $\rho(M')$ is a subgroup of $\rho(E')$. Let $T'(U)$ be the largest two-row subgroup of $\text{GL}(V')$ with respect to the subspace $U$ of $V'$, then it is easily to verify that $\rho(M')$ is normalized by any such elements $a'$ and $b'$ of $T'(U)$ whose actions on $U$ are given by the following:

$$\overline{a'} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \overline{b'} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$
Thus, by induction on the dimension of $V$, we may assume that $\rho(M')$ is a full Nakajima $p$-group with respect to a basis $\{x_1, x_2, x_4', \ldots, x_n'\}$ of $V'$, which is enlarged from $X_0$. Note that $M'$ acts trivially on $\{x_1, x_2, x_3\}$. It follows that $M'$ is also a Nakajima $p$-group with respect to the basis $X' = \{x_1, x_2, x_3, x_4', \ldots, x_n'\}$. This implies easily that $M$ is a full Nakajima two-row $p$-group with respect to the basis $X'$, which is enlarged from $X_0$. This completes the proof.

2. We prove the conclusion holds for the case where $M$ is normalized by $c$. The case where $M$ is normalized by $d$ follows similarly.

Let $X$ be a basis of $V$ which is enlarged from $X_0$. First, if $M$ is a one-row subgroup of $E(U)$, then it is easily seen that $M$ is a Nakajima $p$-group with respect to a basis of $V$ which is enlarged from $X_0$. We now assume that $M$ is a two-row subgroup of $E(U)$. It follows that there must be an element $g \in M$ whose tail matrix under $X$ can be expressed as

$$g = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

where $\alpha$ and $\beta$ are row vectors of $\mathbb{F}_p^{n-2}$ with $\beta$ non-zero. Since $c$ normalizes $M$, it follows that $g_1 := cgc^{-1}g^{-1} \in M$, whose tail matrix under $X$ can be expressed as

$$g_1 = \begin{bmatrix} 0 \\ (\zeta - 1) \beta \end{bmatrix}.$$

Up to a change of the basis $X$ on the elements not in $X_0$ and up to raising $g_1$ to some power, we may further assume that the tail matrix of $g_1$ under $X$ can be expressed
 CHAPTER 4. POLYNOMIAL INVARIANT RINGS

as

\[
g_1 = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix}_{2 \times (n-2)}.
\]

Put \( X = \{ x_1, \ldots, x_n \} \). Now we have two cases to consider according to whether there is an element \( g' \in M \) such that the (1,1)-entry of the tail matrix of \( g' \) under \( X \) is non-zero.

Case 1. Assume that there is no such an element \( g' \). Let \( E_1 \) be the subgroup of \( E(U) \) which consists of the elements whose tail matrices under \( X \) form this set

\[
\left\{ \begin{bmatrix} 0 & \lambda_1 & \cdots & \lambda_{n-3} \\ 0 & \mu_1 & \cdots & \mu_{n-3} \end{bmatrix} \left| \lambda_i, \mu_i \in \mathbb{F}_p, i = 1, \ldots, n-3 \right. \right\}.
\]

It is easy to see that \( M = \langle g_1, M_1 \rangle \), where \( M_1 = E_1 \cap M \). Let \( V_1 \) be the subspace of \( V \) which is spanned by \( \{ x_1, x_2, x_4, \ldots, x_n \} \). Then there is a natural faithful representation \( \rho_1 : E_1 \to \text{GL}(V_1) \) such that \( \rho_1(E_1) \) is the largest two-row subgroup of \( \text{GL}(V_1) \) which acts trivially on \( U \). Clearly \( \rho_1(M_1) \) is a subgroup of \( \rho_1(E_1) \). Let \( T_1(U) \) be the largest two-row subgroup of \( \text{GL}(V_1) \) with respect to the subspace \( U \) of \( V_1 \), then it is easily to verify that \( \rho_1(M_1) \) is normalized by any such elements \( a_1 \) and \( b_1 \) of \( T_1(U) \) whose actions on \( U \) under \( X_0 \) are given by the following:

\[
\overline{a_1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \overline{b_1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.
\]

Case 2. Assume that we have such an element \( g' \). Its tail matrix under \( X \) is can be written as

\[
g' = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix},
\]
where $\alpha'$ and $\beta'$ are row vectors of $\mathbb{F}_p^{n-2}$, and $\alpha' = (\alpha'_3, \ldots, \alpha'_n)$ with $\alpha'_3$ non-zero. Then, as we argued before, we have the element whose tail matrix under $X$ can be written as
\[
\begin{bmatrix}
0 \\
(\zeta - 1)\beta'
\end{bmatrix}.
\]
Hence we see that we have the element $g_2 \in M$ whose tail matrix under $X$ is of this form
\[
g_2 = \begin{bmatrix}
\alpha' \\
0
\end{bmatrix}.
\]
We may assume $\alpha'_1 = 1$. Now change $X$ to this basis
\[
X' = \{x_1, x_2, x_3, x'_4 := x_4 - \alpha'_4 x_1, \ldots, x'_n := x_n - \alpha'_n x_1\}.
\]
Thus the tail matrices of $g_1$ and $g_2$ under $X'$ can be written as
\[
\begin{align*}
g_1 &= \begin{bmatrix}
0 & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0
\end{bmatrix}_{2 \times (n-2)}, \\
g_2 &= \begin{bmatrix}
1 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0
\end{bmatrix}_{2 \times (n-2)}.
\end{align*}
\]
Let $E_2$ be the subgroup of $E(U)$ which consists of the elements whose tail matrices under $X'$ form this set
\[
\left\{ \begin{bmatrix}
0 & \lambda_1 & \cdots & \lambda_{n-3} \\
0 & \mu_1 & \cdots & \mu_{n-3}
\end{bmatrix} \middle| \lambda_i, \mu_i \in \mathbb{F}_p, i = 1, \ldots, n-3 \right\}.
\]
It is not hard to see that $M = \langle g_1, g_2, M_2 \rangle$, where $M_2 = E_2 \cap M$. Let $V_2$ be the subspace of $V$ which is spanned by $\{x_1, x_2, x'_4, \ldots, x'_n\}$. Then there is a natural faithful representation $\rho_2 : E_2 \to \text{GL}(V_2)$ such that $\rho_2(E_2)$ is the largest two-row
subgroup of GL($V_2$) which acts trivially on $U$. Clearly $\rho_2(M_2)$ is a subgroup of $\rho_2(E_2)$. Let $T_2(U)$ be the largest two-row subgroup of GL($V_2$) with respect to the subspace $U$ of $V_2$, then it is easily to verify that $\rho_2(M_2)$ is normalized by any such elements $a_2$ and $b_2$ of $T_2(U)$ whose actions on $U$ under $X_0$ are given by the following:

