INVERSE DEFORMATION PROBLEMS FOR SPECIAL LINEAR AND SYMPLECTIC GROUPS

Timothy Allen Eardley

A thesis submitted for the degree of Doctor of Philosophy

School of Mathematics and Statistics,
University of Sheffield

November 2015

Contents

Abstract

The principal result of this thesis is an affirmative answer to the inverse deformation problem which asks: Does a given complete noetherian local ring have a realisation as the unrestricted universal deformation ring of any residual representation? This is proved in two ways: firstly a complete answer is given using the family of special linear groups over complete noetherian local rings and secondly, if the finite field is not $\mathbb{F}_3$ or does not have characteristic 2, it is answered using the family of symplectic groups.

Of central importance to the result in the symplectic case is the establishment of a structure theorem for subgroups of special linear groups which surject onto symplectic groups over finite fields.

Chapter 1

Introduction

1.1 Universal Deformations

The central objects required for a precise formulation of the main results are deformations of profinite groups. As a pre-requisite to this, we outline some basic group theory and ring theory.

We commence by describing the algebraic construction of profinite groups of which a thorough exposition may be found in Chapter 1 of [21]. To this end, we introduce the notion of an inverse system of groups:

Let I be a directed partially ordered set which is the indexing set both for a collection of groups $\{G_i \mid i \in I\}$ and a collection of homomorphisms between these groups $\{\varphi_{ij} : G_i \to G_j \mid i \geq j \in I\}$. This collection of groups and homomorphisms between them constitute an *inverse system of groups* if the following hold:

(i) φ_{ii} is the identity

(ii) $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ for all $i \geq j \geq k \in I$.

An inverse system of groups is written $\{G_i, \varphi_{ij}\}$. Now suppose H is a group accompanied by a collection of homomorphisms $h_i : H \to G_i$ for each index i of I. If $\varphi_{ij} \circ h_i = h_j$ for all $i \geq j$ then the h_i are *compatible* with $\{G_i, \varphi_{ij}\}$. This leads us to the following definition.

Definition 1.1.1. A group G with homomorphisms g_i compatible with an inverse system $\{G_i, \varphi_{ij}\}$ is the *inverse limit* if G is universal in the following sense. Suppose H is another group with homomorphisms h_i compatible with $\{G_i, \varphi_{ij}\}$ then there exists a unique homomorphism $h : H \to G$ such that $g_i \circ h = h_i$.

The inverse limit of an inverse system $\{G_i, \varphi_{ij}\}$ will be written as $\varprojlim G_i$. With this construction in place we make the following definition.

Definition 1.1.2. A group which is the inverse limit of an inverse system of finite groups is called profinite.

Profinite groups have a natural topology which is defined by specifying that subgroups of finite index are open. The topology of these groups is also explained in detail in Chapter 1 of [21].

Next, we continue by introducing some basics of local ring theory. Let $\mathbb{F}_q$ be the finite field with q elements. Thus $q = p^d$ where p is a prime number denoting the characteristic of $\mathbb{F}_q$ and d is a positive integer. The letter k will be used to denote a choice of finite field.

We denote by (A, m_A) a local ring, i.e. a non-zero commutative ring with a unique maximal ideal m_A. The ring (A, m_A) is a noetherian local ring if in addition its ideals satisfy the ascending chain condition i.e. all chains of ideals of A of the form:

$$I_1 \subseteq I_2 \subseteq \dots$$

eventually become stationary which means that there exists a positive integer d such that for all integers e greater than d there is the equality $I_d = I_e$.

Now we define the notion of the completion of a local ring.

Definition 1.1.3. Let (A, m_A) be a local ring then its completion is the ring $\hat{A} := \varprojlim(A/m_A^i)$ where i is interpreted as both a power and as a member of the indexing set $\mathbb{N}$.

If $A = \hat{A}$ i.e. A is its own completion, then A is called *complete*.

For a fixed finite field k the set of all complete noetherian local rings with residue field k form the objects of a category denoted by $\mathcal{C}(k)$. These rings are either written A or (A, m_A) if the maximal ideal is to be explicitly specified. The morphisms in $\mathcal{C}(k)$ are *local ring homomorphisms*: if A and B are two rings in $\mathcal{C}(k)$, a ring homomorphism $A \to B$ is a local ring homomorphism if the inverse image of m_B is m_A and the induced map on residue fields is an isomorphism.

The following result, from [25], links our discussions on complete noetherian local rings and profinite groups.

Lemma 1.1.4. *If A belongs to $\mathcal{C}(k)$, then $GL_n(A)$ is a profinite group.*

Finally, we pass further comment on the structure of the elements of $\mathcal{C}(k)$. Let k be a fixed finite field and denote the ring of Witt vectors over k by $W := W(k)$ (for a detailed account of its construction see Section 2.6 of [30]). Every element (A, m_A) in $\mathcal{C}(k)$ is endowed with the structure of a W-algebra in the sense that given a field homomorphism $\bar{\phi} : k \to A/m_A$ there is a unique local ring homomorphism $\iota_A : W \to A$ which induces $\bar{\phi}$ on the residue fields. The image of ι_A is of particular significance and so we define

$$W_A = \iota_A(W). \tag{1.1.1}$$

Also of importance will be the quotients of W by powers of the ideal (p) and so we make the definition:

$$W_r = W/p^r. \tag{1.1.2}$$

We are ready now to introduce the deformation theory of profinite groups and for the rest of this section Γ will denote a fixed choice of profinite group. To begin we require the notion of a *residual representation* of Γ which is a continuous homomorphism

$$\bar{\rho} : \Gamma \to GL_n(k).$$

We will study $\bar{\rho}$ by considering how it may be deformed to other rings in $\mathcal{C}(k)$. The concept is formalised precisely by the notion of deformations which we now describe.

Definition 1.1.5. For a fixed residual representation $\bar{\rho}$ of Γ a lifting of $\bar{\rho}$ to a ring A in $\mathcal{C}(k)$ is a representation of the form

$$\rho : \Gamma \to GL_n(A)$$

such that there is the following commutative diagram

$$\begin{array}{ccc} & & GL_n(A) \\ & \overset{\rho}{\nearrow} & \downarrow m \\ \Gamma & \xrightarrow{\bar{\rho}} & GL_n(k) \end{array}$$

where $m : GL_n(A) \to GL_n(k)$ is the group homomorphism which is componentwise reduction modulo m_A.

A deformation of $\bar{\rho}$ to A is an equivalence class of liftings where two liftings ρ_1, ρ_2 of $\bar{\rho}$ to A are equivalent if there exists an element T of $GL_n(A)$ in the kernel of m so that for all g in $GL_n(A)$:

$$T\rho_2(g)T^{-1} = \rho_1(g).$$

Moreover, if ρ is a given lifting of $\bar{\rho}$ then the deformation to which it belongs is denoted $[\rho]$.

We will require that our residual representations are absolutely irreducible and so we define this concept:

Let K/k be a finite extension of fields and let $\iota : k \to K$ be the inclusion of fields, thus $\iota \circ \bar{\rho} : \Gamma \to GL_n(K)$ is another representation of Γ. If $\bar{\rho}$ is irreducible and $\iota \circ \bar{\rho}$ is irreducible for all K then $\bar{\rho}$ is called *absolutely irreducible.*

All is now in place to state the next result by Mazur which is Proposition 1 of Section 1.2 in [18] and is fundamental to the deformation theory of profinite groups. We note that this result introduces universal deformations and universal deformation rings.

Theorem 1.1.6. *Let Γ be a profinite group with the property that for every open subgroup $\Gamma_0 < \Gamma$ of finite index the number of continuous homomorphisms from Γ_0 to $\mathbb{F}_p$ is finite. In addition, let $\bar{\rho} : \Gamma \to GL_n(k)$ be a representation.*

Then there exist: a ring $R := R(\bar{\rho})$ and a deformation $[\rho_R] : \Gamma \to GL_n(R)$; so that for each lifting $\rho : \Gamma \to GL_n(A)$ there is a local ring homomorphism $\pi : R \to A$ which makes the following diagram commute.

$$\begin{array}{ccc} & & GL_n(R) \\ & & \downarrow \pi \\ & \overset{[\rho_R]}{\nearrow} & GL_n(A) \\ & \overset{\rho}{\nearrow} & \downarrow m \\ \Gamma & \xrightarrow{\bar{\rho}} & GL_n(k) \end{array}$$

Furthermore, if $\bar{\rho}$ is absolutely irreducible R, $[\rho_R]$ and π are unique. If this is the case, R is called the universal deformation ring and $[\rho_R]$ the universal deformation.

We remark that if $\bar{\rho} : \Gamma \to GL_n(k)$ is irreducible the condition of absolute irreducibility is equivalent to the centraliser of $\bar{\rho}(\Gamma)$ in $M_n(k)$ consisting of scalar matrices, where $M_n(k)$ denotes the $n \times n$ matrices with coefficients in k (see Theorem 9.2 of [17]).

1.2 Main Results

The principal result of this thesis is to provide an affirmative answer to the *inverse deformation problem* which asks:

Inverse Deformation Problem. *Which complete noetherian local rings have a realisation as the unrestricted universal deformation ring of some residual representation?*

More precisely, let A be a fixed choice of ring in $\mathcal{C}(k)$. Does there exist a profinite group Γ and a representation $\bar{\rho} : \Gamma \to GL_n(k)$ with a universal deformation ring equal to A?

Note that in this formulation of the inverse deformation problem there are no restrictions on what Γ or n may be.

The question in its current formulation was posed by Bleher, Chinburg and De Smit in [6] although its origins lie in an earlier form raised by Flach in [9].

Now an overview of the developments in this area is given. Recall that k is a fixed finite field of prime characteristic p and W is the Witt ring of k. As mentioned above, the inverse deformation problem stems from a question in [9]. This question asked if it is possible for an unrestricted universal deformation ring not to be a complete intersection. This was first answered by Bleher and Chinburg in [3] (also see [4]) where if k has characteristic 2 rings of the form $W[[t]]/(t^2, 2t)$ were proven to be deformation rings. Bleher, Chinburg and De Smit then greatly extended this first example to encompass all rings of the form $W[[t]]/(p^n t, t^2)$ in [5] with no restrictions on k. Then in [6] the same three authors provided a complete categorisation of possible deformation problems with these deformation rings.

In [24] Rainone showed that rings of the form

- $\mathbb{Z}_p[[t]]/(p^n, p^m t)$ for $p > 3$ and $n > m$
- $\mathbb{Z}/p^n\mathbb{Z}$ for $p \geq 5$

are universal deformation rings. For an expanded account of the progress specifically regarding rings which are not complete intersections refer to [6].

At this point we reflect on the achievements of Rainone contextualising them within the work of this thesis, [12] - the joint paper by this author and Manoharmayum and the work of Dorobisz [11] which is discussed in more detail below. In [24] , Rainone made the first use of a so-called standard representation: the $\bar{\rho}$ in the following result which is Theorem 3.1.1 in [24]:

Theorem 1.2.1. *Let $p \geq 5$ be a prime, $\Gamma := GL_2(\mathbb{F}_p)$ and $\bar{\rho} : \Gamma \xrightarrow{\cong} GL_2(\mathbb{F}_p)$. Then $\mathbb{F}_p$ is the universal deformation ring for this deformation problem.*

In [16] Manoharmayum used an identity representation on the rings $W_r = W/(p^r)$ to show that W_r where k has cardinality greater than 3 are universal deformation rings in the next result:

Theorem 1.2.2. *Let k be a finite field of cardinality greater than or equal to 4 and let $n \geq 2$ be an integer subject to the restrictions:*

- *If $k = \mathbb{F}_5$ then $n \neq 2$*
- *If $k = \mathbb{F}_4$ then $n \neq 3$.*

In addition let $\Gamma := SL_n(W_r)$ and $\bar{\rho} : \Gamma \to GL_n(k)$ be reduction modulo p of the standard representation $\rho_{W_r} : \Gamma \to SL_n(W_r)$.

Then W_r is the universal deformation ring for the deformation problem defined by Γ and $\bar{\rho}$.

We reflect in more detail on the results and methods of [16]: the quoted deformation ring proof is a simple consequence of the paper's main result which through a sophisticated cohomological argument describes the structure of certain subgroups of general linear groups over complete noetherian local rings. In [12] (the author's joint work with Manoharmayum) the application of the method of Manoharmayum's Theorem 1.2.2 above was greatly extended to show that all complete noetherian rings are universal deformation rings, thus providing the first complete affirmative answer to the inverse deformation problem. To be more precise, the following result was proved in [12].

Theorem 1.2.3. *Let k be a finite field of characteristic p. Then every element of $\mathcal{C}(k)$ is a universal deformation ring.*

More precisely, let $(A, m_A) \in \mathcal{C}(k)$ and $\Gamma := SL_n(A)$ with $n \geq 3$. Furthermore, if $k = \mathbb{F}_2$ also assume that $n \geq 5$. Now, let $\bar{\rho} : \Gamma \to GL_n(k)$ be the componentwise reduction modulo m_A of the identity representation $\rho_A : \Gamma \xrightarrow{\cong} SL_n(A)$. Then ρ_A is the universal deformation and A the universal deformation ring for the deformation problem defined by Γ and $\bar{\rho}$.

In this thesis, the method of [12] is extended to include SL_2. Namely, we prove the following result.

Main Theorem 1. *Let k be a finite field with characteristic p. Then every element of $\mathcal{C}(k)$ is an unrestricted universal deformation ring.*

More precisely, let: $A \in \mathcal{C}(k)$, $\Gamma = SL_n(A)$ and $\bar{\rho} : \Gamma \to GL_n(k)$ be reduction modulo m_A of the standard representation $\rho_A : \Gamma \to SL_n(A)$ where n is subject to the restrictions:

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ or $k = \mathbb{F}_5$ then $n \geq 3$.*

Then ρ_A is the universal deformation and A the universal deformation ring for the deformation problem defined by Γ and $\bar{\rho}$.

At this point we remark that Main Theorem 1 is an improved version of Theorem 1.2.3 above (which is the Main Theorem in [12]) extended to include the case where $n = 2$ and $A \in \mathcal{C}(k)$ with $k \notin \{\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5\}$.

To complete this overview we remark that the unrestricted inverse deformation problem was independently answered by Dorobisz in [11] which appeared shortly after [12]. In [11] Dorobisz investigates the same deformation problem (i.e. where $\Gamma := SL_n(A)$, $\rho_A : \Gamma \xrightarrow{\cong} SL_n(A)$ and $\bar{\rho} : \Gamma \to SL_n(k)$ is componentwise reduction modulo m_A) but uses an approach not involving cohomology but rather relying solely on properties of special linear groups. The principal result of [11] phrased in the language and notation of this work is the following:

Theorem 1.2.4. *Let $A \in \mathcal{C}(k)$ where k is a finite field, $\Gamma := SL_n(A)$ and $\bar{\rho} : \Gamma \to GL_n(k)$ be reduction modulo m_A of the standard representation $\rho_A : \Gamma \to SL_n(A)$ where n is subject to the restrictions*

- *If $k = 2$ then $n \geq 4$*
- *If $k = \mathbb{F}_3$ or $k = \mathbb{F}_5$ then $n \geq 3$.*

Then ρ_A is the universal deformation and A the universal deformation ring for the deformation problem defined by Γ and $\bar{\rho}$.

Especially noteworthy is the inclusion above of the case $n = 4$ and $k = \mathbb{F}_2$ which is not included in Main Theorem 1 (or in Theorem 1.2.3 - the result from [12]).

The method in this thesis and [12] utilisies cohomological properties of special linear groups and as certain symplectic groups share these cohomological properties our method produces analagous results within the context of these groups as well.

This brings us to survey other significant results of this thesis. The first is the following theorem, a crucial component in the proof of Main Theorem 1, which describes the important subgroup structure of GL_n over complete noetherian local rings.

Theorem 1.2.5. *Let (B, m_B) be an element of $\mathcal{C}(k)$. Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$*

and let G be a subgroup of $SL_n(B)$. Assume that $G \bmod m_B = SL_n(k)$. Then there exists an $X \in GL_n(B)$ satisfying $X \equiv I \bmod m_B$ such that $SL_n(W_B) \subseteq XGX^{-1}$.

We remark that this result is an extension of Manoharmayum's Main Theorem of [16] which proved the result for finite fields with cardinality greater than or equal to 4 and let $n \geq 2$ subject to the restrictions:

- If $k = \mathbb{F}_5$ then $n \neq 2$
- If $k = \mathbb{F}_4$ then $n \neq 3$.

This result of [16] was then extended by Manoharmayum and Eardley in [12] to include:

- $k = \mathbb{F}_3$ when $n \geq 3$
- $k = \mathbb{F}_2$ when $n \geq 5$.

Thus Theorem 1.2.5 collates the results of [16] and [12].

The second significant result (motivated by the observation that in addition to belonging to the family of special linear groups the groups $SL_2(A)$ also belong to the family of symplectic groups) extends the principles of the cohomological argument of [16] to a more complicated setting. This result, Main Theorem 3 in Chapter 8, provides an analogue of Theorem 1.2.5 for subgroups of $GL_n(B)$ containing $SL_n(W_B)$ subject to the restrictions:

- If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$
- If $n \geq 2$ then $p \geq 3$, the cardinality of k is greater than or equal to 5 and n is coprime to p.

The third, Main Theorem 2 in Chapter 8, uses Main Theorem 3 to prove that subject to the restrictions

- k does not have characteristic 2
- $k \neq \mathbb{F}_3$

all rings A in $\mathcal{C}(k)$ are universal deformations rings, i.e. the inverse deformation problem may also be answered by symplectic groups. Thus a family of smaller (in the sense of inclusion of groups) groups which answer the inverse deformation problem is provided.

The fourth, Main Theorem 4 in Chapter 14, applies the methods used for symplectic groups in a new setting; that of symplectic deformations. This situation is considerably simpler and after proving another analogous structural result we show that, excepting the restrictions on p and k the *inverse symplectic deformation problem* also has an affirmative answer.

Finally, we make reference to some results which here play an intermediary role but may be of independent interest:

- in Theorem 12.0.7 part (i) from Chapter 12 we prove that $H^1(SP_{2n}(W_r), \mathfrak{M}_0) = (0)$ subject to some restrictions on p, q and n.
- in Main Theorem 3 we prove a symplectic analogue to Theorem 1.2.5.