$$\bar{a}_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \bar{b}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Thus, by induction on the dimension of $V$, for each $i = 1, 2$, we may assume that $\rho_i(M_i)$ is a Nakajima $p$-group under some basis of $V_i$, say $\{x_1, x_2, x_{i4}, \ldots, x_{in}\}$. It follows that $M_i$ is a Nakajima $p$-group under the basis $\{x_1, x_2, x_3, x_{i4}, \ldots, x_{in}\}$, where $i = 1, 2$. This implies easily that in each case $M$ is a Nakajima $p$-group with respect to some basis of $V$ which is enlarged from $X_0$. This completes the proof.

3. We prove the conclusion holds for the case where $M$ is normalized by $a$. The case where $M$ is normalized by $b$ follows similarly.

Let $X$ be a basis of $V$ which is enlarged from $X_0$. First, if $M$ is a one-row subgroup of $E(U)$, then it is easily seen that $M$ is a Nakajima $p$-group with respect to a basis of $V$ which is enlarged from $X_0$. We now assume that $M$ is a two-row subgroup of $E(U)$. It follows that there must be a reflection $g \in M$ such that the second row of the tail matrix of $g$ under $X$ is non-zero. Up to a change of the basis $X$ on the elements not in $X_0$ and up to raising $g$ to some power, we may assume that the tail
matrix of $g$ under $X$ is of this form:

$$g = \begin{bmatrix} \zeta & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)}.$$ 

Since $a$ normalizes $M$, it follows that both $g_1 = aga^{-1}g^{-1}$ and $g_2 = gg_1^{-\zeta}$ are in $M$, whose tail matrices under $X$ are of the following form:

$$g_1 = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)},$$

$$g_2 = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix}_{2 \times (n-2)}.$$

Putting $X = \{x_1, x_2, \ldots, x_n\}$, let $E'$ be the subgroup of $E(U)$ which consists of the elements whose tail matrices under $X$ form this set

$$\left\{ \begin{bmatrix} 0 & \lambda_1 & \ldots & \lambda_{n-3} \\ 0 & \mu_1 & \ldots & \mu_{n-3} \end{bmatrix} \bigg| \lambda_i, \mu_i \in \mathbb{F}_p, i = 1, \ldots, n-3 \right\}.$$

It is not hard to see that $M = \langle g_1, g_2, M' \rangle$, where $M' = E' \cap M$. Let $V'$ be the subspace of $V$ which is spanned by $\{x_1, x_2, x_4, \ldots, x_n\}$. Then there is a natural faithful representation $\rho: E' \to \text{GL}(V')$ such that $\rho(E')$ is the largest two-row subgroup of $\text{GL}(V')$ which acts trivially on $U$. Clearly $\rho(M')$ is a subgroup of $\rho(E')$. Let $T'(U)$ be the largest two-row subgroup of $\text{GL}(V')$ with respect to the subspace $U$ of $V'$, then it is easily to verify that $\rho(M')$ is normalized by any such elements $a'$ and $b'$ of $T'(U)$ whose actions on $U$ are given by the following:

$$\overline{a'} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \overline{b'} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$
Thus, by induction on the dimension of $V$, we may assume that $\rho(M')$ is a Nakajima $p$-group with respect to a basis $\{x_1, x_2, x'_4, \ldots, x'_n\}$ of $V'$, which is enlarged from $X_0$. It follows that $M'$ is a Nakajima $p$-group with respect to the basis $X' = \{x_1, x_2, x_3, x'_4, \ldots, x'_n\}$. This implies easily that $M$ is a Nakajima $p$-group with respect to the basis $X'$, which is enlarged from $X_0$. \hfill \qed

4.2 Two-Row Groups with Non-normal Sylow $p$-Subgroups

We prove the following result.

**Proposition 4.2.1.** Let $U$ be a two-dimensional vector space over the prime field $\mathbb{F}_p$. If there are two elements $g_1$ and $g_2$ of order $p$ in $\text{GL}(U)$ such that neither is a power of the other, then $\langle g_1, g_2 \rangle = \text{SL}(U)$. Moreover, there exists a basis of $U$ such that the matrices of $g_1$ and $g_2$ under such a basis are of the following forms respectively

\[
\begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
1 & 0 \\
1 & 1
\end{bmatrix},
\]

where $\alpha$ and $\beta$ are non-zero scalars in $\mathbb{F}_p$.

**Proof.** Since $g_1$ and $g_2$ are $p$-elements, it follows that both $U_1 := U^{g_1}$ and $U_2 := U^{g_2}$ are one-dimensional. Let $X := \{x_1, x_2\}$ be a basis of $U$, where $x_1 \in U_1$. Then it is
not hard to see that \( g_1 \) has this matrix
\[
[g_1]_X = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}
\]
for some non-zero scalar \( \alpha \).

We claim that \( U_1 \neq U_2 \). Otherwise, \( g_2 \) would have this matrix
\[
[g_2]_X = \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix}
\]
for some non-zero scalar \( \gamma \). This would imply that \( g_2 \) is a power of \( g_1 \), a contradiction.