- in Main Theorem 4 of Chapter 14 the deformation problem associated with $\bar{\rho} : SL_2(A) \to SL_2(k)$ given by reduction modulo m_A is generalised in a different fashion. This time it is considered as a symplectic deformation i.e. as a representation in the form $\bar{\rho} : \Gamma \to SP_{2n}(k)$ and where deformations of $\bar{\rho}$ are of the form $\rho : \Gamma \to SP_{2n}(A)$. The final result mentioned here answers the so-called *inverse symplectic deformation problem*: Which rings in $\mathcal{C}(k)$ have a realisation as a universal deformation ring to a symplectic deformation?

1.3 Thesis Outline

The thesis essentially comprises two parts. The first part, chapters 2-7, are dedicated to proving Main Theorem 1 thus answering the inverse deformation problem for all complete noetherian local rings. This is achieved by considering identity representation of special linear groups over rings in $\mathcal{C}(k)$ and residual representations induced from componentwise reduction modulo maximal ideal. Of central importance to the argument is the invocation of Theorem 1.2.5 which allows us to assume that a representative of the deformation class contains $SL_n(W_A)$.

In Chapter 2 we state and investigate the relevant group theoretic properties of SL_n over complete noetherian local rings. Then in Chapter 3 we complete the proof of Main Theorem 1 subject to proving Theorem 1.2.5.

Thus all that remains in this part is to prove Theorem 1.2.5, to this end in Chapter 4 we provide background material on group cohomology and extensions. This leads us to an examination of the submodule structure of $kSL_n(W_r)$-modules in Chapter 5 and the calculation of the relevant cohomological groups for $kSL_n(W_r)$-modules in Chapter 6. Then, with all this in place, we finish the proof of Theorem 1.2.5 in Chapter 7.

In the second part of the thesis (Chapters 8-14) the focus is on deformation problems of symplectic groups. More specifically, in Chapters 9-13 we prove Main Theorem 2 providing (with a few exceptions) another class of groups which answer the inverse deformation problem. The model for the proof of Main Theorem 2 follows that for SL_n. Namely, we begin with a discussion of the relevant group theoretic properties of SP_{2n} over complete noetherian local rings. Then we assume the result of Main Theorem 3 to complete the proof of Main Theorem 2 in Chapter 10. As before, all that is now required is to prove Main Theorem 2 hence in Chapter 11 we examine the submodule structure of $kSP_{2n}(W_r)$-modules and in Chapter 12 we make the necessary calculations of cohomological groups of $kSP_{2n}(W_r)$-modules. This allows us to complete the proof of Main Theorem 3 in Chapter 13.

Finally, in Chapter 14 we utilise the work of previous chapters to provide an answer for the symplectic deformation problem, i.e. we prove Main Theorem 4.

Chapter 2

Special Linear Groups

The main objective of this chapter is to collect the group theoretic and structural properties of special linear groups over rings in $\mathcal{C}(k)$ required for the deformation ring calculations in Chapter 3. In addition, some results from this chapter are used to determine $kSL_n(k)$-modules and module homomorphisms in Chapter 5.

In Section 2.1 elementary matrices are introduced and a well known generating set for SL_n over complete local rings is established. Then in Section 2.2 the Steinberg relations for elementary matrices are used to determine which special linear groups over local rings are perfect. Finally, Section 2.3 identifies the subgroup of signed permutations in SL_n and derives a number of elemental consequences and related results. However, we begin by fixing the notation used.

For (A, m_A) in $\mathcal{C}(k)$: the set of $n \times n$ matrices over A is denoted $M_n(A)$; and the familiar general linear and special linear groups of dimension n over A are denoted $GL_n(A)$ and $SL_n(A)$ respectively. In each of these groups the identity element will simply be written I: its dependence on n being suppressed.

2.1 Elementary Matrices

Let (A, m_A) belong to $\mathcal{C}(k)$ and $n \geq 2$ be an integer. For all pairs of integers (i, j) in the range $1 \leq i, j \leq n$ the matrix units are defined to be the elements of $M_n(A)$ which have a 1 in the (i, j)-th entry and zeros in all others. These matrices are denoted e_{ij} and their multiplication is governed by the formula $e_{ij}e_{kl} = \delta_{jk}e_{il}$ where δ_{jk} is the Kronecker Delta i.e.

$$\delta_{jk} := \begin{cases} 1 & \text{if } j = k \\ 0 & \text{if } j \neq k. \end{cases}$$

Furthermore, as $n \geq 2$ this allows us to choose distinct indices i and j as above and make the definition

$$E_{ij}(\lambda) = I + \lambda e_{ij}.$$

Elements of this form are called *elementary matrices* and clearly belong to $SL_n(A)$. The elementary matrices generate a subgroup of $SL_n(A)$ denoted by $E(n, A)$. Next we present the following result, which is essentially Whitehead's Lemma.

Lemma 2.1.1. *Let a belong to $A^\times$. There is the identity:*

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = E_{21}(a^{-1})E_{12}(1-a)E_{21}(-1)E_{12}(1-a^{-1}).$$

More generally, the diagonal matrix which differs from the identity only in that its (i,i)-th entry is a and its (j,j)-th entry is a^{-1} may be expressed as the following product of elementary matrices:

$$E_{ji}(a^{-1})E_{ij}(1-a)E_{ji}(-1)E_{ij}(1-a^{-1}).$$

The next theorem is a special case of result 1.2.11 in [13] and holds in the more general setting of Euclidean domains. The theorem shows that over finite fields elementary matrices generate the special linear group.

Theorem 2.1.2. *If k is a finite field then $E(n,k) = SL_n(k)$.*

The following corollary extends the conclusion of the theorem to all complete local rings, hence in particular to all the elements of $\mathcal{C}(k)$.

Corollary 2.1.3. *If A is a complete local ring then $E(n,A) = SL_n(A)$.*

Proof. As each of the $E_{ij}(\lambda)$ belong to $SL_n(A)$ it is clear that $E(n,A)$ is a subgroup of $SL_n(A)$ therefore we must show the converse as well. The method is to show that for an arbitrary element g of $SL_n(A)$ there exist two products of elements of $E(n,A)$, L and R, such that $LgR = I$. This would then imply that $g = L^{-1}R^{-1}$ and thus clearly belongs to $E(n,A)$.

Let $g \in SL_n(A)$ and let $\bar{g}$ be the element of $SL_n(k)$ obtained from g by componentwise reduction modulo m_A. Then, as a consequence of the theorem above, there exist $\bar{L}$ and $\bar{R}$ in $E(n,k)$ such that $\bar{L}\bar{g}\bar{R} = I$. These matrices can be lifted to L and R in $SL_n(A)$ so that $LgR \equiv I \bmod m_A$. Therefore we have reduced to the case of elements of $SL_n(A)$ with the form $g = I + M$ where M is a $n \times n$ matrix with entries in m_A.

The next step is to show that by the multiplication of suitable matrices on the left $I + M$ may be assumed diagonal. This is completed for each row individually; therefore we choose the r-th row to focus on and form the product:

$$\left(\prod_{i\neq r} E_{ri}(\lambda_i)\right)(I+M) = I + M + \sum_{i\neq r}\left(\lambda_i(1+m_{ii})e_{ri} + \lambda_i\sum_{y\neq i} m_{iy}e_{ry}\right). \quad (2.1.1)$$

Let s be an index different from r and consider the (r,s)-th coefficient of the right-hand side of the equation above. This is:

$$m_{rs} + \lambda_s(1+m_{ss}) + \sum_{i\neq r,s}\lambda_i m_{is}.$$

If we set:

$$\lambda_s = -(1+m_{ss})^{-1}[m_{rs} + \sum_{i\neq r,s}\lambda_i m_{is}]$$

then the (r, s)-th coefficient of equation (2.1.1) is zero. Therefore by choosing the appropriate value for each λ_s we find that, with the exception of the (r, r)-th entry, the r-th row of equation (2.1.1) consists of zeros. This process may be continued over all values of r. Hence replacing λ_i with $\lambda_i^{(r)}$ to reflect the dependence of these scalars on r implies that

$$N := \left(\prod_{r=1}^{n} \left(\prod_{i \neq r} E_{ri}(\lambda_i^{(r)}) \right) \right) (I + M)$$

is a diagonal matrix. Furthermore, each of these diagonal entries are units because, as a product of elements of $SL_n(A)$, N is invertible.

Therefore we may write $N = \text{diag}((n_i))$. Now define a set u_i of units in the ring A and a corresponding set of elements of $SL_n(A)$ by:

$$u_i := \prod_{r=1}^{i} n_r^{-1}, \quad W_i := E_{i+1,i}(u_i^{-1}) E_{i,i+1}(1 - u_i) E_{i+1,i}(-1) E_{i,i+1}(1 - u_i^{-1}).$$

Lemma 2.1.1 implies that W_i is diagonal with: u_i in the (i, i)-th position, u_i^{-1} in the $(i + 1, i + 1)$-th position and 1s on the remaining diagonal entries. With this in place we form the product

$$\left(\prod_{i=1}^{n-1} W_i \right) N$$

of which the first $n - 1$ diagonal entries are 1; this follows directly from the definitions of u_i and W_i. The (n, n)-th entry is

$$\prod_{i=1}^{n} n_i$$

which must also equal 1 because N belongs to $SL_n(A)$ and this product is thus an expression of its determinant. □

2.2 Commutator Subgroups of Special Linear Groups

In this section the notions of a derived group and a perfect group are introduced and explored within the context of special linear groups. Let g and h be two arbitrary elements of G then their commutator is

$$[g, h] := ghg^{-1}h^{-1}.$$

The set of all commutators of G generates a normal subgroup called the *derived group* of G denoted by $[G, G]$. If the commutators generate the whole of G then G is called *perfect*.

This leads us to considering representations of perfect groups.

Proposition 2.2.1. *Let $\rho : G \to GL_n(A)$ be a group homomorphism. If G is a perfect group then the image of ρ is in fact contained in $SL_n(A)$.*

Proof. As G is perfect it suffices to show that the images of commutators have determinant equal to 1. Let $g = [g_1, g_2]$ then by the multiplicative property of the group homomorphisms ρ and det:

$$\det(\rho(g)) = \det([\rho(g_1), \rho(g_2)]) = I.$$

□

The commutator relations for special linear groups play an important role in our deformation ring calculations. This brings us to the following lemma, known as the Steinberg relations, a discussion of which is found in Chapter 5 of [20].

Lemma 2.2.2. *Let $n \geq 3$. The elementary matrices satisfy the following, which are called the Steinberg relations:*

(a) $E_{ij}(x)E_{ij}(y) = E_{ij}(x + y)$,

(b) $[E_{ij}(x), E_{jk}(y)] = E_{ik}(xy)$ *if* $i \neq k$

(c) $[E_{ij}(x), E_{kl}(y)] = I$ *if* $i \neq l, j \neq k$.

If $n \geq 3$ then the elementary matrices in conjunction with the Steinberg relations specify $SL_n(A)$. However, if $n = 2$ the relations (b) and (c) are vacuous and so in this case these relations are insufficient. Fortunately, Lemma 2.1.1 may be used to determine which of the SL_2 over complete local rings are perfect.

Lemma 2.2.3. *Let (A, m_A) be in $\mathcal{C}(k)$ where k has q elements. Then if the pair (n, q) is neither $(2, 2)$ nor $(2, 3)$ the group $SL_n(A)$ is perfect.*

Proof. When $n \geq 3$ Lemma 2.2.2 (b) shows that each elementary matrix is a commutator, hence the conclusion follows from Corollary 2.1.3.

If $n = 2$ the restriction $q \geq 4$ implies that there exists an element a in $A^\times$ such that $a^2 \neq 1$, which we use to define the following element of $SL_2(A)$:

$$w := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Then there are the commutator relations

$$E_{12}(b) = [w, E_{12}(b(a^2 - 1)^{-1})] \tag{2.2.1}$$
$$E_{21}(b) = [w, E_{21}(b(a^2 - 1)^{-1})] \tag{2.2.2}$$

which together with Corollary 2.1.3 complete the proof when $q > 3$. □

2.3 Permutation Matrices

In this section certain signed permutation matrices are identified which allow us to conjugate elementary matrices to each other by elements of $SL_n(W_A)$. With this in mind recall that the symmetric group S_n can be identified with a subgroup of $GL_n(\mathbb{Z})$ in a natural fashion. We note that for A in $\mathcal{C}(k)$, the unique homomorphism $\mathbb{Z} \to A$ defines a subring of A which is also a subring of W_A and if extended componentwise determines a subgroup of $SL_n(W_A)$ via $SL_n(\mathbb{Z}) \to SL_n(A)$.

Let x be an arbitrary element of A. We will need to conjugate, using elements of $SL_n(W_A)$ exclusively, the elementary matrix $E_{1n}(x)$ to each of the other matrices of the form $E_{ij}(x)$. From the discussion above it is clear that it is sufficient to find suitable matrices belonging to $SL_n(\mathbb{Z})$. This leads us to signed permutation matrices.

Definition 2.3.1. Let $1 \leq r, s \leq n$ with $r \neq s$ and define

- $(rs) \in GL_n(\mathbb{Z})$ to be the permutation matrix which differs from the identity only in that its r-th and s-th rows have been transposed,
- $D_r \in GL_n(\mathbb{Z})$ to be the diagonal matrix that differs from the identity only in its (r,r)-th entry which is -1.

The notation (rs) intentionally suggests the familiar notation of transpositions in S_n. It is clear that the matrices (rs) and D_r all have determinant -1 and thus do not belong to $SL_n(\mathbb{Z})$. However, a product of any two of these elements will have determinant 1 and thus belongs to $SL_n(\mathbb{Z})$.

Now let $n \geq 3$. Given $1 \leq i, j \leq n$ with $i \neq j$ we define the following collection of signed permutations $T_{ij} \in SL_n(\mathbb{Z})$ by:

$$T_{ij} := \begin{cases} I & \text{if } (i,j) = (1,n), \\ D_2(1n) & \text{if } (i,j) = (n,1), \\ D_n(jn) & \text{if } i = 1 \text{ and } j \neq n, \\ D_1(1i) & \text{if } i \neq 1 \text{ and } j = n, \\ (1i)(nj) & \text{if } i \neq 1 \text{ and } j \neq n \text{ and } (i,j) \neq (n,1) \end{cases} \tag{2.3.1}$$

This brings us to the following result.

Proposition 2.3.2. *Let $A \in \mathcal{C}(k)$ and $n \geq 2$ be an integer.*

(i) Suppose $X \in GL_n(A)$. Then $XE_{ij}(1) = E_{ij}(1)X$ for all elementary matrices $E_{ij}(1)$ with $1 \leq i < j \leq n$ if and only if $X = \lambda E_{1n}(x)$ for some $\lambda \in A^\times$, $x \in A$.

(ii) $T_{ij}E_{1n}(x)T_{ij}^{-1} = E_{ij}(x)$ for all $1 \leq i \neq j \leq n$ and $x \in A$.

Proof. For (i): if $n \geq 3$ the Steinberg relations (Proposition 2.2.2 (c)) imply that $\lambda E_{1n}(x)$ commutes with $E_{ij}(1)$ for $1 \leq i < j \leq n$, if $n = 2$ this is equivalent to

$E_{12}(x)E_{12}(y) = E_{12}(y)E_{12}(x)$. In the opposite direction, suppose X commutes with $E_{ij}(1)$. Then the relation $E_{ij}(1)X = XE_{ij}(1)$ implies

$$\sum_{m=1}^{n} x_{jm}e_{im} = \sum_{m=1}^{n} x_{mi}e_{mj}.$$

From which it is clear that: $x_{jj} = x_{ii}$, the non-diagonal entries of the j-th row are zero and the non-diagonal entries of the i-th column are zero. By varying over all permissible values of the pair (i, j) the conclusion follows.

For part (ii): we note that by the definition of (rs) it is clear that multiplication with (rs) on the right, respectively left, swaps the r-th and s-th rows, respectively columns. It is also clear that multiplication with D_r on the right, respectively left, multiplies by -1 the entries in the r-th row, respectively r-th column. We conclude by observing that in each of the middle three products of equation (2.3.1) the subscript of D_r has been chosen distinct from i and j. □

Corollary 2.3.3. *If $n \geq 3$ and $A \in \mathcal{C}(k)$ then:*

$$T_{ij}(xe_{1n})T_{ij}^{-1} = xe_{ij} \text{ for all } 1 \leq i \neq j \leq n \text{ and } x \in A. \tag{2.3.2}$$

Furthermore, given any two pairs of indices $i \neq j$ and $k \neq l$, e_{ij} may be conjugated by elements of $SL_n(W_A)$ to e_{kl}; and $e_{ii} - e_{jj}$ may also be conjugated by elements of $SL_n(W_A)$ to $e_{kk} - e_{ll}$.

If $n = 2$ then e_{12} may be conjugated to $-e_{12}$ by the element $D_2(12)$ of $SL_n(W_A)$ (see Definition 2.3.1 for the definitions) and vice versa.

Proof. The observation of (2.3.2) follows from Proposition 2.3.2 (ii) as is demonstrated by the equality:

$$\begin{aligned} I + xe_{ij} &= T_{ij}(I + xe_{1n})T_{ij}^{-1} \\ &= I + T_{ij}(xe_{1n})T_{ij}^{-1}. \end{aligned}$$

For the next claim we note that $T_{ij}^{-1}e_{ij}T_{ij} = e_{1n}$ by Proposition 2.3.2 (ii). Then e_{1n} may be conjugated to e_{kl} by the argument above. Next, we observe that $T_{ij}^{-1}(e_{ii} - e_{jj})T_{ij} = e_{11} - e_{nn}$ and the argument follows similarly.

If $n = 2$ then the matrix $D_2(12)$, see Definition 2.3.1 for the definitions, may be used to effect the conjugations.

□

Chapter 3

Skeleton Proof

3.1 The Main Argument

In this section the main thrust of the argument proving Main Theorem 1 is presented. In so doing, certain technical elements are left until later. We begin by establishing the notation used.

Let k be a fixed choice of finite field, (A, m_A) a fixed element of $\mathcal{C}(k)$ and $n \geq 2$ an integer subject to the restrictions:

- If $k = \mathbb{F}_2$ then $n \geq 5$
- If $k = \mathbb{F}_3$ or $\mathbb{F}_5$ then $n \geq 3$.

We then define $\Gamma = SL_n(A)$, $\rho_A : \Gamma \xrightarrow{\cong} SL_n(A)$ to be the identity representation (i.e. given by a fixed choice of isomorphism) and $\bar{\rho} : \Gamma \to GL_n(k)$ to be componentwise reduction modulo m_A of ρ_A.

Lemma 3.1.1. *The residual representation $\bar{\rho}$ given above is absolutely irreducible.*

Proof. We begin by observing that $\bar{\rho} : SL_n(A) \to SL_n(k)$ is clearly surjective.