Thus we may suppose that \( x_2 \in U_2 \). Then \( g_2 \) has this matrix
\[
[g_2]_X = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}
\]
for some non-zero scalar \( \beta \). Therefore, by Theorem 8.4 in Gorenstein [12], we have
\[
\langle g_1, g_2 \rangle = \text{SL}(U).
\]

Recall that the order of \( \text{GL}(2, p) \) is \((p^2 - 1)(p^2 - p)\) and that the order of \( \text{SL}(2, p) \) is \((p + 1)(p - 1)p\).

**Theorem 4.2.2.** Let \( V \) be a finite-dimensional vector space over the prime field \( \mathbb{F}_p \), and \( G \) a two-row subgroup of \( \text{GL}(V) \). If there is a non-normal Sylow \( p \)-subgroup of \( G \), then \( S(V)^G \) is a polynomial ring.

**Proof.** By assumption, there are at least two distinct Sylow \( p \)-subgroups of \( G \), say \( Q_1 \) and \( Q_2 \). Note that \( K_G \) is a proper normal subgroup of both \( Q_1 \) and \( Q_2 \). It follows
that $\overline{Q}_1$ and $\overline{Q}_2$ are two distinct cyclic subgroups of $\mathcal{G}$, where $\mathcal{G}$ is the image of the restriction map, which are generated by two elements of order $p$, say $\overline{g}_1$ and $\overline{g}_2$. By Lemma 4.2.1, we have $\langle \overline{g}_1, \overline{g}_2 \rangle = \text{SL}(V_G)$. Thus $\text{SL}(V_G)$ is a normal subgroup of $\mathcal{G}$.

Note that $\mathcal{G}/\text{SL}(V_G)$ is a cyclic group whose order divides $p - 1$. This implies that $\mathcal{G}$ is generated by $\text{SL}(V_G)$ and a non-modular element $\overline{\omega}$ with

$$[\overline{\omega}]_{X_0} = \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}.$$ 

There is an element $\overline{\lambda} \in \text{SL}(V_G)$ with

$$[\overline{\lambda}]_{X_0} = \begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{bmatrix},$$

where $\epsilon$ is a primitive $(p - 1)$-st root of unit.

Let $\omega'$ and $\lambda'$ be two elements of $G$ such that their restrictions to $V_G$ are $\overline{\omega}$ and $\overline{\lambda}$ respectively. Consider the group $H' = \langle K_G, \omega', \lambda' \rangle$. Obviously $H'/K_G$ is non-modular. By the Schur-Zassenhaus Theorem (see Gorenstein [12, Theorem 2.1, p. 221]), there is a subgroup $H$ of $H'$, which is isomorphic to $H'/K_G$, such that $H' = HK_G$. Then $\omega' = \omega l_1$ and $\lambda' = \lambda l_2$ for some elements $\omega, \lambda \in H$ and $l_1, l_2 \in K_G$.

It follows that $\overline{\omega} = \overline{\omega'}$ and $\overline{\lambda} = \overline{\lambda'}$. Note that $H$ is a non-modular subgroup of $G$ and $V_G$ is a $H$-module. It follows from Maschke’s Theorem (c.f. Dummit and Foote [17, p. 849]) that there is a complementary $H$-module $W$ of $V_G$ in $V$. Clearly $H$ acts trivially on $W$. Now enlarge the basis $X_0$ of $V_G$ to a basis $X$ compatible with the
CHAPTER 4. POLYNOMIAL INVARIANT RINGS

33

direct sum $V = V_G \oplus W$. Then

$$[\omega]_X = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & I_{n-2} \end{bmatrix}_{n \times n} \quad \text{and} \quad [\lambda]_X = \begin{bmatrix} \epsilon & 0 & \cdots & 0 \\ 0 & I_{n-2} \end{bmatrix}_{n \times n}.$$

Since $S(V) \subset \overline{G}$, there are two elements $\tau$ and $\pi$ in $G$ such that

$$[\tau]_X = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & I_{n-2} \end{bmatrix}_{n \times n} \quad \text{and} \quad [\pi]_X = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & I_{n-2} \end{bmatrix}_{n \times n}.$$

Since both $\tau$ and $\pi$ normalize $K_G$, it follows from Lemma 4.1.1 that $K_G$ is a Nakajima $p$-group with respect to a basis $Y = Y_0 \cup Y_1$, where $Y_0 = X_0$ and $Y_1$ is a basis of $W$. Thus we may simply think of $X$ as $Y$. Putting $X = \{x_1, x_2, \ldots, x_n\}$, we see that $K_G$ is a Nakajima $p$-group which can be written as $K_G = K_{s+1}K_{s+2} \cdots K_n$, where $K_i$ is a subgroup generated by two elements $g_{1i}$ and $g_{2i}$ which satisfy these conditions: both act trivially on all the elements of $X$ other than $x_i$, and $(g_{1i} - 1)x_i = x_1$ and $(g_{2i} - 1)x_i = x_2$. Moreover, it is not hard to see that any element of $T := T(V_G)$ which acts trivially on $x_1, x_2, \ldots, x_s$ lies in $K_G$. Then it is not hard to see that $K_G$ is normal in $T$.

Computing $\phi := \lambda \tau \lambda^{-1} \tau - \epsilon^2$, we find

$$[\phi]_X = \begin{bmatrix} I & \delta t_{\tau} \\ 0 & I \end{bmatrix},$$

where

$$\delta = \begin{bmatrix} \epsilon - \epsilon^2 & * \\ 0 & \epsilon^{-1} - \epsilon^2 \end{bmatrix}$$

is a $2 \times 2$ invertible matrix. Obviously we have $\phi \in K_G$. Let $\delta$ be the element of $T$
which satisfies
\[ [\delta]_X = \begin{bmatrix} \delta & 0 \\ 0 & I \end{bmatrix}. \]

Since \( K_G \) is normal in \( T \), it follows that \( \xi := \delta^{-1} \phi \delta \in K_G \) and
\[ [\xi]_X = \begin{bmatrix} I & t_{\tau} \\ 0 & I \end{bmatrix}. \]

Thus there is an element \( \tau' \in G \) with
\[ [\tau']_X = \begin{bmatrix} \tau & 0 \\ 0 & I \end{bmatrix}. \]

Similarly, we can show that there is an element \( \pi' \) with
\[ [\pi']_X = \begin{bmatrix} \pi & 0 \\ 0 & I \end{bmatrix}. \]

Now it is easy to see that
\[ G = \langle K_G, \tau', \pi', \omega \rangle = K_G G', \]
where \( G' = \langle \tau', \pi', \omega \rangle \). Since we have \( \text{SL}(V_G) \leq G' \leq \text{GL}(V_G) \), it is not hard to see that \( S(V)^{G'} \) is a polynomial algebra generated by \( u, v, x_3, \ldots, x_n \) for some \( u, v \in S(V) \). Since \( K_G \) is a Nakajima \( p \)-group, then \( S(V)^G = S(V)^{K_G} \) is a polynomial algebra generated by norms \( x_1, x_2, N_3, \ldots, N_n \). Now it is routine to verify that \( S(V)^G \) is a polynomial algebra generated by \( u, v, N_3, \ldots, N_n \). \( \square \)
4.3 Two-Row Groups with a Normal Sylow

$p$-Subgroup

When two-row groups over $\mathbb{F}_p$ are not equal to their kernels and have normal Sylow $p$-subgroups, by imposing the condition of being generated by reflections on both the two-row groups and their Sylow $p$-subgroups, we can prove the invariant rings of such two-row groups are polynomial.

Recall that an element $g \in \text{GL}(V)$ is called a generalized reflection (on $\text{S}(V)$) if there is a homogenous polynomial $a$ of positive degree such that $gb - b \in aS(V)$ for all $b \in S(V)$. The following result is essentially a theorem of Nakajima.

**Theorem 4.3.1.** Let $V$ be a finitely dimensional vector space over the prime field $\mathbb{F}_p$. Let $G$ be a reflection subgroup of $\text{GL}(V)$, and $L$ a normal subgroup of $G$ such that $G/L$ is non-modular. If $S(V)^L$ is a polynomial ring, then $S(V)^G$ is a polynomial ring.

**Proof.** Let $g \in G$ be a reflection with root vector $x$, and $(x)$ the corresponding prime ideal in $S(V)$. It is known that $(g - 1)S(V) \subset (x)$. Since $S(V)^L \cap (x)$ is a homogeneous prime ideal of $S(V)^L$ of height one and $S(V)^L$ is a unique factorization domain, it follows that $(g - 1)S(V)^L \subset S(V)^L \cap (x) = S(V)^L f$ for some homogeneous polynomial $f$ of $S(V)^L$. Hence $G/L$ is generated by generalized reflections on $S(V)^L$. It follows that $S(V)^L$ is a finitely generated free module over $S(V)^G$ (c.f. Hochster
and Eagon [13, Proposition 16]). Since $S(V)^L$ is polynomial, it follows that $S(V)^G$ is polynomial.

\[ \square \]

**Theorem 4.3.2.** Let $G$ be a reflection two-row subgroup of GL($V$). If $G/K_G$ is a non-trivial non-modular group, then $S(V)^G$ is a polynomial ring.

**Proof.** Since $G$ is a reflection group with non-trivial $G/K_G$, there must be a reflection $g \in G \setminus K_G$. Since $G/K_G$ is non-modular, it follows that $gK_G$ is of order $t$, co-prime to $p$. Since any non-identity element in $K_G$ is of order $p$, it follows that the order of $g$ is either $t$ or $tp$. Put $h = g^p$, then $h$ is a reflection of order $t$ which is not in $K_G$. Thus there exists a basis $X$ enlarged from $V_G$ such that $h$ has this matrix

$$
[h]_X = \begin{bmatrix}
1 & 0 & \vdots & 0 \\
0 & a & \vdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & I_{n-2}
\end{bmatrix}_{n \times n},
$$

where $a$ is a non-zero scalar in $\mathbb{F}_p$. Since $h$ normalizes $K_G$, it follows from (2) of Lemma 4.1.1 that $K_G$ is a Nakajima $p$-group. Thus $S^{K_G}$ is a polynomial ring. By Theorem 4.3.1, we see $S^G$ is a polynomial ring. \[ \square \]

Any $p$-subgroup of $G$ which properly contains $K_G$ is a Sylow $p$-subgroup of $G$. Since $K_G$ is a normal $p$-subgroup of $G$, it follows that every Sylow $p$-subgroup of $G$ contains $K_G$.

**Lemma 4.3.3.** Let $G$ be a two-row subgroup of GL($V$). Let $P$ be a reflection $p$-subgroup of $G$ which contains $K_G$. If $P/K_G$ is non-trivial, then $P$ and $K_G$ are Nakajima groups with respect to the same Nakajima basis $X$ enlarged from $V_G$. 
Moreover, we have \( P = \langle \tau, K_G \rangle \), where \( \tau \) is the element of \( \text{GL}(V) \) which has this matrix

\[
[\tau]_X = \begin{bmatrix}
\frac{1}{a} & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 1 & \frac{1}{a} \\
\end{bmatrix}_{n \times n}.
\]

**Proof.** Obviously \( P/K_G \) is a non-trivial cyclic group of order \( p \). Since \( P \) is a reflection \( p \)-group, there must be a reflection \( \tau \) of order \( p \) outside of \( K_G \) such that \( P = \langle \tau, K_G \rangle \).