Next, we show that $\bar{\rho}$ is irreducible. This is equivalent to showing that the n-dimensional vector space k^n has no non-trivial subspaces. Let $v = (v_1, \ldots, v_n)$ be an arbitrary element of k^n. Also let $1 \leq i, j \leq n$ be distinct integers and consider the action of $E_{ij}(1)$ on v. If v is fixed by $E_{ij}(1)$ then equating this with v and looking at the i-th components implies $v_i = v_i + v_j$. Therefore the component v_j must be zero and continuing by running through all permissible values of i and j the result follows.

Finally, recall that as $\bar{\rho} : \Gamma \to GL_n(k)$ is irreducible the condition of absolute irreducibility is equivalent to the centraliser of $\bar{\rho}(\Gamma)$ in $M_n(k)$ consisting of scalar matrices (see Theorem 9.2 of [17]). The first part of Proposition 2.3.2 implies that an element in the centre of $SL_n(k)$ could have the form $\lambda E_{1n}(x)$. However, as such an element also commutes with $E_{n1}(1)$, x must be zero. □

Therefore, invoking Theorem 1.1.6 we have proved the following.

Corollary 3.1.2. *For the deformation problem defined by Γ and $\bar{\rho}$ (as above) there exists a universal deformation ring R and a universal deformation ρ_R (see Theorem 1.1.6).*

Now for a simple observation about the images of the deformations introduced here.

Corollary 3.1.3. *For the deformation problem defined by Γ and $\bar{\rho}$ (as above) the following hold:*

- *the image $\rho_R(\Gamma) \subseteq SL_n(A)$.*
- *the image $\bar{\rho}(\Gamma) \subseteq SL_n(k)$.*

Proof. Lemma 2.2.3 tells us that Γ is perfect therefore the result follows from Proposition 2.2.1. □

Recall from Theorem 1.1.6 the existence of a unique local ring homomorphism $\pi : R \to A$ for which $\pi \circ \rho_R$ is strictly equivalent to ρ_A and recall that $m : A \to k$ is componentwise reduction modulo m_A. We may summarise the relationships between the deformations $\bar{\rho}$, ρ_A and ρ_R in the commutative diagram below:

$$\begin{array}{ccc} & & SL_n(R) \\ & \overset{\rho_R}{\nearrow} & \downarrow \pi \\ \Gamma & \xrightarrow{\rho_A} & SL_n(A) \\ & \underset{\bar{\rho}}{\searrow} & \downarrow m \\ & & SL_n(k). \end{array}$$

Proof of Main Theorem 1. For clarity the argument is split into three small steps.

Step 1. We begin by observing some characteristics of the universal deformation. Let (R, m_R) together with $\rho_R : \Gamma \to SL_n(R)$ be the universal deformation ring for the deformation problem defined by $\overline{\rho} : \Gamma \to SL_n(k)$. We note that $\rho_R(\Gamma)$ mod $m_R = SL_n(k)$. Therefore, we may invoke Theorem 1.2.5 and upon replacement of ρ_R with a strictly equivalent representation we may assume that $\rho_R(\Gamma)$ contains a copy of $SL_n(W_R)$.

Step 2. We now note that the unique local ring homomorphism $\pi : R \to A$ which is associated with ρ_A by the universal property of R, i.e. so that $\pi \circ \rho_R$ is strictly equivalent to ρ_A, is compatible with W-algebra structure morphisms ι_A and ι_R. This is tantamount to the following commutative diagram:

$$\begin{array}{ccc} & & W_R \\ & \overset{\iota_R}{\nearrow} & \downarrow \pi \\ W & \xrightarrow{\iota_A} & W_A. \end{array} \tag{3.1.1}$$

With this in place, we make the following simple observations of the salient homomorphisms.

Proposition 3.1.4. *With the notation defined above, we have the properties:*

(i) $\rho_R : \Gamma \to SL_n(R)$ *is injective and* $\pi : \rho_R(\Gamma) \to SL_n(A)$ *is an isomorphism.*

(ii) The map $\pi : R \to A$ *is surjective.*

Proof. Part (i) follows from the fact that $\pi \circ \rho_R$ is an equivalent lifting to ρ_A, and that ρ_A is an isomorphism. Part (ii) also follows immediately from these properties. □

Step 3. To complete this outline of the proof we need the following result whose proof is given in the next section.

Proposition 3.1.5. *There exists a local ring homomorphism of elements of* $\mathcal{C}(k)$*, represented by* $s : A \to R$*, which is a section to* $\pi : R \to A$*.*

To complete the proof of Main Theorem 1 we verify that $\rho_A : \Gamma \to SL_n(A)$ is equivalent to the universal deformation. Recall that, by Proposition 2.2.2, the elementary matrices $E_{ij}(x)$ generate $SL_n(A)$. Therefore matrices of the form $E_{ij}(s(x))$ generate $\rho_R(\Gamma)$ where $s : A \to R$ is the section to $\pi : R \to A$ from Proposition 3.1.5. As $\pi \circ s$ is the identity on A this implies the equality:

$$\pi \circ s \circ \pi \circ \rho_R = \pi \circ \rho_R. \tag{3.1.2}$$

We observe that the restriction $\pi|_{\mathrm{Im}(s)}$ is injective and thus may be cancelled in the above compositions of maps. Hence giving the equality:

$$s \circ \pi \circ \rho_R = \rho_R. \tag{3.1.3}$$

From this equality and the universal property of the pair R and ρ_R the map $s \circ \pi : R \to R$ must be the identity on R. Therefore $\pi : R \to A$ is an isomorphism with inverse $s : A \to R$. Finally, as ρ_A is strictly equivalent to $\pi \circ \rho_R$ by the universal property of the pair R and ρ_R, $s \circ \rho_A$ is strictly equivalent to ρ_R. Thus $A \cong R$.

□

3.2 Proof of the Proposition 3.1.5

The prove the existence of the section $s : A \to R$ of Proposition 3.1.5 we require Theorem 1.2.5 which is stated again below for convenience.

Theorem 1.2.5. *Let* (B, m_B) *be an element of* $\mathcal{C}(k)$*. Let* $n \geq 2$ *be an integer,* p *be a prime and* $\mathbb{F}_q$ *be the finite field with* $q = p^d$ *elements. We make the following restrictions on* n *and* k*:*

- *If* $k = \mathbb{F}_2$ *then* $n \geq 5$

- *If* $k = \mathbb{F}_3$ *then* $n \geq 3$
- *If* $k = \mathbb{F}_5$ *then* $n \geq 3$

and let G *be a subgroup of* $SL_n(B)$*. Assume that* $G \bmod m_B = SL_n(k)$*. Then there exists an* $X \in GL_n(B)$ *satisfying* $X \equiv I \bmod m_B$ *such that* $SL_n(W_B) \subseteq XGX^{-1}$*.*

The proof of the Theorem 1.2.5 is substantial requiring the background of chapters 5-6 and as such its proof is deferred until Chapter 7.

Proposition 3.2.1. *Let* $\pi : R \to A$ *be the unique local ring homomorphism which makes* $\pi \circ \rho_R$ *strictly equivalent to* ρ_A*. Then the restriction* $\pi|_{W_R} : W_R \to W_A$ *is an isomorphism.*

Proof. We begin by observing that $\rho_R(\Gamma) \bmod m_R = SL_n(k)$, thus Theorem 1.2.5 allows us to assume that $SL_n(W_R)$ belongs to the image of a representative of the deformation class to which ρ_R belongs. The compatibility of the W-algebra structure morphisms, see the diagram in 3.1.1, and Proposition 3.1.4 (ii) imply that the group homomorphism:

$$\pi|_{SL_n(W_R)} : SL_n(W_R) \to SL_n(W_A)$$

is surjective. Furthermore, Proposition 3.1.4 (i) implies that this map, $\pi|_{SL_n(W_R)} : SL_n(W_R) \to SL_n(W_A)$, is an isomorphism. Therefore the underlying ring homomorphism $\pi|_{W_R} : W_R \to W_A$ is a ring isomorphism. □

The above assertion allows us to identify W_R and W_A. Henceforth, we will not differentiate between $\iota_R(x)$ and $\iota_A(x)$ for $x \in W$.

Next we investigate the local ring homomorphism π in further detail.

Lemma 3.2.2. *Let* k *be a finite field,* (A, m_A) *a fixed element of* $\mathcal{C}(k)$ *and* $n \geq 2$ *an integer subject to the restrictions:*

- *If* $k = \mathbb{F}_2$ *then* $n \geq 5$
- *If* $k = \mathbb{F}_3$ *or* $\mathbb{F}_5$ *then* $n \geq 3$.

In addition let $x \in A$*.*

(i) There exist a unique λ_x *in* $R^\times$ *and a unique* $s(x)$ *in* R *such that there is an element* $\lambda_x E_{1n}(s(x))$ *in* $\rho_R(\Gamma)$ *with* $\pi(\lambda_x E_{1n}(s(x))) = E_{1n}(x)$*.*

(ii) Furthermore, $E_{ij}(s(x))$ *belongs to* $\rho_R(\Gamma)$ *and is the unique pre-image of* $E_{ij}(x)$ *under* π*.*

Therefore the map $s : A \to R$ *characterised by the following property is well defined:*

> *If* $x \in A$ *then* $s(x)$ *is the unique element in* R *such that* $\pi(s(x)) = x$ *and that* $E_{ij}(s(x))$ *belongs to* $\rho_R(\Gamma)$ *for all* $1 \leq i, j \leq n$ *with* $i \neq j$*.*

Proof. Part (i): Proposition 3.1.4(i) states that $\pi : \rho_R(\Gamma) \to SL_n(A)$ is an isomorphism which implies that there exists a unique $X \in \rho_R(\Gamma)$ such that $\pi(X) = E_{1n}(x)$. We now investigate the form which X takes.

Proposition 3.2.1 together with our identification of W_R with W_A, imply that the elementary matrices $E_{ij}(1)$ with $1 \leq i < j \leq n$ belong to both $SL_n(A)$ and $\rho_R(\Gamma)$. Recall that π is a local ring homomorphism, therefore as $E_{1n}(x) \in SL_n(A)$ commutes with the $E_{ij}(1)$ with $1 \leq i < j \leq n$ so must X. Thus Proposition 2.3.2 (i) implies that $X = \lambda_x E_{1n}(s(x))$ for some $s(x)$ in R and λ_x in $R^\times$.

Part (ii) for $n \geq 3$: For $x \in A$ let $s(x)$ and $\lambda_x \in R$ be defined as in part (i). We may assume that, as elements of $SL_n(W_R)$, the signed permutation matrices T_{ij} belong to $\rho_R(\Gamma)$ (see the defining relations (2.3.1)). Hence Proposition 2.3.2 implies that $\lambda_x E_{ij}(s(x)) = T_{ij}\lambda_x E_{1n}(s(x))T_{ij}^{-1}$. From this, we see that $\lambda_x E_{ij}(s(x))$ is in $\rho_R(\Gamma)$ and is the unique pre-image of $E_{ij}(x)$ for any pair $1 \leq i, j \leq n$ with $i \neq j$. Note that if $x \in W_A$ then $\lambda_x = 1$ and $s(x) = x$ (as $\pi|_{W_R} : W_R \to W_A$ is an insomorphism and we are identifying W_A and W_R). We now show that λ_x is in fact equal to 1 for all elements. Let i, j, k be three distinct integers in $\{1, 2, \ldots, n\}$. By considering their inverse images in $\rho_R(\Gamma)$, the relation $E_{ij}(x) = E_{ik}(x)E_{kj}(1)E_{ik}(x)^{-1}E_{kj}(1)^{-1}$ implies that

$$\begin{aligned}\lambda_x E_{ij}(s(x)) &= \lambda_x E_{ik}(s(x))E_{kj}(1)\lambda_x^{-1}E_{ik}(s(x))^{-1}E_{kj}(1)^{-1} \\ &= E_{ij}(s(x)),\end{aligned}$$

and hence $\lambda_x = 1$.

Part (ii) for $n = 2$: Let's first look at the inverse image of $E_{12}(x)$. Lemma 3.2.2 implies that the inverse image of $E_{12}(mx) = (E_{12}(x))^m$ is

$$\lambda_x{}^m E_{12}(m.s(x)). \tag{3.2.1}$$

In particular, this holds if $m = l^2 - 1$ for a unit $l \in W_A$, thereby giving the alternative identity:

$$E_{12}((l^2 - 1)x) = [L, E_{12}(x)]$$

where $L \in SL_n(W_A)$ is the diagonal matrix which has l in the $(1,1)$-th entry and l^{-1} in the $(2,2)$-th entry. This identity implies that the inverse image of $E_{12}((l^2 - 1)x)$ must also be given by:

$$\begin{aligned}[L, \lambda_x E_{12}(s(x))] &= L\lambda_x E_{12}(s(x))L^{-1}\lambda_x{}^{-1}E_{12}(-s(x)) \\ &= E_{12}((l^2 - 1)s(x)).\end{aligned}$$

This implies that $\lambda_x{}^{l^2-1} = 1$. Given the restriction on k, we may assume that A has two distinct units u and v such that the expressions $u^2 - 1$ and $v^2 - 1$ are both non-trivial and distinct. Therefore $\lambda_x^{u^2-1} = \lambda_x^{v^2-1}$, hence $\lambda_x = 1$.

Now, let's look at the inverse image of $E_{21}(x)$. The equation (3.2.1) implies that $\pi^{-1}(E_{12}(-x)) = E_{12}(-s(x))$. By observing the following identity:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix}$$

we see that the inverse image of $E_{21}(-x)$ under π is $E_{21}(-s(x))$.

From the argument above it is clear that $s : A \to R$ is well defined. □

As we have shown that the set-theoretic section $s : A \to R$ is well defined all that remains to prove Proposition 3.1.5 is to show that s is a local ring homomorphism.

Proposition 3.2.3. *The map $s : A \to R$ defined in Lemma 3.2.2 is a local ring homomorphism which is a section for π.*

Proof. From the construction of $s : A \to R$ it is clear that $s|_{W_A}$ is the inverse to $\pi|_{W_R}$; and that $\pi \circ s$ is the identity on A. Also, Proposition 2.2.2(a) implies that $s(x + y) = s(x) + s(y)$ for all $x, y \in A$. If $n \geq 3$ and $1 \leq i, j, k \leq n$ are three distinct integers, then the commutation relation $[E_{ij}(s(x)), E_{jk}(s(y))] = E_{ik}(s(x)s(y))$ shows that $s(xy) = s(x)s(y)$. Therefore $s : A \to R$ is a ring homomorphism. Finally, by its construction $s(m_A) \subseteq m_R$ and s induces the identity on $A/m_A = R/m_R = k$ and is thus a local ring homomorphism.

All that remains is to show when $n = 2$ that s exhibits the multiplicative property as well. To this end, let $a \in A^\times$ then Whitehead's Lemma (Lemma 2.1.1) gives:

$$\begin{aligned} E_{21}(a^{-1})E_{12}(1-a)E_{21}(-1)E_{12}(1-a^{-1}) &= \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \\ E_{21}(a)E_{12}(1-a^{-1})E_{21}(-1)E_{12}(1-a) &= \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}. \end{aligned}$$

After mapping these matrices under $s : A \to R$ and invoking the additive property, these become:

$$\begin{aligned} E_{21}(s(a^{-1}))E_{12}(s(1-a))E_{21}(-1)E_{12}(s(1-a^{-1})) &= \alpha \\ E_{21}(s(a))E_{12}(s(1-a^{-1}))E_{21}(-1)E_{12}(s(1-a)) &= \beta \end{aligned}$$

respectively, where

$$\begin{aligned} \alpha &= \begin{pmatrix} s(a) & 1 - s(a)s(a^{-1}) \\ s(a^{-1})s(a) - 1 & s(a^{-1})[2 - s(a)s(a^{-1})] \end{pmatrix} \\ \beta &= \begin{pmatrix} s(a^{-1}) & 1 - s(a^{-1})s(a) \\ s(a)s(a^{-1}) - 1 & s(a)[2 - s(a)s(a^{-1})] \end{pmatrix}. \end{aligned}$$

By definition $\beta = \alpha^{-1}$ and looking at the $(1, 2)$-th entries we see that:

$$1 - s(a^{-1})s(a) = -[1 - s(a)s(a^{-1})]$$

which implies that $s(a^{-1}) = s(a)^{-1}$ if the characteristic of k is not equal to 2. If the characteristic of k is 2 then also observe that the $(1, 1)$-th entry of α must equal the $(2, 2)$-nd entry of β hence:

$$s(a) = s(a)[2 - s(a)s(a^{-1})]$$

which implies that $s(a) = s(a)s(a)s(a^{-1})$. As a is a unit we may cancel a factor of $s(a)$ and thus $s(a^{-1}) = s(a)^{-1}$.

Suppose that a_1, a_2 are both units in A and consider the inverse image of a_1a_2 and the diagram:

$$\begin{array}{ccc}
\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix} & \longrightarrow & \begin{pmatrix} s(a_1) & 0 \\ 0 & s(a_1^{-1}) \end{pmatrix}\begin{pmatrix} s(a_2) & 0 \\ 0 & s(a_2^{-1}) \end{pmatrix} \\
\downarrow & & \downarrow \\
\begin{pmatrix} a_1a_2 & 0 \\ 0 & a_1^{-1}a_2^{-1} \end{pmatrix} & \longrightarrow & \begin{pmatrix} s(a_1a_2) & 0 \\ 0 & s(a_1^{-1}a_2^{-1}) \end{pmatrix}
\end{array}$$

which imply that $s(a_1)s(a_2) = s(a_1a_2)$. Now we consider the case where a_1 is a unit and a_2 is a non-unit. As A is a local ring this means that $1 + a_2$ is a unit and using the diagram as above we have:

$$\begin{aligned}
s(a_1)s(1 + a_2) &= s(a_1(1 + a_2)) \\
\implies s(a_1)(1 + s(a_2)) &= s(a_1 + a_1a_2) \\
\implies s(a_1) + s(a_1)s(a_2) &= s(a_1) + s(a_1a_2)
\end{aligned}$$

which again implies that $s(a_1)s(a_2) = s(a_1a_2)$. To conclude we consider the case where both a_1 and a_2 are non-units which follows similarly from:

$$\begin{aligned}
s(1 + a_1)s(1 + a_2) &= s((1 + a_1)(1 + a_2)) \\
\implies (1 + s(a_1))(1 + s(a_2)) &= s(1 + a_1 + a_2 + a_1a_2) \\
\implies 1 + s(a_1) + s(a_2) + s(a_1)s(a_2) &= 1 + s(a_1) + s(a_2) + s(a_1a_2).
\end{aligned}$$

□

.