Since \((\tau - 1)V_G\) is non-zero and \((\tau - 1)V_G \subset (\tau - 1)V\), it follows that \( \tau \) is a reflection of order \( p \) on \( V_G \). Thus there is a basis \( X \) enlarged from \( V_G \) such that \( \tau \) has this matrix

\[
[\tau]_X = \begin{bmatrix}
\frac{1}{a} & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 1 & \frac{1}{a} \\
\end{bmatrix}_{n \times n},
\]

where \( a \) is a non-zero scalar and \( A \) is a \( 2 \times (n-2) \) matrix over \( \mathbb{F}_p \). Since \( \tau \) is a reflection, up to a change of the basis \( X \) on the elements outside of \( V_G \) and up to a change to a power of \( \tau \), we may further assume that \( \tau \) has this matrix

\[
[\tau]_X = \begin{bmatrix}
\frac{1}{a} & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 1 & \frac{1}{a} \\
\end{bmatrix}_{n \times n}.
\]

This implies that \( \tau \) acts trivially on a complementary subspace of \( V_G \). Since \( P \) is a reflection group, it follows that \( K_G \) is a reflection group. Since \( \tau \) normalizes \( K_G \), it follows from Lemma 4.1.1.(3) that \( K_G \) is a Nakajima \( p \)-group with the Nakajima basis \( X \).

**Theorem 4.3.4.** Let \( G \) be a reflection two-row subgroup of \( \text{GL}(V) \) which contains a normal reflection Sylow \( p \)-subgroup. If \( G/K_G \) is modular, then \( \text{S}(V)^G \) is a polynomial ring.
Proof. Since $K_G$ is a $p$-group, it is contained in a Sylow $p$-subgroup $Q$ of $G$, which, by assumption, is generated by reflections. Since $G/K_G$ is modular, it is not hard to see that $Q$ is generated by $K_G$ and a reflection $\tau$ of order $p$.

Note that $S(V)^Q$ is always a polynomial ring by Lemma 4.3.3. Since $Q$ is normal in $G$, then $S(V)^G$ is a polynomial ring by Theorem 4.3.1.
Chapter 5

Hypersurface Invariant Rings

Roughly speaking, the simplest two-row groups are subgroups of $GL(2, p)$. Throughout this chapter, we always assume that $p$ is an odd prime number. In section 1, we derive a simple result from a result due to Nakajima on hypersurface invariant rings.

In section 2, we rework Dickson’s classic result that invariant rings of subgroups of $SL(2, p)$ are all hypersurfaces, which was previously obtained by exhibiting generators of invariant rings in all cases. We give a simpler, direct and transparent proof which does not touch any invariants except for a few simple cases. Our method works for the complex numbers and even more generally for other fields of characteristic zero. In section 3, we show an example of a particular non-modular cyclic subgroup of $GL(2, p)$ whose invariant ring is not a complete intersection.
5.1 A Theorem of Nakajima

Let $V$ be a finite-dimensional vector space over an arbitrary field $\mathbb{F}$. Given a subspace $W$ of $V$ which is of codimension one, let $G_W$ be the set of elements of $G$ which fix $W$ point-wise. (In non-modular case, it is not hard to show that $G_W$ is a cyclic group.) If $G_W$ is non-trivial, then $W$ is called a \textbf{reflecting hyperplane of} $G$, and we refer to the order of $G_W$ as \textbf{the order of the reflecting hyperplane} $W$. We now present a criterion on hypersurfaces due to Nakajima [21, Corollary 4.3].

**Theorem 5.1.1.** Let $V$ be a vector space over a field of positive characteristic $p$. Let $G$ be a finite reflection subgroup of $\text{GL}(V)$ whose order is not divisible by $p$, and $H$ a normal subgroup of $G$ such that $G/H$ is Abelian. If $H$ contains no reflections, then $S(V)^H$ is a hypersurface if and only if there is a reflection subgroup $L$ of $G$ such that $H = L \cap \text{SL}(V)$ and the orders of reflecting hyperplanes of $L$ are equal to the index of $H$ in $L$.

Using this theorem, we can prove the following lemma. This lemma will be used to show that the invariant rings of the subgroups of $\text{SL}(2, p)$ are all hypersurfaces.

**Lemma 5.1.2.** Let $V$ be a vector space over a field of positive characteristic $p$. Let $G$ be a non-modular reflection subgroup of $\text{GL}(V)$, and $H$ a normal subgroup of $G$ such that $G/H$ is Abelian. If $H = G \cap \text{SL}(V)$ and $G/H$ is a cyclic group of order a prime number, then $S(V)^H$ is a hypersurface.
Proof. Since $\text{SL}(V)$ does not contain any diagonalizable reflections and $H$ is non-modular, it follows that $H$ contains no reflections. By Theorem 5.1.1, we only need to prove the orders of all reflecting hyperplanes of $G$ are equal to the order of $G/H$. Let $W$ be reflecting hyperplane of $G$. Consider the group $G_W$ consisting of elements of $G$ which fix $W$ point-wise. Obviously $G_W$ is non-modular. So its non-identity elements are all diagonalizable reflections. This implies $G_W \cap \text{SL}(V) = 1$. Since $H$ is a normal subgroup of $G$, it follows that we have

$$(G_W H)/H \cong G_W/(G_W \cap H) \cong G_W/(G_W \cap \text{SL}(V)) \cong G_W.$$ 

Note that $(G_W H)/H$ is a subgroup of $G/H$. Thus $G_W$ can be embedded into $G/H$. Since the order of $G/H$ is a prime number and $G_W \neq 1$, it follows that $|G_W| = |G/H|$.

This completes the proof.

\section{5.2 Subgroups of $\text{SL}(2, p)$}

Let $Z = \{\pm I\}$ be the center of $\text{SL}(2, p)$ with $p$ odd. Denote by $\text{PSL}(2, p)$ the factor group of $\text{SL}(2, p)$ by $Z$. In this section, we list all subgroups of $\text{SL}(2, p)$ up to isomorphisms. This list can be derived from a classical result due to Dickson [11, pp. 285] (c.f. Huppert [15, 8.27 Hauptsatz]). In the following we present a special case of the Dickson’s result by restricting to the prime field $\mathbb{F}_p$.