Chapter 4

Group Cohomology and Extensions

4.1 Group Cohomology

Throughout this section let G be a profinite group. We give a utilitarian approach to the cohomology of G defining only what is required in this thesis. Unfortunately, this approach shrouds the true elegancy of the subject, which is better described in [21]. As a lead-in to cohomology we introduce G-modules:

Definition 4.1.1. Let G be a group with identity e and M an abelian group. If there is a map $G \times M \to M : (g, m) \to g \cdot m$ satisfying

- $g \cdot (m + n) = g \cdot m + g \cdot n$
- $e \cdot m = m$
- $(gh) \cdot m = g \cdot (h \cdot m)$

for all $g, h \in G$ and $m, n \in M$, then M is called G-module.

We begin with the definitions of the zeroth, first and second cohomology groups.

Definition 4.1.2. For a G and M as above: $H^0(G, M) = M^G$.

In order to define the first cohomology group we introduce:

Definition 4.1.3. Let G and M be as above, then 1-cocycles are defined as:

$$Z^1(G, M) = \{f : G \to M \mid f(gh) = f(g) + g \cdot f(h)\ \forall g, h, \in G\}$$

and 1-coboundaries are defined as:

$$B^1(G, M) = \{f \in Z^1(G, M); \mid \exists m \in M \text{ such that } f(g) = g \cdot m - m,\ \forall g \in G\}.$$

Then the 1-cohomology group is the following factor group:

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

Lemma 4.1.4. *Let G be a group which acts trivially on a module $\mathcal{M}$. Then with regard to $H^1(G,\mathcal{M})$ the only 1-coboundary is the zero map. Also, as G acts trivially a 1-cocycle f in $H^1(G,\mathcal{M})$ is a map satisfying*

$$f(gh) = f(g) + f(h)$$

for all g and h in G. Therefore $H^1(G,\mathcal{M}) = \mathrm{Hom}(G,\mathcal{M})$.

Similarly, to introduce the second cohomology group we require:

Definition 4.1.5. Let G and M be as above, then 2-cocycles are defined as:

$$Z^2(G,M) = \{f : G\times G \to M \,|\, f(g_1,g_2g_3) - f(g_1g_2,g_3) + g_1\cdot f(g_2,g_3) - f(g_1,g_2) = 0\}$$

and 2-coboundaries are defined as:

$$\begin{aligned} B^2(G,M) \;=\; & \{f \in Z^2(G,M) \mid \exists h : G \to M \text{ such that} \\ & f(g_1,g_2) = g_1\cdot h(g_2) - h(g_1g_2) + h(g_1),\ \forall g_1,g_2 \in G\}. \end{aligned}$$

Then the 2-cohomology group is the following factor group:

$$H^2(G,M) = Z^2(G,M)/B^2(G,M).$$

We will make great use of the following well known result, called the inflation-restriction exact sequence, which may be found in [21].

Proposition 4.1.6. *Let N be a closed normal subgroup of G and M be a G-module. Then there is the following exact sequence:*

$$0 \to H^1(G/N,M^N) \xrightarrow{inf} H^1(G,M) \xrightarrow{res} H^1(N,M)^{G/N} \xrightarrow{tr} H^2(G/N,M^N) \xrightarrow{inf} H^2(G,M)$$

where the maps are

- $inf : H^n(G/N,M^N) \to H^n(G,M)$ *is the inflation map*
- $res : H^n(G,M) \to H^n(N,M)^{G/N}$ *is the restriction map*
- $tr : H^n(N,M)^{G/N} \to H^{n+1}(G/N,M)$ *is the transgression map.*

4.2 Extensions

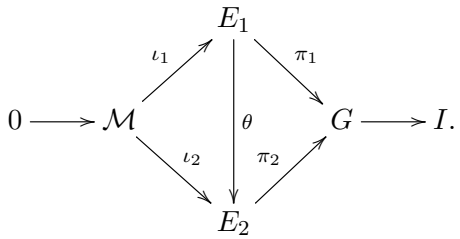
In this section we discuss standard results about group extensions, for a more complete exposition see [8]. We remark that in this section I will denote both the identity element in a given group and the set which has the identity as its only element.

Definition 4.2.1. Let G be a finite group with identity I and $\mathcal{M}$ be a finite abelian group. Then a short exact sequence of groups:

$$0 \to \mathcal{M} \xrightarrow{\iota} E \xrightarrow{\pi} G \to I \tag{4.2.1}$$

is called an extension of G by $\mathcal{M}$.

Next we consider the notion of equivalence of extensions. Let E_1 and E_2 be two extensions of G by $\mathcal{M}$. The extensions E_1 and E_2 are *equivalent* if there exists a homomorphism $\theta : E_1 \to E_2$ so that the following diagram commutes:



A crucial feature of group extensions, as defined in Definition 4.2.1, is that there is a consequent well defined action of G on $\mathcal{M}$ i.e. $\mathcal{M}$ has an interpretation as a G-module as we now outline.

As the map $\iota : \mathcal{M} \to E$ is injective it gives rise to an embedding of $\mathcal{M}$ as a normal subgroup in E. Thus E acts on $\mathcal{M}$ via conjugation which is denoted by $\gamma \cdot m$ for $\gamma \in E$ and $m \in \mathcal{M}$ and is specified by the following:

$$\gamma \cdot m = \gamma \iota(m) \gamma^{-1}.$$

Moreover, the action of $\mathcal{M}$ on itself is trivial as $\mathcal{M}$ is abelian. Therefore, this induces an action of $E/\mathcal{M} = G$ on $\mathcal{M}$. We shall now define the action of G on $\mathcal{M}$ precisely.

Let $g \in G$ and choose a lifting, $\tilde{g}$, of g to E, i.e. such that $\pi(\tilde{g}) = g$. Then the action of G on $\mathcal{M}$, denoted $g \cdot m$ for $g \in G$ and $m \in \mathcal{M}$, is specified by the following:

$$\iota(g \cdot m) = \tilde{g} \iota(m) \tilde{g}^{-1}.$$

Definition 4.2.2. Suppose we are given an extension of G by M, i.e. an exact sequence of the form of equation 4.2.1. In addition, suppose there exists a group-theoretic section $s : G \to E$ for π, i.e. such that $\pi \circ s : G \to G$ is the identity on G. Then the extension is said to split.

Now we investigate split extensions further, of central importance is the following definition of the semi-direct product.

Definition 4.2.3. Let $\mathcal{M}$ be a G-module and denote the action of an element $g \in G$ on $m \in \mathcal{M}$ by $g \cdot m$. Then we can define the following group law on the set $\mathcal{M} \times G$:

$$(m, g)(n, h) = (m + g \cdot n, gh) \tag{4.2.2}$$

for $m, n \in \mathcal{M}$ and $g, h \in G$. The group thus defined is written $\mathcal{M} \rtimes G$. Then the canonical inclusion map $\iota : \mathcal{M} \to \mathcal{M} \rtimes G$ defined by $\iota(m) = (m, 1)$ and projective map $\pi : \mathcal{M} \rtimes G$ defined by $\pi(m, g) = g$ specify the following extension of G by $\mathcal{M}$:

$$0 \to \mathcal{M} \xrightarrow{\iota} \mathcal{M} \rtimes G \xrightarrow{\pi} G \to I \tag{4.2.3}$$

which is called the semi-direct product of G and $\mathcal{M}$ with respect to the given action of G on $\mathcal{M}$.

Proposition 4.2.4. *The semi-direct product of G and $\mathcal{M}$ with respect to the given action of G on $\mathcal{M}$ is a split extension. Furthermore, every split extension of G by $\mathcal{M}$ with a given action of G on $\mathcal{M}$ is equivalent to the semi-direct product of G and $\mathcal{M}$ with respect to the same given action of G on $\mathcal{M}$.*

Proof. Firstly, observe that the map $s : G \to \mathcal{M} \rtimes G$ given by $s(g) = (0, g)$ is a group theoretic section for π, hence the semi-direct product is a split extension.

Secondly, suppose we are given an extension of the form of equation 4.2.1 which splits. Now, as $\pi \circ s$ is the identity on G there is a subgroup $\tilde{G} < E$ isomorphic to G such that $\iota(M) \cap \tilde{G} = 1$. Therefore we can write each element of E uniquely in the form

$$\iota(m)\tilde{g}$$

for some $m \in \mathcal{M}$ and $\tilde{g} \in \tilde{G}$. Thus, the map $\theta : \mathcal{M} \rtimes G \to E$ given by

$$\theta(m, g) = \iota(m)\tilde{g}$$

is a group isomorphism making the extension equivalent to the semi-direct product. □

We remark that if the action of G on $\mathcal{M}$ in Definition 4.2.3 is trivial then we have the group law:

$$(m, g)(n, h) = (m + n, gh)$$

which is the direct product of the abelian group $\mathcal{M}$ with the group G.

The next theorem is a standard classification theorem for group extensions up to equivalence and may be found in [2] where it is Theorem VI.15.6. Prior to stating the theorem we make the definition that an element x in $H^2(G, \mathcal{M})$ is said to be normalised if

$$x(g, I) = x(I, g) = 0$$

for all g in G.

Definition 4.2.5. Let G act on $\mathcal{M}$ and $x \in H^2(G, \mathcal{M})$. We can define another group law on the set $\mathcal{M} \times G$ by:

$$(m_1, g_1)(m_2, g_2) = (x(g_1, g_2) + m_1 + g_1 \cdot m_2, g_1 g_2)$$

for $g_1, g_2 \in G$ and $m_1, m_2 \in \mathcal{M}$. The group thus defined is called the twisted semi-direct product of G and $\mathcal{M}$ and is written $\mathcal{M} \rtimes_x G$. Similarly to the semi-direct product above the inclusion map ι and projection map π specify the following extension:

$$0 \to \mathcal{M} \xrightarrow{\iota} \mathcal{M} \rtimes_x G \xrightarrow{\pi} G \to I$$

for the given action of G on $\mathcal{M}$.

We remark that if we take the trivial cocycle in $H^2(G, \mathcal{M})$, i.e. $x = 0$, in Definition 4.2.5 then the group law reverts to $(m_1, g_1)(m_2 g_2) = (m_1 + g_1 \cdot m_2, g_1 g_2)$ and we obtain the usual semi-direct product.

We also observe that if we are given a twisted semi-direct product, $\mathcal{M} \rtimes_x G$, then the set-theoretic map $s : G \to \mathcal{M} \rtimes_x G$ is no longer necessarily a group homomorphism as shown by the equality:

$$(0, g_1)(0, g_2) = (x(g_1, g_2), g_1 g_2).$$

This indicates that in general, there is no reason to suggest that the twisted semi-direct product should split.

Theorem 4.2.6. *Let $\mathcal{M}$ be a G-module and let $\mathcal{E}(G, \mathcal{M})$ be the set of equivalence classes of extensions of G by $\mathcal{M}$ inducing the given action of G on $\mathcal{M}$. Then there is a one-to-one correspondence:*

$$\mathcal{E}(G, \mathcal{M}) \leftrightarrow H^2(G, \mathcal{M}).$$

4.3 Extensions and Group Cohomology

The next result, which is Proposition 2.1 of [16], uses the transgression map to establish a connection between extensions and the group $H^1(\mathcal{M} \rtimes_x I, \mathcal{M})^G$.

Proposition 4.3.1. *Let $\mathcal{M}$ be a G-module and consider the group extension $\mathcal{M} \rtimes_x G$ for some normalised $x \in H^2(G, \mathcal{M})$. This gives rise to the exact sequence of groups:*

$$I \to \mathcal{M} \rtimes_x I \to \mathcal{M} \rtimes_x G \to G \to I$$

thus identifying $\mathcal{M}$ with the normal subgroup $\mathcal{M} \rtimes_x I \trianglelefteq \mathcal{M} \rtimes_x G$. Now apply the inflation-restriction exact sequence to the preceding exact sequence of groups and the G-module $\mathcal{M}$ and define $-\phi : \mathcal{M} \rtimes_x I \to \mathcal{M}$ by $-\phi(m, I) = -m$.

Then the transgression map

$$tr : \mathrm{Hom}_G(\mathcal{M} \rtimes_x I, \mathcal{M}) = H^1(\mathcal{M} \rtimes_x I, \mathcal{M})^G \to H^2(G, \mathcal{M})$$

takes $-\phi$ to the cohomology class of x.

We continue our recapitulation of the discussion in [16].

Lemma 4.3.2. *Let $\mathcal{M}$ be an $\mathbb{F}_p[G]$-module of finite cardinality and $\mathcal{N} \subseteq \mathcal{M}$ be an $\mathbb{F}_p G$-submodule such that the following map is injective*

$$H^2(G, \mathcal{N}) \to H^2(G, \mathcal{M}).$$

In addition, let $x \in H^2(G, \mathcal{N}) \subseteq H^2(G, \mathcal{M})$ and suppose $H < \mathcal{M} \rtimes_x G$ is a group extension of G by $\mathcal{N}$ with respect to the restriction of the action of G on $\mathcal{M}$.

Then there exists an isomorphism

$$\theta : \mathcal{N} \rtimes_x G \cong H$$

which makes these two extensions of G by $\mathcal{N}$ equivalent.

Proof. The statement of the lemma implies that by Theorem 4.2.6 the extension

$$0 \to \mathcal{N} \to H \to G \to I$$

corresponds to x in $H^2(G, \mathcal{N})$ and hence is equivalent to the extension $\mathcal{N} \rtimes_x G$. Thus implying the existence of the isomorphism θ. □

This section ends with the following result which is Proposition 2.2 in [16].

Proposition 4.3.3. *Let $\mathcal{M}$ be an $\mathbb{F}_p[G]$-module of finite cardinality and $\mathcal{N} \subseteq \mathcal{M}$ be an $\mathbb{F}_pG$-submodule such that the following map is injective*

$$H^2(G, \mathcal{N}) \to H^2(G, \mathcal{M}).$$

As in Lemma 4.3.2 above, let $x \in H^2(G, \mathcal{N}) \subseteq H^2(G, \mathcal{M})$ and suppose $H < \mathcal{M} \rtimes_x G$ is a group extension of G by $\mathcal{N}$ with respect to the restriction of the action of G on $\mathcal{M}$. Finally, let $\theta : \mathcal{N} \rtimes_x G \cong H$ be the resulting isomorphism.

Then, we may define a map $\eta : G \to \mathcal{M}$ satisfying

$$\theta(0, g) = (\eta(g), g)$$

for all $g \in G$.

Furthermore, these maps have the following properties:

1. *$\theta(n, g) = (n + \eta(g), g)$ for all $n \in \mathcal{N}$, $g \in G$.*
2. *The map $\eta : G \to \mathcal{M}$ is a 1-cocycle.*
3. *If $H^1(G, \mathcal{M}) = 0$ then θ is conjugation by (m, e) for some $m \in \mathcal{M}$.*

Chapter 5

Modules for $kSL_n(W_r)$

The aim of this chapter is twofold: in the first section to investigate the submodule structure of certain $kSL_n(k)$-modules and in the second to relate this to the structure of $kSL_n(W_r)$-modules and 1-cohomology groups. We begin by fixing the notation used in this chapter.

Definition 5.0.4. Let $\mathfrak{M} := \mathfrak{M}(n)$ denotes the set of $n \times n$ matrices with coefficients in k. The subset consisting of matrices with trace zero is written $\mathfrak{M}_0 := \mathfrak{M}_0(n)$.

Let k be a fixed choice of finite field, (A, m_A) a fixed element of $\mathcal{C}(k)$ and $n \geq 2$ an integer. We then define $\rho_A : SL_n(A) \xrightarrow{\cong} SL_n(A)$ to be the identity representation and $\bar{\rho} : SL_n(A) \to SL_n(k)$ to be the componentwise reduction of ρ_A modulo m_A. The residual representation $\bar{\rho}$ defines an action of $SL_n(A)$ on $\mathfrak{M}$ via:

$$\gamma \cdot M = \bar{\rho}(\gamma) M \bar{\rho}(\gamma)^{-1} \tag{5.0.1}$$

for all γ in $SL_n(A)$ and M in $\mathfrak{M}$. Furthermore, as the trace is similarity invariant, $\mathfrak{M}_0$ is naturally endowed with the structure of a $SL_n(A)$-submodule of $\mathfrak{M}$.

Finally, we remark that if M is a $SL_n(A)$-module then we can linearly extend the action of $SL_n(A)$ to give an action of $kSL_n(A)$ thus making M a $kSL_n(A)$-module.

5.1 Modules for $kSL_n(k)$

This section examines the $kSL_n(k)$-submodule structure of $\mathfrak{M}$ and $\mathfrak{M}_0$ and concludes by calculating homomorphism groups between them. To this end, we begin by listing the generators of $\mathfrak{M}$ and $\mathfrak{M}_0$ in the following lemma.

Lemma 5.1.1. *The $kSL_n(k)$-module $\mathfrak{M}$ is generated by $a_{ij} := e_{ij}$ where the indices satisfy $1 \leq i, j \leq n$ and are not necessarily distinct.*

The $kSL_n(k)$-submodule $\mathfrak{M}_0$ is generated by the elements:

1. *a_{ij} where $i \neq j$*

2. $h_{i,i+1} := e_{ii} - e_{i+1,i+1}$ *where* $1 \leq i \leq n-1$.

Let $\mathfrak{S}$ denote the scalar matrices in $\mathfrak{M}$. It is immediately clear that $\mathfrak{S} \cap \mathfrak{M}_0$ is a $kSL_n(k)$-submodule of $\mathfrak{M}_0$. The trace of a scalar matrix λI_n is $n\lambda$, therefore this intersection is non-trivial if and only if the characteristic of k divides n.

Proposition 5.1.2. *Let p be the characteristic of k and $n \geq 2$.*

(i) If p does not divide n then $\mathfrak{M}_0$ is a simple $kSL_n(k)$-module,

(ii) If p divides n and the pair $(n, q) \neq (2, 2)$ then $\mathfrak{S}$ is the only non-trivial $kSL_n(k)$-submodule of $\mathfrak{M}_0$.

Proof. For part (i) assume that $\mathcal{M}$ is an arbitrary non-zero $kSL_n(k)$-submodule of $\mathfrak{M}_0$. Then $\mathcal{M}$ contains a non-zero element

$$v = \sum_{i=1}^{n-1} \lambda_i (e_{ii} - e_{i+1,i+1}) + \sum_{i \neq j} \mu_{ij} e_{ij}$$

where at least one of the coefficients λ_i or μ_{ij} is not zero and as p is coprime to n we may assume v is not a scalar either. The procedure for the proof is: show that an element $w = \nu e_{ij}$ with i and j distinct belongs to $\mathcal{M}$, then conclude by showing that w may be conjugated to all elements of $\mathfrak{M}_0$ by listing suitable elements of $SL_n(k)$.