**Theorem 5.2.1 (Dickson [11, p. 285]).** The group $\text{PSL}(2, p)$ has only the following
subgroups up to isomorphisms.

1). An elementary Abelian $p$-group.

2). A cyclic group of order $m$, where $2m$ divides $p \pm 1$.

3). A Dihedral group of order $2m$, where $2m$ divides $p \pm 1$.

4). The alternating group $A_4$ for $p > 2$.

5). The symmetric group $S_4$ for $p^2 \equiv 1 \pmod{16}$.

6). The alternating group $A_5$ for $p = 5$ or $p^2 \equiv 1 \pmod{5}$.

7). A semidirect product of an elementary Abelian group of order $p^m$ with a cyclic group of order $t$, where $t$ divides $p - 1$.

8). The group $\text{PSL}(2, p)$.

From the theorem above, it is not hard to derive all the subgroups of $\text{SL}(2, p)$ by straightforward but tedious computations (c.f. Dickson [10, §9]).

**Proposition 5.2.2.** The group $\text{SL}(2, p)$ with $p$ odd has only the following subgroups up to isomorphisms.

1). The group $\text{SL}(2, p)$.

2). A modular subgroup $H$ of $\text{SL}(2, p)$ containing a normal cyclic group $P$ of order $p$ such that $H/P$ is a cyclic group of order dividing $p - 1$. 
3). A non-modular cyclic subgroup.

4). A non-modular subgroup $H$ of order $4m$, where $m$ divides $(p \pm 1)/2$, which is generated by two elements $a$ and $b$ satisfying conditions $a^m = -I$, $b^2 = -I$, and $bab^{-1} = a^{-1}$.

5). Non-modular subgroups $H_3$, $H_4$ and $H_5$, where $H_m = \langle a, b \mid a^m = b^3 = (ab)^3 = -I \rangle$, and $p \geq 5$ if $m = 3$, $p^2 \equiv 1 \pmod{16}$ if $m = 4$, and $p^2 \equiv 1 \pmod{5}$ if $m = 5$.

The rest of this chapter is devoted to showing that all subgroups of $\text{SL}(2, p)$ have hypersurface rings of invariants. It is known that the invariant ring of $\text{SL}(2, p)$ is a polynomial. By simple straightforward computation it is not hard to see that the invariant rings of the groups described in 2) and 3) of the above proposition are hypersurfaces.

Consider a subgroup $H$ of $\text{SL}(2, p)$ which is described in 4) of Proposition 5.2.2. Let the notation be as in Proposition 5.2.2. We work over $\mathbb{F}_p^2$. Let $\omega = \epsilon_2 + \epsilon_2^{-1}$, where $\epsilon_2 \in \mathbb{F}_p^2$ is a primitive $2m$-th root of unit. Clearly $\omega \in \mathbb{F}_p$ regardless of whether $2m$ divides $p - 1$ or $p + 1$. We write

$$a = \begin{bmatrix} \omega & 1 \\ -1 & 0 \end{bmatrix}.$$  

Using direct computations, we may find $k \in \text{GL}(2, p^2)$ such that

$$kHk^{-1} = \left\langle \begin{bmatrix} \epsilon_2 & 0 \\ 0 & \epsilon_2^{-1} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle = H'.$$
Let $R := \left \langle H', \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right \rangle$. It is easily seen that $R$ is a reflection group containing $H'$ of index 2. Thus, by Lemma 5.1.2, the invariant ring of $H'$, and hence of $H$, is a hypersurface.

In the following propositions, we show that the invariant rings of $H_m$ are all hypersurfaces.

**Proposition 5.2.3.** Rings of invariants of $H_3$ and $H_5$ are hypersurfaces.

**Proof.** Put $c = b^{-1}ab$. Since $cab = b^{-1}(ab)^2 = -b^{-1}$, we see $H_m = \langle a, c \rangle$. We work over $\mathbb{F}_p^2$. Let $\omega = \epsilon_{2m} + \epsilon_{2m}^{-1}$, where $\epsilon_{2m} \in \mathbb{F}_p^2$ is a primitive $2m$-th root of unit. Again, $\omega \in \mathbb{F}_p$ regardless of whether $2m$ dividing $p - 1$ or $p + 1$. We write

$$a = \begin{bmatrix} \omega & 1 \\ -1 & 0 \end{bmatrix}.$$  

Let $R_m = \langle a, c, \epsilon_{2m}I \rangle$. It is not hard to see that $R_m = \langle \epsilon_{2m}^{\pm 1}a, \epsilon_{2m}^{\pm 1}c \rangle$ is a reflection group. Since $(\epsilon_{2m}I)^m = -I \in H_m$, we see the order of $R_m/H_m$ is the prime number $m$. Lemma 5.1.2 completes the proof.  

**Proposition 5.2.4.** The invariant ring of $H_4$ is a hypersurface.

**Proof.** Put $c = b^{-1}ab$. Then we have $H_4 = \langle a, c \rangle$. Let $\omega = \epsilon_{2m} + \epsilon_{2m}$. Write

$$a = \begin{bmatrix} \omega & 1 \\ -1 & 0 \end{bmatrix}.$$  

Now put $R_4 = \langle a, b, \epsilon_4I \rangle$. It is not hard to show that $R_4 = \langle \epsilon_4a^2, \epsilon_4c^2, \epsilon_4ab \rangle$ is a reflection group. Since the index of $H_4$ in $R_4$ is 2, it follows from Lemma 5.1.2 that the invariant ring of $H_4$ is a hypersurface.
5.3 A Counterexample

Consider the following non-modular cyclic subgroup of \( \text{GL}(2, p) \), with \( p \geq 5 \):

\[
H = \langle \begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon \end{bmatrix} \rangle,
\]

where \( \epsilon \) is a primitive \((p - 1)\)-st root of unit in \( \mathbb{F}_p \). Clearly \( H \) is a two-row group.

Since \( H \) contains no reflections and is not a subgroup of \( \text{SL}(2, p) \), it follows from Theorem 1.1.4 that the invariant ring of \( H \) is not Gorenstein, and so is not a complete intersection.
Chapter 6

Concluding Remarks

The main results of this thesis are displayed in the following:

**Theorem (Theorem 3.2.1).** Let $G$ be an Abelian reflection two-row $p$-subgroup of $\text{GL}(V)$. Then $S(V)^G$ is a complete intersection.

**Theorem (Theorem 4.2.2).** Let $V$ be a finite-dimensional vector space over the prime field $\mathbb{F}_p$, and $G$ a two-row subgroup of $\text{GL}(V)$. If there is a non-normal Sylow $p$-subgroup of $G$, then $S(V)^G$ is a polynomial ring.

**Theorem (Theorem 4.3.2).** Let $G$ be a reflection two-row subgroup of $\text{GL}(V)$. If $G/K_G$ is a non-trivial non-modular group, then $S(V)^G$ is a polynomial ring.

**Theorem (Theorem 4.3.4).** Let $G$ be a reflection two-row subgroup of $\text{GL}(V)$ which contains a normal reflection Sylow $p$-subgroup. If $G/K_G$ is modular, then $S(V)^G$ is a polynomial ring.
**Theorem (Theorem A.0.2).** Let $\mathbb{F}$ be a field of characteristic $p$, $V$ an $n$-dimensional vector space over $\mathbb{F}$, and $G$ a finite $p$-subgroup of $GL(V)$. If $S(V)^G$ is a polynomial algebra generated by norms $N_i := \prod_{x \in G(y_i)} x$, $i = 1, ..., n$, of a basis $\{y_1, ..., y_n\}$ of the vector space $V$, then $G$ is a Nakajima $p$-group.

Finally we reworked Dickson’s classic result that invariant rings of subgroups of $SL(2, p)$ are all hypersurfaces, which was previously obtained by exhibiting generators of invariant rings in all cases. We give a simpler, direct and transparent proof which does not touch any invariants except for a few simple cases. Our method works for the complex numbers and even more generally for other fields of characteristic zero.

There is much future work to do: How to deal with modular two-row groups generated by bireflections? Can we extend the prime field to a bigger field? Can we adopt the systematic method mentioned in Neusel [22].
Bibliography


48


Appendix A

Characterizing Nakajima $p$-groups

Recall that, given any two finite subgroups $S$ and $T$ of a group $G$, we always have $|ST||S \cap T| = |S||T|$ (note that $ST$ need not be a group). This is a classical result in the theory of finite groups (see Rotman [25, Theorem 2.20] for a proof).

Lemma A.0.1. Let $S_1, \ldots, S_m$ be $m$ subgroups of a finite group $S$, then we have

$$\prod_{i=1}^{m} |S_i| = \left| \bigcap_{i=1}^{m} S_i \right| \cdot \prod_{j=2}^{m} \left| \left( \bigcap_{i=1}^{j-1} S_i \right) S_j \right| \leq \left| \bigcap_{i=1}^{m} S_i \right| |S|^{m-1}.$$  

Proof. By induction on $m$, it is easy to show that the equality holds using the result mentioned above. As for the inequality, it holds by the observation that

$$\left| \left( \bigcap_{i=1}^{j-1} S_i \right) S_j \right| \leq |S|$$  

for $j = 2, \ldots, m$. □

Let $G$ be a finite group and $X$ a $G$-set. Recall that, for $x \in X$, the isotropy group of $x$ under $G$ is $G_x = \{ g \in G : gx = x \}$ and the orbit of $x$ under $G$ is $G(x) = \{ gx : g \in G \}$.  

52
Theorem A.0.2. Let $\mathbb{F}$ be a field of characteristic $p$, $V$ an $n$-dimensional vector space over $\mathbb{F}$, and $G$ a finite $p$-subgroup of $GL(V)$. If $S(V)^G$ is a polynomial algebra generated by norms $N_i := \prod_{x \in G(y_i)} x$, $i = 1, \ldots, n$, of a basis $\{y_1, \ldots, y_n\}$ of the vector space $V$, then $G$ is a Nakajima $p$-group.

Proof. For $i = 1, \ldots, n$, let $H_i := \bigcap_{j=1, j \neq i}^n G_{y_j}$. First of all we are going to show $G = H_{\sigma(1)} \cdots H_{\sigma(n)}$ for any permutation $\sigma$ on $\{1, \ldots, n\}$. Since each norm $N_i$ is just the product of elements in $G(y_i)$, we have

$$|G| = |G_{y_i}| |G : G_{y_i}| = |G_{y_i}| |G(y_i)| = |G_{y_i}| \cdot \deg(N_i).$$

On the other hand, since $N_1, \ldots, N_n$ generate the polynomial invariant ring of $G$, we have $|G| = \prod_{i=1}^n \deg(N_i)$. Thus

$$|G|^n = \prod_{i=1}^n (|G_{y_i}| \cdot \deg(N_i))$$

$$= \left( \prod_{i=1}^n |G_{y_i}| \right) \left( \prod_{i=1}^n \deg(N_i) \right)$$

$$= \left( \prod_{i=1}^n |G_{y_i}| \right) |G|,$$

which implies that $|G|^{n-1} = \prod_{i=1}^n |G_{y_i}|$.