Suppose that $\mu_{ij} \neq 0$. For ease of presentation write the element v with respect to the standard basis for $\mathfrak{M}$, i.e.

$$v = \sum_{a,b} m_{ab} e_{ab}$$

where by assumption $m_{ij} = \mu_{ij} \neq 0$. There are of course restrictions on the diagonal entries but these are unimportant here. To begin with assume $n \geq 3$ and fix an index $x \neq i, j$. The following elements belong to $\mathcal{M}$:

$$\begin{aligned} v' = (E_{xi}(1) - I) \cdot v &= \sum_s m_{is} e_{xs} - \sum_r m_{rx} e_{ri} - m_{ix} e_{xi}, \\ v'' = (I - E_{ji}(1)) \cdot v' &= m_{ix} e_{ji} + m_{ij} e_{xi}, \\ v''' = (E_{jx}(1) - I) \cdot v'' &= m_{ij} e_{ji}. \end{aligned}$$

If $n = 2$ assume $m_{ij} \neq 0$ where i and j are distinct. Firstly, let $p \geq 3$ then the element

$$2E_{ji}(1) \cdot v - E_{ji}(2) \cdot v - v = 2m_{ij} e_{ji}$$

belongs to $\mathcal{M}$. Secondly, let $p = 2$ and $q \geq 4$ thus there exists $x \in k^\times$ such that $x^2 - 1 \neq 0$. Define an element of $SL_2(k)$ by

$$X = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}.$$

Then the following element belongs to $\mathcal{M}$:

$$(X - I) \cdot ((E_{ji}(1) - I) \cdot v) = (x^2 - 1)m_{ij}e_{ji}.$$

Suppose that $\lambda_i \neq 0$ (in this case there is no need to differentiate between $n = 2$ and $n \geq 3$). If at least one of the μ_{ab} is non-zero then the previous argument may be invoked. Therefore assume $v = \sum_r m_{rr}e_{rr}$. As $\lambda_i \neq 0$ and v is not a scalar it is implied that at least one entry of v is non-zero, although not necessarily the (i, i)-th. Label this entry σe_{xx}. In addition, at least one other entry differs from σ; label this entry τe_{yy} (τ may or may not be zero). Then the following belongs to $\mathcal{M}$:

$$(E_{xy}(1) - I) \cdot v = m_{yy}e_{xy} - m_{xx}e_{xy} = (\tau - \sigma)e_{xy}.$$

Therefore we may assume that a non-zero element $\mu_{ij}e_{ij}$ is in $\mathcal{M}$. By Corollary 2.3.3 if e_{ij} belongs to $\mathcal{M}$ then so do the e_{ab} with $a \neq b$. This also implies that $e_{ij} + e_{ji}$ is contained in $\mathcal{M}$. The following conjugation

$$E_{ji}(-1) \cdot (e_{ij} + e_{ji}) = e_{ij} + e_{ii} - e_{jj}$$

implies that $e_{ii} - e_{jj}$ also belongs to $\mathcal{M}$. Invoking Corollary 2.3.3 again implies that $\mathcal{M}$ contains all elements $e_{aa} - e_{bb}$ for $a \neq b$. Therefore if p does not divide n then $\mathcal{M} = \mathfrak{M}_0$.

For part (ii) observe that the elements of $\mathfrak{S}$ clearly commute with the action of $SL_n(k)$ and constitute a $kSL_n(k)$-submodule of $\mathfrak{M}_0$. The argument of part (i) implies that $\mathfrak{S}$ is the only $kSL_n(k)$-submodule of $\mathfrak{M}_0$. □

Corollary 5.1.3. *Let $p|n$ and $\mathfrak{V} := \mathfrak{M}_0/\mathfrak{S}$. The module $\mathfrak{V}$ is a simple $kSL_n(k)$-module.*

Proof. This follows directly from the argument proving Proposition 5.1.2 (i) by regarding the elements described as belonging to $\mathfrak{V}$ rather than $\mathfrak{M}_0$. □

Note that $\mathfrak{M}/\mathfrak{M}_0 \cong k$ and recall $\mathfrak{V} := \mathfrak{M}_0/\mathfrak{S}$ then we have the following.

Corollary 5.1.4. *The following sequences of $kSL_n(k)$-modules are exact:*

1. $0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0$. *Furthermore if p does not divide n then this sequence splits giving the direct sum decomposition $\mathfrak{M} = \mathfrak{M}_0 \oplus \mathfrak{S}$.*

2. *Suppose that $p|n$, $0 \to \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{V} \to 0$.*

Proposition 5.1.5. *Let $n \geq 2$. Firstly, assume that p does not divide n, if ϕ belongs to $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0)$ then $\phi(e_{1n}) = \lambda e_{1n}$.*

Secondly, assume $p|n$ then the following hold:

- *if $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0)$ then $\phi|_{\mathfrak{S}} : \mathfrak{S} \to \mathfrak{S}$*
- *if $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{V})$ then $\phi|_{\mathfrak{S}} : \mathfrak{S} \to \mathfrak{V}$ is the zero map.*

Suppose that ϕ belongs to either $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{V})$ *or* $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{V}, \mathfrak{V})$ *then* $\phi(e_{1n}) = \lambda e_{1n}$ *where depending on the context e_{1n} refers to either the matrix unit or its image in $\mathfrak{V}$.*

Proof. Let γ be an arbitrary element of $SL_n(k)$ and m an arbitrary element of a $kSL_n(k)$-module $\mathcal{M}$. Then by definition ϕ in $\mathrm{Hom}_{kSL_n(k)}(\mathcal{M}, \mathcal{M})$ must exhibit the property:

$$\phi(\gamma \cdot m) = \gamma \cdot \phi(m) \tag{5.1.1}$$

for all $\gamma \in SL_n(k)$.

For the first part (when p does not divide n), we show that for $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0)$ equation (5.1.1) completely specifies the form which $\phi(e_{1n})$ takes. Let $1 \leq i \leq n-1$ be an integer and observe that $E_{i,i+1} \cdot e_{1n} = e_{1n}$. Therefore equation 5.1.1 implies that for all i:

$$E_{i,i+1}\phi(e_{1n}) = \phi(e_{1n})E_{i,i+1}.$$

If we write $\phi(e_{1n}) = \sum_{a,b} m_{ab}e_{ab}$ then this implies that

$$\phi(e_{1n}) + \sum_b m_{i+1,b}e_{ib} = \phi(e_{1n}) + \sum_a m_{ai}e_{a,i+1}.$$

This itself implies that

$$\begin{cases} m_{i+1,i+1} = m_{ii} & \\ m_{i+1,x} = 0 & \text{if } x \neq i+1 \\ m_{xi} = 0 & \text{if } x \neq i. \end{cases} \tag{5.1.2}$$

Running through all values of i we see that $\phi(e_{1n}) = \mu I + \lambda e_{1n}$. However, as $\phi(e_{1n}) \in \mathfrak{M}_0$ and p does not divide n this means that $\mu = 0$.

For the second part, observe that the proof of Lemma 3.1.1 implies that the elements of $\mathfrak{S}$ are fixed by $SL_n(k)$ and thus so must their images under ϕ. This proves the assertions in bullet points. The remaining assertions are a direct consequence of the bullet points in combination with the proof of the first part. □

Corollary 5.1.6. *Let $n \geq 2$ then:*

1. $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0) \cong k$
2. $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, k) = 0.$
3. $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{V}) \cong k$
4. $\mathrm{Hom}_{kSL_n(k)}(\mathfrak{V}, \mathfrak{V}) \cong k$

Proof. For part (1). Let $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0)$ and λ belong to k. We define the functions $f(M) = \phi(M) - \lambda M$ for M in $\mathfrak{M}_0$ and make the observations:

- If $p|n$ then for a suitable choice of λ the submodule $\mathfrak{S}$ belongs to $ker(f)$.

- If p does not divide n then e_{1n} belongs to $ker(f)$ by Proposition 5.1.5.

Given the submodule structure of $\mathfrak{M}_0$ (see Lemma 5.1.1) and that both $\ker(f)$ and $\mathrm{Im}(f) \cong \mathfrak{M}_0/\ker(f)$ are submodules of $\mathfrak{M}_0$ the observations above imply that $\ker(f) = \mathfrak{M}_0$. Therefore we may write $\phi(M) = \lambda M$ and the result follows.

For part (3). Let $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{V})$ and define f in an analogous way by taking its image in $\mathfrak{V}$. By the preceding proposition $e_{1n} \in \ker(f)$ and as $\mathfrak{V}$ is a simple $kSL_n(k)$-module by Corollary 5.1.3 the result follows. The similar result for part (4) for $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{V}, \mathfrak{V})$ is immediate.

Finally, we look at part (2). Let $\phi \in \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, k)$ and note that $SL_n(k)$ acts trivially on k. Therefore we must have $\phi(\gamma \cdot M) = \phi(M)$ for all $\gamma \in SL_n(K)$ and for all $M \in \mathfrak{M}_0$. Let

$$I' = \sum_{i=2}^{n-1} e_{ii}$$

and define the matrix:

$$N = e_{1n} - e_{n1} + I'$$

(we remark that if $n = 2$ then $N = e_{12} - e_{21}$ or if $n = 3$ then $N = e_{13} - e_{31} + e_{22}$). Observe that $N \cdot e_{1n} = -e_{n1}$. This implies that $\phi(e_{1n}) = \phi(N \cdot e_{1n}) = \phi(-e_{n1})$, thus $e_{1n} + e_{n1}$ belongs to the kernel of ϕ. Therefore as $\mathfrak{M}_0$ is simple the result follows. □

5.2 $kSL_n(W_r)$-modules

Recall from the introduction to this chapter that $\bar{\rho} : SL_n(A) \to SL_n(k)$ defines an action of $SL_n(A)$ on $\mathfrak{M}$ and $\mathfrak{M}_0$. In particular this holds for rings of the form W_r. In this section we investigate $kSL_n(W_r)$-module homomorphisms and relate them to 1-cohomology groups.

However prior to this, we let $\pi : W_{r+1} \to W_r$ be reduction modulo p^r and discuss the group extension obtained from the resulting group homomorphism:

$$\pi : SL_n(W_{r+1}) \to SL_n(W_r) \tag{5.2.1}$$

defined to be componentwise reduction modulo p^r

Recall that $M_n(W_{r+1})$ denotes the ring of $n \times n$ matrices over W_{r+1}. The kernel of π is a normal subgroup of $SL_n(W_{r+1})$ given by

$$K_r := \{I + p^r M \mid M \in M_n(W_{r+1}) \text{ with trace } 0\}.$$

Therefore the map π defines the exact sequence:

$$1 \to K_r \to SL_n(W_{r+1}) \xrightarrow{\pi} SL_n(W_r) \to I \tag{5.2.2}$$

we observe that K_r is an abelian subgroup of $SL_n(W_{r+1})$ which can be seen from the product

$$(I + p^r M)(I + p^r N) = I + p^r(M + N + p^r MN) = I + p^r(M + N)$$

where M, N belong to $M_n(W_{r+1})$ (the second equality holds because p annihilates p^r in W_{r+1}).

As K_r is abelian it may be written additively. With this in mind, let $I + p^r M$ belong to K_r, as p annihilates any matrix of the form $p^r M$ the matrix M depends only on its image in $M_n(k)$. Hence we may define a group isomorphism $\phi : K_r \to \mathfrak{M}_0$ by

$$\phi(I + p^r M) = M \bmod p^r. \tag{5.2.3}$$

Therefore $SL_n(W_{r+1})$ is an extension of $SL_n(W_r)$ by $\mathfrak{M}_0$ with respect to the action of $\gamma \in SL_n(W_r)$ on $M \in \mathfrak{M}_0$ given by

$$\gamma \cdot M = \bar{\rho}(\gamma) M \bar{\rho}(g^{-1}).$$

Now we construct a map $\varepsilon : \mathfrak{M}_0 \to SL_n(W_{r+1})$ which is a one-sided inverse for ϕ: for $M \in \mathfrak{M}_0$ take a lift $\widetilde{M} \in M_n(W_r)$ of M and define

$$\varepsilon(M) = I + p^r \widetilde{M}. \tag{5.2.4}$$

This means that the extension $SL_n(W_{r+1})$ is equivalent to

$$0 \to \mathfrak{M}_0 \xrightarrow{\varepsilon} \mathfrak{M}_0 \rtimes_x SL_n(W_r) \xrightarrow{\pi} SL_n(W_r) \to I \tag{5.2.5}$$

for some class x in $H^2(SL_n(W_r), \mathfrak{M}_0)$.

If $p|n$ then we can define another exact sequence as we now explain. In this instance the centre of $SL_n(W_{r+1})$ is not trivial given by:

$$Z_r = \{(1 + p^r w)I \mid w \in W_r\}. \tag{5.2.6}$$

The map $\pi : SL_n(W_{r+1}) \to SL_n(W_r)$ induces the map:

$$\pi' : SL_n(W_{r+1})/Z_r \to SL_n(W_r)$$

with kernel K_r/Z_r. This implies that there is the additional exact sequence of groups:

$$I \to K_r/Z_r \to SL_n(W_{r+1})/Z_r \xrightarrow{\pi'} SL_n(W_r) \to I. \tag{5.2.7}$$

Recall the isomorphism $\phi : K_r \to \mathfrak{M}_0$ of equation (5.2.3), its restriction $\phi|_{Z_r}$ defines an isomorphism between Z_r and $\mathfrak{S}$. This observation induces an isomorphism $\phi' : K_r/Z_r \to \mathfrak{V}$ with a similar one-sided inverse $\varepsilon' : \mathfrak{V} \to SL_n(W_{r+1})/Z_r$ such that the extension $SL_n(W_{r+1})/Z_r$ is equivalent to

$$0 \to \mathfrak{V} \xrightarrow{\varepsilon'} \mathfrak{V} \rtimes_x SL_n(W_r) \xrightarrow{\pi'} SL_n(W_r) \to I \tag{5.2.8}$$

for some class x in $H^2(SL_n(W_r), \mathfrak{V})$.

At this point we apply the inflation-restriction exact sequence of cohomology groups (Proposition 4.1.6) to the extensions (5.2.2) and (5.2.7) and a $SL_n(W_{r+1})$-module (respectively $SL_n(W_{r+1})/Z_r$-module) $\mathcal{M}$. This gives the exact sequence

$$0 \to H^1(SL_n(W_r), \mathcal{M}^{K_r}) \to H^1(SL_n(W_{r+1}), \mathcal{M}) \to H^1(K_r, \mathcal{M})^{SL_n(W_r)} \to H^2(SL_n(W_r), \mathcal{M}),$$

respectively

$$0 \to H^1(SL_n(W_r), \mathcal{M}^{K_r/Z_r}) \to H^1(SL_n(W_{r+1})/Z_r, \mathcal{M}) \to H^1(K_r/Z_r, \mathcal{M})^{SL_n(W_r)} \to H^2(SL_n(W_r), \mathcal{M}).$$

In the next proposition we examine the two terms below:

$$H^1(K_r, \mathcal{M})^{SL_n(W_r)} \text{ and } H^1(K_r/Z_r, \mathcal{M})^{SL_n(W_r)}.$$

Proposition 5.2.1. *Let $\mathcal{M}$ be one of $\mathfrak{M}_0$, $\mathfrak{V}$ or k (the latter being interpreted as isomorphic to either $\mathfrak{S}$ or $\mathfrak{M}/\mathfrak{M}_0$). There are the following isomorphisms:*

1. $H^1(K_r, \mathcal{M})^{SL_n(W_r)} \cong \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathcal{M})$
2. *If $p|n$ then* $H^1(K_r/Z_r, \mathcal{M})^{SL_n(W_r)} \cong \mathrm{Hom}_{kSL_n(k)}(\mathfrak{V}, \mathcal{M})$

Proof. First recall that K_r acts on $\mathcal{M}$ via conjugation of $\bar{\rho}$. However, as K_r is the kernel of $\bar{\rho}$ this action is trivial. Therefore Lemma 4.1.4 implies the elements of $H^1(K_r, \mathcal{M})^{SL_n(W_r)}$ are those f in $H^1(K_r, \mathcal{M}) \cong \mathrm{Hom}(K_r, \mathcal{M})$ such that $f(\kappa) = g \cdot f(g^{-1}\kappa g)$ for all $g \in SL_n(W_r)$ and $\kappa \in K_r$. This means we have the isomorphism

$$H^1(K_r, \mathcal{M})^{SL_n(W_r)} \cong \mathrm{Hom}_{kSL_n(W_r)}(K_r, \mathcal{M}).$$

Moreover, the isomorphism ϕ of equation (5.2.3) implies the isomorphisms

$$H^1(K_r, \mathcal{M})^{SL_n(W_r)} \cong \mathrm{Hom}_{kSL_n(W_r)}(\mathfrak{M}_0, \mathcal{M}) \cong \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathcal{M})$$

where the second isomorphism follows from the fact that $SL_n(W_r)$ acts on $\mathcal{M}$ by conjugation via $\bar{\rho}$.

A similar examination of $H^1(K_r/Z_r, \mathcal{M})^{SL_n(W_r)}$ utilising the isomorphism $\bar{\phi}$ leads to the isomorphism

$$H^1(K_r/Z_r, \mathcal{M}) \cong \mathrm{Hom}_{kSL_n(k)}(\mathfrak{V}, \mathcal{M}).$$

□

This brings us to the following corollary.

Corollary 5.2.2. *There are the following group isomorphisms:*

1. $H^1(K_r, \mathfrak{M}_0)^{SL_n(W_r)} \cong k$
2. $H^1(K_r, k)^{SL_n(W_r)} \cong (0)$.

If $p|n$ then there are the additional isomorphisms:

3. $H^1(K_r, \mathfrak{V})^{SL_n(W_r)} \cong k$

4. $H^1(K_r/Z_r, \mathfrak{V})^{SL_n(W_r)} \cong k$.

Proof. For part (1) we apply Proposition 5.2.1 (1) which implies

$$H^1(K_r, \mathfrak{M}_0)^{SL_n(W_r)} \cong \mathrm{Hom}_{kSL_n(k)}(\mathfrak{M}_0, \mathfrak{M}_0)$$

and the result follows from Corollary 5.1.6 (1).

For parts (2) and (3) we again apply Proposition 5.2.1 (1) and Corollary 5.1.6 (2) and (3). For part (4) we apply Proposition 5.2.1 (2) and then Corollary 5.1.6 (4). □

Chapter 6

Cohomology of $SL_n(W_r)$-modules

The objective of this chapter is to prove Theorem 6.0.3 below which is fundamental to the proof of Theorem 1.2.5. In so doing, it collates our discussions in previous chapters on group extensions and SL_n group and module structure. This chapter is partitioned into two sections; one dedicated to each part of Theorem 6.0.3.