By Lemma 2, for each $k = 1, \ldots, n$, we have

$$\prod_{i=1 \atop i \neq k}^n |G_{y_i}| \leq \left| \bigcap_{i=1 \atop i \neq k}^n G_{y_i} \right| |G|^n = |H_k| |G|^{n-2}.$$

Thus

$$|G|^{n-1} = \prod_{i=1}^n |G_{y_i}| = |G_{y_k}| \prod_{i=1 \atop i \neq k}^n |G_{y_i}| \leq |G_{y_k}| |H_k| |G|^{n-2}.$$
APPENDIX A. CHARACTERIZING NAKAJIMA P-GROUPS

So $|G| \leq |G_{y_k}| H_k|$. On the other hand, since $G_{y_k} \cap H_k = \bigcap_{i=1}^{n} G_{y_i} = e$, we have $|G_{y_k}| H_k| = |G_{y_k} H_k| \leq |G|$. Therefore $|G_{y_k}| H_k| = |G|$ for $k = 1, ..., n$.

Now we have

$$|G|^n = \prod_{i=1}^{n} (|G_{y_i}| |H_i|) = \left( \prod_{i=1}^{n} |G_{y_i}| \right) \left( \prod_{i=1}^{n} |H_i| \right) = |G|^{n-1} \left( \prod_{i=1}^{n} |H_i| \right),$$

which implies $|G| = \prod_{i=1}^{n} |H_i|$.

Now we proceed to show $G = H_{\sigma(1)} \cdots H_{\sigma(n)}$ for any permutation $\sigma$ on $\{1, ..., n\}$.

For $k = 1, ..., n - 1$, we observe that $(H_{\sigma(1)} \cdots H_{\sigma(k)}) \cap H_{\sigma(k+1)} = e$, whence

$$|H_{\sigma(1)} \cdots H_{\sigma(k+1)}| = |H_{\sigma(1)} \cdots H_{\sigma(k)}||H_{\sigma(k+1)}|.$$

Thus it is easy to see that

$$|H_{\sigma(1)} \cdots H_{\sigma(n)}| = |H_{\sigma(1)}| \cdots |H_{\sigma(n)}| = \prod_{i=1}^{n} |H_i| = |G|,$$

which implies $G = H_{\sigma(1)} \cdots H_{\sigma(n)}$.

Next we are going to show that there exists a permutation $\tau$ on $\{1, ..., n\}$ such that the group $G$ is upper triangular with respect to the ordered basis $\{y_{\tau(1)}, ..., y_{\tau(n)}\}$.

Since $G$ is a finite $p$-group acting in characteristic $p$, we have the following chain

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_m = V,$$

where $m$ is some positive integer and each $V_l$ is a subspace of $W$ defined inductively by

$$V_l := \begin{cases} 0, & \text{if } l = 0; \\
\{w \in V \mid (g - 1)w \in V_{l-1} \text{ for all } g \in G\}, & \text{if } l \geq 1. \end{cases}$$
Now let \( d_l := \dim_\mathbb{F}(V_l) \) for all \( l \). Choose a basis \( \{x_1, ..., x_n\} \) for \( W \) such that \( \{x_1, ..., x_{d_l}\} \) is a basis of \( V_l \) for all \( l \). We note that \( G \) is upper triangular with respect to any basis of \( V \) chosen this way. Since \( \{y_1, ..., y_n\} \) is also a basis of \( V \), we can write

\[
x_i = \sum_{j=1}^{n} \alpha_{ji} y_j \quad \text{for} \quad i = 1, ..., n,
\]

where each \( \alpha_{ji} \) is just a scalar in \( \mathbb{F} \). Now for each \( i \) we define a set \( \mathcal{R}_i := \{y_j \mid \alpha_{ji} \neq 0, \text{ where } 1 \leq j \leq n\} \), which must be nonempty. Now for each \( l = 1, ..., m \), let \( \mathcal{Y}_l := \bigcup_{i=1}^{d_l} \mathcal{R}_i \). Obviously we have

\[
\mathcal{Y}_1 \subset \mathcal{Y}_2 \subset \cdots \subset \mathcal{Y}_m = \{y_1, ..., y_n\}.
\]

We proceed to show \( \text{Span}_\mathbb{F}(\mathcal{Y}_l) = V_l \) for each \( l \). Suppose \( y_k \in \mathcal{Y}_l \) for some \( k \in \{1, ..., n\} \). Then there exists some \( x_t \in V_l \) such that

\[
x_t = \sum_{j=1}^{n} \alpha_{jt} y_j, \quad \text{where } \alpha_{kt} \text{ must be non-zero}.
\]

Now take \( g \in G \). Since \( G = H_k H_1 \cdots H_{k-1} H_{k+1} \cdots H_n \) by what we have proved above, we can write \( g = g_k g_1 \cdots g_{k-1} g_{k+1} \cdots g_n \) with some \( g_i \in H_i \) for \( i = 1, ..., n \). Thus \( (g - 1)y_k = (g_k - 1)y_k \). We note \( (g_k - 1)x_t = \alpha_{kt}(g_k - 1)y_k \). Since \( x_t \in V_l \), we have \( (g - 1)y_k = \alpha_{kt}^{-1}(g_k - 1)x_t \in V_{l-1} \), which implies that \( y_k \in V_l \), and hence \( \mathcal{Y}_l \subset V_l \).

On the other hand, by the construction of \( \mathcal{Y}_l \), since each \( x_i \ (i = 1, ..., d_l) \) is a linear combination of some elements in \( \mathcal{Y}_l \), we see \( \text{Span}_\mathbb{F}(\mathcal{Y}_l) = V_l \). Thus it is not hard to see that there exists a permutation \( \tau \) on \( \{1, ..., n\} \) such that \( \mathcal{Y}_l = \{y_{\tau(1)}, ..., y_{\tau(d_l)}\} \)
for all \( l \). This implies that \( G \) is upper triangular with respect to the ordered basis \( \{y_{\tau(1)}, ..., y_{\tau(n)}\} \). Since \( G = H_{\tau(1)} \cdots H_{\tau(n)} \), it follows that \( G \) is a Nakajima \( p \)-group.

\( \square \)