Theorem 6.0.3. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$.*

The following hold:

1. *(a) If p does not divide n then $H^1(SL_n(W_r), \mathfrak{M}_0) = (0)$*
   (b) $H^1(SL_n(W_r), \mathfrak{M}) = (0)$ (whether or not p divides n).
2. *If $p|n$ then the map $H^2(SL_n(W_r), \mathfrak{S}) \to H^2(SL_n(W_r), \mathfrak{M}_0)$ induced from inclusion is injective.*

In this chapter great use is made of the following standard result. In fact, its use prevails in all cohomological calculations of this thesis. It is often referred to as the long exact cohomology sequence and for example may be found in [21] where it is Theorem 1.3.2.

Proposition 6.0.4. *Let G be a group and A, B, C be G-modules. If*

$$0 \to A \to B \to C \to 0$$

is an exact sequence then there is a long exact sequence of cohomology groups

$$\begin{aligned} 0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to \dots \\ \to H^n(G, C) \to H^{n+1}(G, A) \to \dots \end{aligned}$$

6.1 Proof of Part 1 of Theorem 6.0.3

In this section the 1-cohomology groups of Theorem 6.0.3 (1) are derived from base case $r = 1$, i.e. $W_r = k$, which is the next result. It is a combination of the results of Cline, Parshall and Scott in [10] for $q > 3$ and Jones in [14] for $q = 2$ or 3.

Theorem 6.1.1. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$.*

Then the following hold:

1. *If p does not divide n then $H^1(SL_n(k), \mathfrak{M}_0) = (0)$*
2. *If $p|n$ then $H^1(SL_n(k), \mathfrak{M}_0) \cong k$.*

Proof. If $q \geq 4$ the results are from Table 4.5 of [10]. Therefore, we are left to examine the cases $q = 2, 3$. We apply Proposition 6.0.4 (the long exact cohomology sequence) to the exact sequence of $SL_n(k)$-modules $0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0$ of Corollary 5.1.4. If p and n are coprime, this yields the following excerpt of the exact sequence

$$\to {\mathfrak{M}_0}^{SL_n(k)} \to \mathfrak{M}^{SL_n(k)} \xrightarrow{f'} k^{SL_n(k)} \xrightarrow{f} H^1(SL_n(k), \mathfrak{M}_0) \to H^1(SL_n(k), \mathfrak{M}) \to .$$

We simplify this sequence by noting the following: ${\mathfrak{M}_0}^{SL_n(k)} = 0$ and $\mathfrak{M}^{SL_n(k)} = \mathfrak{S}$ by Proposition 5.1.2; $k^{SL_n(k)} = k$ as the action of $SL_n(k)$ on kI is trivial; and $H^1(SL_n(k), \mathfrak{M}) = (0)$ by Proposition 8.6 of [14]. Therefore we obtain the exact sequence:

$$0 \to \mathfrak{S} \xrightarrow{f'} k \xrightarrow{f} H^1(SL_n(k), \mathfrak{M}_0) \to 0.$$

We automatically see that f' must be injective and hence it must be an isomorphism. Observe that the image of f is trivial and as the subsequent map is zero f must in fact be surjective. Therefore $H^1(SL_n(k), \mathfrak{M}_0) = (0)$.

Now assume $p|n$, we again apply Proposition 6.0.4 to $0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0$. This time we use the simplifications: ${\mathfrak{M}_0}^{SL_n(k)} = \mathfrak{S}$ and $\mathfrak{M}^{SL_n(k)} = \mathfrak{S}$ by Proposition 5.1.2; $k^{SL_n(k)} = k$ as the action of $SL_n(k)$ on kI is trivial; and $H^1(SL_n(k), \mathfrak{M}) = (0)$ by Proposition 8.6 of [14]. Therefore we obtain the exact sequence:

$$0 \to \mathfrak{S} \xrightarrow{f_0} \mathfrak{S} \xrightarrow{f'} k \xrightarrow{f} H^1(SL_n(k), \mathfrak{M}_0) \to 0.$$

The map f_0 is clearly an isomorphism hence f' is zero and f is injective. This is sufficient as the final map shows f is surjective. Hence, $H^1(SL_n(k), \mathfrak{M}_0) \cong k$. $\square$

The next stage in the proof of the theorem is to show that the $H^1(SL_n(k), \mathfrak{M}_0)$ determine the groups $H^1(SL_n(W_r), \mathfrak{M}_0)$ for all positive integers r. For this we require the following result concerning group extensions which is a combination of the work of Manoharmayum in [16], Sah in [27] and results from [12].

Proposition 6.1.2. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$.*

Let $\pi : SL_n(W_{r+1}) \to SL_n(W_r)$ be componentwise reduction modulo p^r and K_r be the kernel of π.

The exact sequence below does not split:

$$1 \to K_r \to SL_n(W_{r+1}) \xrightarrow{\pi} SL_n(W_r) \to I. \tag{6.1.1}$$

Proof. If $q \geq 4$ and in addition $(n, q) \neq (3, 4)$ then this result is Proposition 3.7 in [16]. The other cases are discussed in Proposition 4.2 of [12]: if $r = 1$ and $q = 2, 3$ then it is a result of Theorem II.7 in [27]. □

The next result completes the proof of part 1a of Theorem 6.0.3 and is also crucial to the proof of part 1b afterwards.

Proposition 6.1.3. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$.*

In addition, let $\pi : SL_n(W_{r+1}) \to SL_n(W_r)$ be componentwise reduction modulo p^r. Then the map

$$H^1(SL_n(W_r), \mathfrak{M}_0) \to H^1(SL_n(W_{r+1}), \mathfrak{M}_0)$$

induced from π is an isomorphism.

As a consequence:

$$H^1(SL_n(W_r), \mathfrak{M}_0) = \begin{cases} (0) & \text{if } p \text{ does not divide } n \\ k & \text{if } p|n. \end{cases} \tag{6.1.2}$$

Proof. We begin by applying the inflation restriction exact sequence (Proposition 4.1.6) to the exact sequence:

$$1 \to K_r \to SL_n(W_{r+1}) \xrightarrow{\pi} SL_n(W_r) \to I$$

and the $SL_n(W_{r+1})$-module $\mathfrak{M}_0$. We recall that as K_r is in the kernel of π it acts trivially on $\mathfrak{M}_0$ and also that $H^1(K_r, \mathfrak{M}_0)^{SL_n(W_r)} \cong k$ by Corollary 5.2.2. The resulting exact sequence simplifies to give:

$$0 \to H^1(SL_n(W_r), \mathfrak{M}_0) \xrightarrow{f} H^1(SL_n(W_{r+1}), \mathfrak{M}_0) \xrightarrow{f'} k \xrightarrow{\delta} H^2(SL_n(W_r), \mathfrak{M}_0) \to . \tag{6.1.3}$$

We would like to show that the inflation map f is an isomorphism; it is obviously injective so all that remains is to show its surjectivity. This equates to showing that f' is the zero map. This is itself equivalent to showing that the transgression map δ is injective.

Therefore all that is required to complete the proof is to show that δ is not the zero map. We recall the definition of the map ε from equation (5.2.4) and the extension

$$0 \to \mathfrak{M}_0 \xrightarrow{\varepsilon} \mathfrak{M}_0 \rtimes_x SL_n(W_r) \xrightarrow{\pi} SL_n(W_r) \to I$$

of equation (5.2.5). Proposition 6.1.2 implies that this extension does not split, hence the cohomology class x in $H^2(SL_n(W_r), \mathfrak{M}_0)$ which represents this extension is non trivial. Furthermore, Proposition 4.3.1 implies that the transgression map, δ, takes the map $-\phi : \mathfrak{M}_0 \rtimes_x I$ given by $-\phi(m, I) = -m$ to the class x in $H^2(SL_n(W_r), \mathfrak{M}_0)$. Thus δ is injective.

Finally, Theorem 6.1.1 implies that

$$H^1(SL_n(k), \mathfrak{M}_0) = \begin{cases} (0) & \text{if p does not divide } n \\ k & \text{if } p|n. \end{cases} \tag{6.1.4}$$

and the concluding consequence follows inductively from the isomorphism

$$H^1(SL_n(W_r), \mathfrak{M}_0) \xrightarrow{\cong} H^1(SL_n(W_{r+1}), \mathfrak{M}_0).$$

□

We reflect on the reasoning which concluded the proof of Theorem 6.1.1 in the case $q = 2$ or 3. In that instance the calculation for $H^1(SL_n(k), \mathfrak{M}_0)$ was garnered from $H^1(SL_n(k), \mathfrak{M})$ by using the long exact cohomology sequence applied to exact sequence of $SL_n(k)$-modules $0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0$. To complete the proof of part 1b of Theorem 6.0.3, we reverse this procedure relating the cohomology of $\mathfrak{M}$ to that of $\mathfrak{M}_0$ and k. This requires the following two results.

Theorem 6.1.4. *Let $n \geq 2$ be an integer and k be a finite field of characteristic p. If the following restrictions are met,*

- *if $k = \mathbb{F}_2$ then $n \geq 5$*

- *if* $k = \mathbb{F}_3$ *then* $n \geq 3$,

then $H^1(SL_n(k), k)$ *is trivial.*

If $p|n$ *and* k *satisfies one of the following:*

- $k \neq \mathbb{F}_2$
- $k = \mathbb{F}_2$ *and* $n \neq 2, 4$

then both $H^1(SL_n(k), k)$ *and* $H^2(SL_n(k), k)$ *are trivial.*

Proof. If $k \neq \mathbb{F}_2$ then the result follows from the proof of Theorem 3.5 of [16]. If $k = \mathbb{F}_2$ then the result is from [27]; $H^1(SL_n(\mathbb{F}_2), \mathbb{F}_2) = (0)$ is mentioned in the proof of Theorem II.7 and $H^2(SL_n(\mathbb{F}_2), \mathbb{F}_2) = (0)$ is contained in Proposition III.7. □

In view of the motivation preceding the statement of the theorem above we use the inflation-restriction exact sequence for the analogy of Proposition 6.1.3 where the module $\mathfrak{M}_0$ is replaced by k. As in the proof of Proposition 6.1.3, applying the inflation-restriction exact sequence (see Proposition 4.1.6) gives the exact sequence

$$0 \to H^1(SL_n(W_r), k) \to H^1(SL_n(W_{r+1}), k) \to H^1(K_r, k)^{SL_n(W_r)} \to .$$

Corollary 5.2.2 states that $H^1(K_r, k)^{SL_n(W_r)}$ is trivial and thus the inflation map $H^1(SL_n(W_r), k) \to H^1(SL_n(W_{r+1}), k)$ is an isomorphism. This discussion in conjunction with Theorem 6.1.4 has proved:

Proposition 6.1.5. *If one of the following holds*

- $n = 2$ *and* $q \geq 4$
- $n = 3$ *and* $q \geq 3$
- $n = 4$ *and* $q \geq 3$
- $n \geq 5$.

then $H^1(SL_n(W_r), k) = (0)$.

We are now ready to complete the proof of part 1 of Theorem 6.0.3.

Proof of Theorem 6.0.3 part 1b. Firstly, suppose p does not divide n. Then by Proposition 6.1.3 and Proposition 6.1.5 respectively both $H^1(SL_n(W_r), \mathfrak{M}_0)$ and $H^1(SL_n(W_r), k)$ are trivial. Then applying Proposition 6.0.4 to the direct sum decomposition $\mathfrak{M} = \mathfrak{M}_0 \oplus \mathfrak{S}$ from Corollary 5.1.4 implies $H^1(SL_n(W_r), \mathfrak{M}) = (0)$.

Secondly assume $p|n$. Again we apply Proposition 6.0.4 to the following sequence from Corollary 5.1.4: $0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0$. Recall, from the proof and statement of Theorem 6.1.1, that ${\mathfrak{M}_0}^{SL_n(k)} = \mathfrak{M}^{SL_n(k)} = \mathfrak{S}$ and $H^1(SL_n(W_r), \mathfrak{M}_0) \cong k$. Therefore there is an exact sequence beginning:

$$0 \to \mathfrak{S} \to \mathfrak{S} \xrightarrow{f_1} k \xrightarrow{\delta} k \xrightarrow{f_2} H^1(SL_n(W_r), \mathfrak{M}) \to 0.$$

The second map is obviously an isomorphism hence the image of f_1 must be zero. This implies that δ is injective and thus an isomorphism. Therefore the image of the map f_2 is zero and as the final map is the zero map f_2 is in fact an isomorphism. Thus $H^1(SL_n(W_r), \mathfrak{M}) = (0)$ in this case too. □

6.2 Proof of Part 2 of Theorem 6.0.3

In this section the injectivity of the 2-cohomology groups is proved using a similar but more involved method to that of part 1 of Theorem 6.0.3 and again centres around showing that inflation maps are isomorphisms. This involves an examination of the transgression map (see Propositions 4.3.1 and 4.1.6) and relies on the fixed first cohomology group calculations of Corollary 5.2.2.

Let $F : \mathfrak{M}_0 \to \mathfrak{V}$ be the projection map, this induces a map

$$F_0 : H^1(SL_n(W_r), \mathfrak{M}_0) \to H^1(SL_n(W_r), \mathfrak{V}).$$

In Proposition 6.2.2 we show that F_0 is an isomorphism and, as we shall see at the end of the section, the proof of Theorem 6.0.3 (2) follows easily.

We commence with a lemma, whose appearance in the proof mirrors that of Proposition 6.1.2 in the previous section.

Lemma 6.2.1. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $k = \mathbb{F}_2$ then $n \geq 5$*
- *If $k = \mathbb{F}_3$ then $n \geq 3$*
- *If $k = \mathbb{F}_5$ then $n \geq 3$*

and let $p|n$. The sequence:

$$I \to K_r/Z_r \to SL_n(W_{r+1})/Z_r \to SL_n(W_r) \to I \tag{6.2.1}$$

does not split.

Proof. If $p \geq 5$ or $r \geq 2$ then the result is Lemma 3.9 of [16]. If $r = 1$, $n \geq 3$ and $p = 2$ or 3 then the result is Proposition 4.2 part v(a) of [12]. The argument in[12] also holds true in the remaining cases. □

Now the lemma is used to prove the following proposition.

Proposition 6.2.2. *Let $p|n$ and let k satisfy one the following:*

- *$k \neq \mathbb{F}_2$*
- *$k = \mathbb{F}_2$ and $n \neq 2, 4$.*

Then the inflation map

$$H^1(SL_n(W_r), \mathfrak{V}) \to H^1(SL_n(W_{r+1}), \mathfrak{V})$$

is an isomorphism.

Consequently the map

$$F_0 : H^1(SL_n(W_r), \mathfrak{M}_0) \to H^1(SL_n(W_r), \mathfrak{V})$$

induced from the projection $F_0 : \mathfrak{M}_0 \to \mathfrak{V}$ is an isomorphism.

Proof. We begin by applying the inflation-restriction exact sequence (Proposition 4.1.6) to the group extension (6.1.1) and $\mathfrak{V}$. Noting that Corollary 5.2.2 implies $H^1(K_r, \mathfrak{V})^{SL_n(W_r)} \cong k$, this gives an exact sequence beginning

$$0 \to H^1(SL_n(W_r), \mathfrak{V}) \xrightarrow{f} H^1(SL_n(W_{r+1}), \mathfrak{V}) \xrightarrow{f'} k \xrightarrow{\delta} H^2(SL_n(W_r), \mathfrak{V}). \quad (6.2.2)$$

We are required to show f is an isomorphism. It is clearly injective so all that remains is to demonstrate surjectivity. If δ is injective then the image of f' is trivial and the result follows. We proceed to show δ is injective.

Firstly, suppose that $n \geq 3$. Apply Proposition 4.1.6 to the sequence (6.2.1) and the $SL_n(W_{r+1})/Z_r$-module, $\mathfrak{V}$. As $H^1(K_r/Z_r, \mathfrak{V})^{SL_n(W_r)} \cong k$ by Corollary 5.2.2, this yields the exact sequence beginning

$$0 \to H^1(SL_n(W_r), \mathfrak{V}) \to H^1(SL_n(W_{r+1})/Z_r, \mathfrak{V}) \to k \xrightarrow{\delta'} H^2(SL_n(W_r), \mathfrak{V}). \quad (6.2.3)$$

Lemma 6.2.1 implies $H^2(SL_n(W_r), \mathfrak{V})$ is non-trivial. Next we show that δ' is injective. To this end, recall the isomorphism $\phi' : K_r/Z_r \to \mathfrak{V}$ and its one-sided inverse $\varepsilon' : \mathfrak{V} \to SL_n(W_{r+1})/Z_r$ from the discussion preceding equation (5.2.8). Also recall that the group extension (6.2.1) may be written additively as:

$$0 \to \mathfrak{V} \xrightarrow{\varepsilon'} \mathfrak{V} \rtimes_y SL_n(W_r) \xrightarrow{\pi'} SL_n(W_r) \to I. \quad (6.2.4)$$

Proposition 4.3.1 then implies that δ' maps $-\phi'$ to the class of y in $H^2(SL_n(W_r), \mathfrak{V})$ and is thus injective. The map δ is shown to be injective by Corollary 5.2.2 which provides the isomorphism

$$H^1(K_r, \mathfrak{V})^{SL_n(W_r)} \cong H^1(K_r/Z_r, \mathfrak{V})^{SL_n(W_r)}.$$

Secondly, let $n = 2$, $r = 1$ and k be a field of cardinality 2^d where $d \geq 2$. We have the following commutative diagram:

$$\begin{array}{ccc} H^1(K_1, \mathfrak{M}_0)^{SL_2(k)} & \xrightarrow{\delta'} & H^2(SL_2(k), \mathfrak{M}_0) \\ \downarrow f & & \downarrow f' \\ H^1(K_1, \mathfrak{V})^{SL_2(k)} & \xrightarrow{\delta} & H^2(SL_2(k), \mathfrak{V}). \end{array}$$

We begin by investigating the arrows stemming from $H^1(K_1, \mathfrak{M}_0)^{SL_2(k)}$. Corollary 5.2.2 implies the map f is an isomorphism and the proof of Proposition 6.1.3

shows that δ is injective. Our attention turns to f'. Proposition 6.0.4 is applied to the exact sequence $0 \to \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{V} \to 0$ resulting in the following excerpt of an exact sequence

$$\to H^2(SL_2(k), \mathfrak{S}) \to H^2(SL_2(k), \mathfrak{M}_0) \xrightarrow{f'} H^2(SL_2(k), \mathfrak{V}) \to .$$

Theorem 6.1.1 implies that the first group quoted in this sequence is trivial. Therefore f' must be injective. We remark that by Corollary 5.2.2 $H^1(K_1, \mathfrak{M}_0)^{SL_2(k)}$ is one-dimensional and thus both δ' and f' are injective. Therefore the map δ must be injective.

We conclude by showing that $F_0 : H^1(SL_n(W_r), \mathfrak{M}_0) \cong H^1(SL_n(W_r), \mathfrak{V})$. To begin with, we apply the long exact cohomology sequence (Proposition 6.0.4) to the exact sequence of $SL_n(k)$ modules

$$0 \to \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{V} \to 0.$$

This gives the excerpt of an exact cohomological sequence:

$$\to H^1(SL_n(k), \mathfrak{S}) \to H^1(SL_n(k), \mathfrak{M}_0) \to H^1(SL_n(k), \mathfrak{V}) \to H^2(SL_n(k), \mathfrak{S}) \to$$

Given the restrictions imposed on n we can invoke Theorem 6.1.4 which implies that both $H^1(SL_n(k), \mathfrak{S})$ and $H^2(SL_n(k), \mathfrak{S})$ are trivial. Therefore we have shown that $F_0 : H^1(SL_n(k), \mathfrak{M}_0) \cong H^1(SL_n(k), \mathfrak{V})$, i.e. the case $r = 1$. Let's rename this isomorphism $\phi_1 : H^1(SL_n(k), \mathfrak{M}_0) \cong H^1(SL_n(k), \mathfrak{V})$, it will serve as the base case for an inductive argument on r. To prove the inductive step assume there is an isomorphism $\phi_r : H^1(SL_n(W_r), \mathfrak{M}_0) \cong H^1(SL_n(W_r), \mathfrak{V})$. In addition, recall we have already shown that the inflation map $H^1(SL_n(W_r), \mathfrak{V}) \xrightarrow{\cong} H^1(SL_n(W_{r+1}), \mathfrak{V})$ is an isomorphism earlier in this proof and that the inflation map $H^1(SL_n(W_r), \mathfrak{M}_0) \xrightarrow{\cong} H^1(SL_n(W_{r+1}), \mathfrak{M}_0)$ is an isomorphism in Proposition 6.1.3. Therefore we obtain the following commutative diagram:

$$\begin{array}{ccc} H^1(SL_n(W_r), \mathfrak{M}_0) & \xrightarrow{\phi_r} & H^1(SL_n(W_r), \mathfrak{V}) \\ \downarrow \cong & & \downarrow \cong \\ H^1(SL_n(W_{r+1}), \mathfrak{M}_0) & \xrightarrow{\phi_{r+1}} & H^1(SL_n(W_{r+1}), \mathfrak{V}). \end{array}$$

from which it is clear that the map ϕ_{r+1} must also be an isomorphism, thus completing the inductive step. Therefore $F_0 : H^1(SL_n(W_r), \mathfrak{M}_0) \cong H^1(SL_n(W_r), \mathfrak{V})$ for all r. □

Proof of Theorem 6.0.3 (2). Recall the exact sequence $0 \to \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{V} \to 0$ of Corollary 5.1.4 and apply Proposition 6.0.4 (long exact cohomology sequence) to it. This yields the following excerpt of an exact sequence

$$\begin{aligned} \to H^1(SL_n(W_r), \mathfrak{M}_0) &\xrightarrow{F_0} H^1(SL_n(W_r), \mathfrak{V}) \xrightarrow{F'} \\ H^2(SL_n(W_r), \mathfrak{S}) &\xrightarrow{F} H^2(SL_n(W_r), \mathfrak{M}_0) \to . \end{aligned}$$

Proposition 6.2.2 implies that $F_0 : H^1(SL_n(W_r), \mathfrak{M}_0) \to H^1(SL_n(W_r), \mathfrak{V})$ is an isomorphism. Thus the image of F' is trivial and hence F, induced from the inclusion $\mathfrak{S} \to \mathfrak{M}_0$, is injective. □

Chapter 7

Proof of Theorem 1.2.5

As we shall see, the proof of Theorem 1.2.5 follows from Proposition 7.0.5. This proposition deals only with artinian rings in $\mathcal{C}(k)$ and before its statement we give a basic introduction to artinian rings.

Definition 7.0.3. A noetherian ring is called *artinian* if it satisfies the *descending* chain condition on ideals i.e. any chain of ideals of A:

$$I_1 \supseteq I_2 \supseteq \dots$$

eventually stabilises.

Suppose that (A, m_A) is an artinian local ring, then considering a descending chain of successive power of m_A leads to the following observation which is significant to Proposition 7.0.5.

Lemma 7.0.4. *Let (A, m_A) be a noetherian local ring, then A is artinian iff there exists a natural number n such that $m_A^n = 0$. Consequently the annihilator of m_A is non trivial.*

Proof. If A is artinian, then considering the descending chain

$$m_A \supseteq m_A^2 \supseteq \dots$$

implies that $m_A^n = m_A^{n+1}$ for some n. Nakayama's lemma then implies $m_A^n = 0$. Conversely, if a noetherian ring (A, m_A) has $m_A^n = 0$ then as every ideal is finitely generated and every generator is nilpotent, every descending chain must stabilise. □

Let A be an artinian element of $\mathcal{C}(k)$. Then Lemma 7.0.4 implies the existence of a non-zero element t of A which annihilates m_A. This element generates an ideal in A which is denoted (t), therefore reduction modulo (t) defines a local ring homomorphism $\pi : A \to A/(t)$ and hence a group homomorphism $\pi : GL_n(A) \to GL_n(A/(t))$.

Proposition 7.0.5. *Let $n \geq 2$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If* $k = \mathbb{F}_2$ *then* $n \geq 5$
- *If* $k = \mathbb{F}_3$ *then* $n \geq 3$
- *If* $k = \mathbb{F}_5$ *then* $n \geq 3$.

Let (A, m_A) *be an artinian ring in* $\mathcal{C}(k)$ *and* $t \in A$ *be a non-zero element such that* $tm_A = 0$. *If* G *is a subgroup of* $SL_n(A)$ *with the property* $G \mod t = SL_n(W_{A/(t)})$, *then there exists an* $X \in GL_n(A)$ *with* $X \equiv I \pmod t$ *such that* $SL_n(W_A) \subseteq XGX^{-1}$.

Proof. We set $B := A/(t)$ and $\pi : A \to B$ to be reduction modulo t. Recall, from the discussion preceding equation (5.2.4), the contruction of the map $\varepsilon : \mathfrak{M}_0 \to SL_n(A)$ by lifting $M \in \mathfrak{M}_0$ to $\widetilde{M} \in M_n(A)$ with trace zero and then taking $\varepsilon(M) := I + t\widetilde{M}$. Therefore there is an exact sequence

$$0 \to \mathfrak{M}_0 \xrightarrow{\varepsilon} SL_n(A) \xrightarrow{\pi} SL_n(B) \to I \tag{7.0.1}$$

Let $\widetilde{G}$ denote the pre-image under π of $SL_n(W_B)$ in $SL_n(A)$ this defines the following exact sequence:

$$0 \to \mathfrak{M}_0 \xrightarrow{\varepsilon} \widetilde{G} \xrightarrow{\pi} SL_n(W_B) \to I. \tag{7.0.2}$$

We observe that both G and $SL_n(W_A)$ are subgroups of $\widetilde{G}$ and examine the possible subgroup structures relating these three. From sequence (7.0.2) we see that a subgroup of $\widetilde{G}$ specifies a corresponding submodule of $\mathfrak{M}_0$. Hence Proposition 5.1.2 leads us to consider the following three possibilities:

1. $G = \widetilde{G}$, in which case $SL_n(W_A) \subseteq G$ and we are finished.
2. $\pi : G \to SL_n(W_B)$ is an isomorphism.
3. If $p|n$ then G may fit into the exact sequence $0 \to \mathfrak{S} \to G \to SL_n(W_B) \to I$.

Let's investigate case 2. Suppose $\pi : G \to SL_n(W_B)$ is an isomorphism which implies that the sequence (7.0.2) splits. If we first assume that $SL_n(W_A)$ is not isomorphic to $SL_n(W_B)$ then, as $\mathfrak{M}_0$ is irreducible by Theorem 6.0.3 (1(a)), $SL_n(W_A) \cong \widetilde{G} \cong \mathfrak{M}_0 \rtimes SL_n(W_B)$. However, as the sequence splits this leads to a contradiction of Proposition 6.1.2. Therefore, the projection map $\pi : SL_n(W_A) \to SL_n(W_B)$ must also be an isomorphism and G is a twist of $SL_n(W_A)$ by an element of $H^1(SL_n(W_B), \mathfrak{M}_0)$.

If p and n are coprime, then Theorem 6.0.3 (1(a)) implies that $H^1(SL_n(W_B), \mathfrak{M}_0) = (0)$ and Proposition 5.1.2 (i) implies that $\mathfrak{M}_0$ is irreducible (hence trivially for all submodules $\mathcal{N} \leq \mathfrak{M}_0$ the maps $H^2(SL_n(W_B), \mathcal{N}) \to H^2(SL_n(W_B), \mathfrak{M}_0)$ are injective). This allows us to invoke Proposition 4.3.3 (3) which implies that there exists $X \in SL_n(A)$ with $\pi(X) = I$ such that $XGX^{-1} \supseteq SL_n(W_A)$.

If p divides n then we define a subgroup $G' < GL_n(A)$ by the exact sequence

$$0 \to \mathfrak{M} \to G' \to SL_n(W_B) \to I.$$

Next, we show that for all $kSL_n(W_r)$-submodules $\mathcal{N} \leq \mathfrak{M}$ the maps

$$H^2(SL_n(W_r), \mathcal{N}) \to H^2(SL_n(W_r), \mathfrak{M})$$

induced from inclusion are injective. Recall that Theorem 6.0.3 (2) allows us to assume that the map $H^2(SL_n(W_B), \mathfrak{S}) \to H^2(SL_n(W_B), \mathfrak{M}_0)$ induced from $\mathfrak{S} \hookrightarrow \mathfrak{M}_0$ is injective. Therefore, all that remains is to show that the map $H^2(SL_nW(_B), \mathfrak{M}_0) \to H^2(SL_n(W_B), \mathfrak{M})$ induced from $\mathfrak{M}_0 \hookrightarrow \mathfrak{M}$ is injective. To this end, Proposition 6.0.4 is applied to the exact sequence

$$0 \to \mathfrak{M}_0 \to \mathfrak{M} \to k \to 0.$$

This yields the following excerpt of an exact sequence

$$\to H^1(SL_n(W_B), k) \to H^2(SL_n(W_B), \mathfrak{M}_0) \to H^2(SL_n(W_B), \mathfrak{M}) \to . \qquad (7.0.3)$$

Recall that Theorem 6.1.4 implies the first group in this sequence is trivial, hence the map $H^2(SL_nW(_B), \mathfrak{M}_0) \to H^2(SL_n(W_B), \mathfrak{M})$ induced from $\mathfrak{M}_0 \hookrightarrow \mathfrak{M}$ is injective. Recall also that Theorem 6.0.3 (1(b)) implies $H^1(SL_n(W_B), \mathfrak{M}) = (0)$ which allows us to again invoke Proposition 4.3.3. Therefore, in an analogous fashion an $X \in GL_n(A)$ is found for which $\pi(X) = I$ and $XGX^{-1} = SL_n(W_A)$.

Finally, we consider case 3 hence G is part of the exact sequence:

$$0 \to \mathfrak{S} \to G \to SL_n(W_B) \to I. \qquad (7.0.4)$$

Theorem 6.0.3 part 2 implies that the map

$$H^2(SL_n(W_B), \mathfrak{S}) \to H^2(SL_n(W_B), \mathfrak{M}_0)$$

induced from $\mathfrak{S} \hookrightarrow \mathfrak{M}_0$ is injective. Therefore, the sequence (7.0.2) splits if and only if sequence (7.0.4) splits. If we assume that $W_A = W_{r+1}$ and $W_B = W_r$ for some natural number r then sequence (7.0.4) defines an isomorphism

$$f : SL_n(W_r) \to G/Z_r$$

which is a section for π. This implies the sequence (6.2.1) splits which leads to a contradiction to Lemma 6.2.1. Therefore, $W_A = W_B$ and the result follows using $H^1(SL_n(W_B), \mathfrak{M}) = 0$ as above. □

We proceed to show how Theorem 1.2.5 follows from Proposition 7.0.5. The artinian objects in $\mathcal{C}(k)$ form a full subcategory and the objects in $\mathcal{C}(k)$ are the inverse limit of their artinian quotients i.e. a ring $A, m_A \in \mathcal{C}(k)$ has the form

$$A = \varprojlim A^i$$

where the $A^i = A/m_A^i$ are artinian quotients of A. Following Schlessinger, in [29] Definition 1.2, we introduce the following.

Definition 7.0.6. Let (A, m_A) and (B, m_B) be artinian elements of $\mathcal{C}(k)$. An exact sequence of the form:

$$0 \to J \to A \to B \to 0 \tag{7.0.5}$$

is called a small extension if J is a non-zero principal ideal which is annihilated by m_A.

We remark that if (A, m_A) and (B, m_B) are artinian and fit into an exact sequence:

$$0 \to J \to A \to B \to 0$$

where $m_A J = (0)$ then J is a finite dimensional vector space over k. Thus, in this situation, we may write $J = (t_1, t_2, \ldots, t_n)$ and the following is a series of small extensions:

$$\begin{aligned}
0 \to (t_1) \to A \to A/(t_1) \to 0 \\
0 \to \frac{(t_2, t_1)}{(t_1)} \to \frac{A}{(t_1))} \to \frac{A}{(t_1, t_2)} \to 0 \\
\vdots \\
0 \to \frac{(t_1, \ldots, t_i)}{(t_1, \ldots, t_{i-1})} \to \frac{A}{(t_1, \ldots, t_{i-1})} \to \frac{A}{(t_1, \ldots, t_i)} \to 0 \\
\vdots \\
0 \to \frac{J}{(t_1, ..., t_{n-1})} \to \frac{A}{(t_1, ..., t_{n-1})} \to \frac{A}{J} = B \to 0
\end{aligned}$$

Now let (A, m_A) be an arbitrary element of $\mathcal{C}(k)$ then as A/m_A^r is artinian we may apply the argument to obtain a refinement of

$$m_A \supseteq m_A^2 \supseteq m_A^3 \supseteq \ldots$$

of the form:

$$m_A = J_1 \supseteq J_2 \supseteq J_3 \ldots$$

so that extensions of the form:

$$0 \to \frac{J_n}{J_{n+1}} \to \frac{A}{J_{n+1}} \to \frac{A}{J_n} \to 0$$

are small and so that $A = \varprojlim A/J_n$. We are now in a position to complete the proof of the theorem.

Proof of Theorem 1.2.5. Let $m_A = J_1 \supseteq J_2 \supseteq J_3 \ldots$ be a refinement of $m_A \supseteq m_A^2 \supseteq m_A^3 \supseteq \ldots$ as described above. In addition, let $G < SL_n(A)$ satisfy $G \bmod m_A = SL_n(k)$. Suppose that $X_r \in GL_n(A/J_r)$ is such that

$$X_r G X_r^{-1} \bmod J_r \supseteq SL_n(W_A) \bmod J_r$$

and that $\tilde{X}_r$ is a lift of X_r to $GL_n(A/J_{r+1})$. Then by Proposition 1 there exists $Y \in GL_n(A)$ with $Y \equiv I \bmod J_s$ for all s, such that

$$Y(\tilde{X}_r G \tilde{X}_r^{-1})Y^{-1} \bmod J_{r+1} \supseteq SL_n(W_A) \bmod J_{r+1}.$$

Therefore let $X_{r+1} = Y\tilde{X}_r$ which implies that $X_{r+1} \bmod J_r = X_r$. Thus we can define inductively $X \in GL_n(A)$ satisfying $X \bmod J_r = X_r$ with the properties in the theorem. $\square$

Chapter 8

Main Results Using Symplectic Groups

The next five chapters are devoted to a new proof of the affirmative answer to the inverse deformation problem. This result is given in Main Theorem 2 by using the family of symplectic groups.

Definition 8.0.7. Let $n \geq 1$ be an integer, I_n be the $n \times n$ identity matrix and define the matrix:

$$J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

The symplectic group of dimension $2n$ over a ring A is defined as

$$SP_{2n}(A) = \{g \in GL_{2n}(A) \mid g^T J_n g = J_n\}. \tag{8.0.1}$$

We remark that if $n = 1$ there is a well known coincidence of $SL_2(A)$ and $SP_2(A)$ which we now explain. Let

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SP_2(A)$$

The symplectic condition becomes

$$g^T J g = \begin{pmatrix} 0 & ad - bc \\ -(ad - bc) & 0 \end{pmatrix} = J$$

from which it is clear that the only restriction on g is that it have determinant 1, i.e. it belongs to $SL_2(A)$. In general, see Corollary 9.1.4, $SP_{2n}(A) \leq SL_{2n}(A)$.

Let k be a finite field with characteristic p where $|k| = 4$ or $|k| \geq 7$. Also let $A \in \mathcal{C}(k)$, $\Gamma = SL_2(A)$ and $\bar{\rho} : \Gamma \to GL_2(k)$ be reduction modulo m_A of the standard representation $\rho_A : \Gamma \to SL_2(A)$. Then Main Theorem 1 implies that ρ_A is the universal deformation and A the universal deformation ring for the deformation problem defined by Γ and $\bar{\rho}$. It is natural to ask if the same holds for SP_{2n}.

Main Theorem 2. *Let $k = \mathbb{F}_q$ where the characteristic of k is p. Then if $q \geq 4$ every element of $\mathcal{C}(k)$ is a universal deformation ring of the residual representation $\bar{\rho} : SP_{2n}(A) \to GL_{2n}(k)$ given by reducing the standard representation $\rho_A : SP_{2n}(A) \to SP_{2n}(A)$ modulo m_A.*

More precisely, for the deformation problem described in this theorem we show that A is the universal deformation ring in the following cases:

1. *$n = 1$ and $q \neq 2$, 3 or 5*

2. *$n \geq 2$, $p \geq 3$, $q \geq 5$ and p is coprime to n.*

The main constituent to the proof of Main Theorem 2 is the following structural property which is a direct analogy to Theorem 1.2.5 in the symplectic group setting.

Main Theorem 3. *Let (B, m_B) belong to $\mathcal{C}(k)$. Let $n \geq 1$ be an integer, p a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions:*

- *If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and p is coprime to n*

and let G be a closed subgroup of $SL_{2n}(B)$. If $G \bmod m_B = SP_{2n}(k)$, then there exists an $X \in GL_{2n}(B)$ satisfying $X \equiv I \bmod m_B$ such that $XGX^{-1} \supseteq SP_{2n}(W_B)$.

The final principal result is Main Theorem 4 in Chapter 14 which answers the inverse symplectic deformation problem formulated in Section 14.1.

Chapter 9

Symplectic Groups

This chapter provides an account of the group theoretic structure of symplectic groups over local rings in a manner akin to Chapter 2. To begin with, the notation for the different types of symplectic group elements is set. Then later in Section 9.1 a generating set for $SP_{2n}(A)$ is found. The next section discusses the subgroup structure of SP_{2n} including a description of a p-sylow subgroup of $SP_{2n}(k)$ and an important subgroup Ω which contains it. Finally, in Section 9.4 the commutator relations for the generating elements are given and are used to determine which of the $SP_{2n}(A)$ are perfect.

9.1 Generating Sets for Symplectic Groups

In this section a subgroup $F(2n, A)$ of $SL_{2n}(A)$ is introduced which, like the elementary matrices in special linear groups, provides a set of generators for $SP_{2n}(A)$. Before continuing we note that from now on we write $J := J_n$ and $I := I_n$ suppressing the dependence on n. This brings us to fixing the notation used for the elements of $F(2n, A)$.

Lemma 9.1.1. *Let x be an arbitrary element of A and let $1 \leq i, j \leq n$ be distinct. Each of the following matrices is symplectic:*

$$\begin{aligned}
E_i(x) &:= E_{i,n+i}(x) \\
E_{n+i}(x) &:= E_{n+i,i}(x) \\
F_{ij}(x) &:= \begin{pmatrix} E_{ij}(x) & 0 \\ 0 & E_{ji}(-x) \end{pmatrix} \\
G_{ij}(x) &:= \begin{pmatrix} I & x(e_{ij}+e_{ji}) \\ 0 & I \end{pmatrix} \\
H_{ij}(x) &:= \begin{pmatrix} I & 0 \\ x(e_{ij}+e_{ji}) & I \end{pmatrix}.
\end{aligned}$$

Proof. Let S be a symmetric $n \times n$ matrix then

$$\begin{pmatrix} I & 0 \\ S & I \end{pmatrix} J \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} = \begin{pmatrix} 0 & I \\ -I & -S+S \end{pmatrix}$$

from which it is clear that $E_i(x)$, $E_{n+i}(x)$, $G_{ij}(x)$ and $H_{ij}(x)$ are symplectic matrices. For the $F_{ij}(x)$ the result follows from the equality:

$$\begin{aligned} F_{ij}(x)JF_{ij}(x)^T &= \begin{pmatrix} E_{ij}(x) & 0 \\ 0 & E_{ji}(-x) \end{pmatrix} J \begin{pmatrix} E_{ji}(x) & 0 \\ 0 & E_{ij}(-x) \end{pmatrix} \\ &= \begin{pmatrix} 0 & E_{ij}(x)E_{ij}(-x) \\ -E_{ji}(-x)E_{ji}(x) & 0 \end{pmatrix} \end{aligned}$$

□

With this notation in place the following definition introduces the group generated by all elements described in Lemma 9.1.1.

Definition 9.1.2. We define the group:

$$F(2n, A) = < E_i(A),\ E_{n+i}(A),\ F_{ij}(A),\ G_{ij}(A) \text{ and } H_{ij}(A) \mid \forall\ 1 \leq i \neq j \leq n > .$$

As all the elements which generate $F(2n, A)$ are all symplectic this group is a priori a subgroup of $SP_{2n}(A)$. Moreover, we will see that $SP_{2n}(A)$ and $F(2n, A)$ coincide. The proof relies on the next result which is from Section 2.2 of [22].

Theorem 9.1.3. *If k is a finite field then $F(2n, k) = SP_{2n}(k)$.*

Corollary 9.1.4. *If k is a finite field and A belongs to $\mathcal{C}(k)$ then $F(2n, A) = SP_{2n}(A)$.*

Proof. The method is analogous to that of Corollary 2.1.3; we show that for every element g of $SP_{2n}(A)$ there exist two products, L and R, of elements of $F(2n, A)$ satisfying $LgR = I$.

Theorem 9.1.3 implies the existence of matrices L and R such that $LgR = I+M$ where M belongs to $M_{2n}(m_A)$. The element $I + M$ is composed of $n \times n$ blocks of the form

$$\begin{pmatrix} I + A' & B' \\ C' & I + D' \end{pmatrix}.$$

Corollary 2.1.3 allows us to assume that A' is zero (for more details see the discussion around equation (2.1.1)). Therefore we obtain a matrix of the form:

$$\tilde{g} = \begin{pmatrix} I & B \\ C & I + D \end{pmatrix}.$$

As this matrix belongs to $SP_{2n}(A)$ we have the equality:

$$\tilde{g}^t J \tilde{g} = \begin{pmatrix} C - C^t & I + D - C^t B \\ -I - D^t + B^t C & B^t + B^t D - B - D^t B \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This implies the following conditions:

$$\begin{aligned} C &= C^t \\ D &= C^t B \\ B^t - B &= D^t B - B^t D. \end{aligned}$$

Substituting the first into the second gives $D = CB$ and substituting this into the third equality gives:

$$B^t - B = (CB)^t B - B^t(CB) = B^t CB - B^t CB = 0.$$

Thus B and C are symmetric. Let $S = (s_{ij})$ be an arbitrary symmetric matrix in $M_n(A)$. If we set $\lambda_i = s_{ii}$ and $\mu_{jk} = s_{jk}$ for $j < k$ then there are the following equalities

$$\begin{pmatrix} I & 0 \\ S & I \end{pmatrix} = \left(\prod_{i=1}^{n} E_{n+i}(\lambda_i) \right) \left(\prod_{j<k} H_{jk}(\mu_{jk}) \right),$$

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix} = \left(\prod_{i=1}^{n} E_{i}(\lambda_i) \right) \left(\prod_{j<k} G_{jk}(\mu_{jk}) \right).$$

If the matrix S is set to both $-B$ and $-C$ separately; then the following observation completes the proof:

$$\begin{pmatrix} I & 0 \\ -C & I \end{pmatrix} \tilde{g} \begin{pmatrix} I & -B \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & 0 \\ -C & I \end{pmatrix} \begin{pmatrix} I & B \\ C & I + CB \end{pmatrix} \begin{pmatrix} I & -B \\ 0 & I \end{pmatrix} = I.$$

□

9.2 Subgroups of $SP_{2n}(\mathbb{F}_q)$

Let p be a prime and $\mathbb{F}_q$ the finite field with $q = p^d$ elements. In this section we construct subgroups N, G and Ω of $SP_{2n}(\mathbb{F}_q)$ such that $\Omega = N \rtimes G$ contains the p-sylow subgroup of $SP_{2n}(\mathbb{F}_q)$. To this end we state the following order formula for symplectic groups which is Theorem 3.1.2 of [22].

Proposition 9.2.1. *If $\mathbb{F}_q$ is the finite field with $q = p^d$ elements then:*

$$|SP_{2n}(\mathbb{F}_q)| = \prod_{i=1}^{n} (q^{2i} - 1) q^{2i-1}.$$

Next we introduce sylow subgroups. Let l be a prime, r an integer coprime to l and H a group of order $l^\mu r$. If $H' < H$ has order l^μ then H' is called an *l-sylow subgroup* of H. The basic theory of these subgroups ensures that l-sylow

subgroups exist and that all such subgroups are conjugate. For a detailed account of these subgroups consult Chapter 3 in [1].

Our attention turns to finding a p-sylow subgroup for $SP_{2n}(k)$. Proposition 9.2.1 implies that a p-sylow subgroup of $SP_{2n}(\mathbb{F}_q)$ has order

$$q^{\sum_{i=1}^{n} 2i-1} = q^{n(n+1)-n} = q^{n^2}.$$

Observe that the elements $F_{ij}(x)$ are an embedding of $SL_n(\mathbb{F}_q)$ as a subgroup of $SP_{2n}(\mathbb{F}_q)$. The order of this subgroup is given by the formula

$$(q-1)^{-1} \prod_{i=0}^{n-1} (q^n - q^i).$$

The subgroup of $SP_{2n}(k)$ isomorphic to $SL_n(k)$ has a p-sylow subgroup of order

$$q^1 q^2 \dots q^{n-1} = q^{n(n-1)/2}.$$

If U represents a p-sylow subgroup of $SL_n(\mathbb{F}_q)$, then U may be taken to be the subgroup of upper triangular matrices with 1s on the diagonal (see Chapter 7 of [1] for example). Clearly U can be embedded in $SP_{2n}(k)$ using the restriction of the embedding of $SL_n(k)$, i.e. let u be belong to U and let $u \mapsto \tilde{u}$ where

$$\tilde{u} = \begin{pmatrix} u & 0 \\ 0 & u^{-T} \end{pmatrix}. \tag{9.2.1}$$

The image of this embedding in $SP_{2n}(\mathbb{F}_q)$ is written $\tilde{U}$; it forms a subgroup of the p-sylow subgroup. As we shall see, the p-sylow subgroup of $SP_{2n}(\mathbb{F}_q)$ has the form of the semidirect product $N \rtimes \tilde{U}$. This leads us to the definition of the subgroup N which is an abelian normal subgroup of the p-sylow subgroup.

Definition 9.2.2. Let N be the abelian group generated by elements of the form $E_i(1)$ and $G_{rs}(1)$.

If S be a symmetric $n \times n$ matrix then N consists of all matrices of the form

$$n = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}.$$

It is clear that N has order $q^{n(n+1)/2}$ and that the intersection of N with $\tilde{U}$ is trivial. We show that $\tilde{U}$ acts on N via conjugation. Let $n \in N$, $\tilde{u} \in U$ and consider the equality

$$\tilde{u}n\tilde{u}^{-1} = \begin{pmatrix} I & uSu^T \\ 0 & I \end{pmatrix}. \tag{9.2.2}$$

As $(uSu^T)^T = uSu^T$ the element $\tilde{u}n\tilde{u}^{-1}$ belongs to N. Therefore, we can form the semidirect product $N \rtimes \tilde{U}$ which has order

$$|N|.|\tilde{U}| = q^{n(n+1)/2} q^{n(n-1)/2} = q^{n^2}.$$

Thus we have shown the following result.

Lemma 9.2.3. *Let N and $\tilde{U}$ be the subgroups of $SP_{2n}(\mathbb{F}_q)$ as above. The subgroup of $SP_{2n}(\mathbb{F}_q)$ they generate is the semidirect product $N \rtimes \tilde{U}$ which is the p-sylow subgroup of $SP_{2n}(\mathbb{F}_q)$.*

In the calculations of Chapter 12 we will make use of a certain subgroup Ω containing the p-sylow subgroup $N \rtimes \tilde{U}$ which we now introduce. The identification given in equation (9.2.1) extends to an embedding of $GL_n(\mathbb{F}_q)$ in $SP_{2n}(\mathbb{F}_q)$, the image of which we denote G. The intersection of G and $\tilde{U}$ is again trivial and the conjugation in equation (9.2.2) extends naturally to G i.e. G acts on N via conjugation.

Definition 9.2.4. Define the following subgroup of $SP_{2n}(\mathbb{F}_q)$:

$$G = \left\{ \begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix} \mid g \in GL_n(\mathbb{F}_q \right\}.$$

As $G \bigcap N = I$ the discussion above allows us to make the definition:

$$\Omega := N \rtimes G.$$

This section is concluded by observing that

$$\sigma(rs) := \begin{pmatrix} (rs) & 0 \\ 0 & (rs) \end{pmatrix} \tag{9.2.3}$$

defines an embedding of S_n in $SP_{2n}(\mathbb{F}_q)$ where (rs) are the transpositions of Definition 2.3.1 (noting that $(rs)^{-T} = (rs)$).

9.3 More on General Linear Groups

Motivated by the embedding of $GL_n(\mathbb{F}_q)$ in $SP_{2n}(\mathbb{F}_q)$, we outline some basic facts about general linear groups. For further details on this material see [1]. Recall that if $n \geq 3$ we have the Steinberg relations which shall be denoted $\mathcal{S}$.

Definition 9.3.1. Let λ be a non-zero element of k and define an integer $n(\lambda)$ by $\lambda^{n(\lambda)} = 1$. The following set of variations are denoted $\mathcal{T}$.

(1) $D_r(\lambda)^{n(\lambda)} = I$

(2) $D_r(\lambda)D_s(\mu) = D_s(\mu)D_r(\lambda)$

Definition 9.3.2. If λ, μ be non-zero elements of k then the following set of relations are called $\mathcal{U}$.

(1) $D_r(\lambda)E_{ij}(\mu)D_r(\lambda^{-1}) = E_{ij}(\mu)$ if $r \neq i, j$

(2) $D_i(\lambda)E_{ij}(\mu)D_i(\lambda^{-1}) = E_{ij}(\lambda\mu)$

(3) $D_j(\lambda)E_{ij}(\mu)D_j(\lambda^{-1}) = E_{ij}(\lambda^{-1}\mu)$

Theorem 9.3.3. *Let μ, λ, $E_{ij}(\mu)$ and $D_r(\lambda)$ be as above. If $n \geq 3$ then we have the presentation:*

$$GL_n(k) =< E_{ij}(\mu), D_r(\lambda) \mid \mathcal{S},\ \mathcal{T},\ \mathcal{U} > . \tag{9.3.1}$$

9.4 Commutator Subgroups of Symplectic Groups

As in the case of special linear groups, commutator relations play an important role in the calculation of deformation rings for symplectic groups. Not least, because the relations in the proposition below show that for almost all pairs (n, k) $SP_{2n}(A)$ is a perfect group.

Proposition 9.4.1. *Let λ and μ be arbitrary elements of A. There are the following commutator relations for the elements generating $SP_{2n}(A)$:*

1. $[E_i(\lambda), E_j(\mu)] = 1$
2. $[E_i(\lambda), E_{n+j}(\mu)] = \begin{cases} M_1 & \text{if } i = j \\ 1 & \text{if } j \neq i \end{cases}$
3. $[E_i(\lambda), F_{rs}(\mu)] = \begin{cases} 1 & \text{if } s \neq i \\ G_{ir}(-\lambda\mu)E_r(-\lambda\mu^2) & \text{if } s = i \end{cases}$
4. $[E_i(\lambda), G_{rs}(\mu)] = 1$
5. $[E_i(\lambda), H_{rs}(\mu)] = \begin{cases} F_{is}(\lambda\mu)E_{n+s}(\lambda\mu^2) & \text{if } r = i \\ F_{ir}(\lambda\mu)E_{n+r}(\lambda\mu^2) & \text{if } s = i \\ 1 & \text{if } r, s \neq i \end{cases}$
6. $[E_{n+i}(\lambda), E_{n+j}(\mu)] = 1$
7. $[E_{n+i}(\lambda), F_{rs}(\mu)] = \begin{cases} H_{is}(\lambda\mu)E_{n+s}(-\lambda\mu^2) & \text{if } r = i \\ 1 & \text{if } r \neq i \end{cases}$
8. $[E_{n+i}(\lambda), G_{rs}(\mu)] = \begin{cases} F_{si}(-\lambda\mu)E_s(\lambda\mu^2) & \text{if } r = i \\ F_{ri}(-\lambda\mu)E_r(\lambda\mu^2) & \text{if } s = i \\ 1 & \text{if } r, s \neq i \end{cases}$
9. $[E_{n+i}(\lambda), H_{rs}(\mu)] = 1$
10. $[F_{ij}(\lambda), F_{rs}(\mu)] = \begin{cases} F_{is}(\lambda\mu) & \text{if } r = j \text{ and } s \neq i \\ M_2 & \text{if } r = j \text{ and } s = i \\ 1 & \text{if } r = i \text{ and } s = j \\ 1 & \text{if } r \neq j \text{ and } s \neq i \end{cases}$
11. $[F_{ij}(\lambda), G_{rs}(\mu)] = \begin{cases} G_{is}(\lambda\mu) & \text{if } r = j \text{ and } s \neq i \\ G_{ir}(\lambda\mu) & \text{if } r \neq i \text{ and } s = j \\ E_r(2\lambda\mu) & \text{if } r = i \text{ and } s = j \\ E_s(2\lambda\mu) & \text{if } r = j \text{ and } s = i \\ I & \text{otherwise} \end{cases}$

12. $[F_{ij}(\lambda), H_{rs}(\mu)] = \begin{cases} H_{js}(-\lambda\mu) & \text{if } r = i \text{ and } s \neq j \\ H_{jr}(-\lambda\mu) & \text{if } r \neq j \text{ and } s = i \\ E_{n+s}(-2\lambda\mu) & \text{if } r = i \text{ and } s = j \\ E_{n+r}(-2\lambda\mu) & \text{if } r = j \text{ and } s = i \\ I & \text{otherwise} \end{cases}$

13. $[G_{ij}(\lambda), G_{rs}(\mu)] = 1$

14. $[G_{ij}(\lambda), H_{rs}(\mu)] = \begin{cases} F_{js}(\lambda\mu) & \text{if } r = i \text{ and } s \neq j \\ F_{is}(\lambda\mu) & \text{if } r = j \text{ and } s \neq i \\ F_{jr}(\lambda\mu) & \text{if } r \neq j \text{ and } s = i \\ F_{ir}(\lambda\mu) & \text{if } r \neq i \text{ and } s = j \\ M_3 & \text{if } r = i \text{ and } s = j \\ M_4 & \text{if } r = j \text{ and } s = i \\ I & \text{if } r, s \notin \{i, j\} \end{cases}$

15. $[H_{ij}(\lambda), H_{rs}(\mu)] = 1$

where the matrices M_1, M_2, M_3 and M_4 are given by:

$$M_1 = \begin{pmatrix} I + \lambda\mu(1+\lambda\mu)e_i i & -\lambda^2\mu e_{ii} \\ \lambda\mu^2 e_{ii} & 1 - \lambda\mu e_{ii} \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 1+\alpha & 0 \\ 0 & 1+\beta \end{pmatrix}$$

$$\text{with } \alpha = \lambda\mu(-e_{ii} + e_{jj} + \mu e_{ij} - \lambda e_{ji} + \lambda\mu e_{jj})$$

$$\text{and } \beta = \lambda\mu(-e_{jj} + e_{ii} + \mu e_{ji} - \lambda e_{ij} + \lambda\mu e_{ii})$$

$$M_3 = \begin{pmatrix} I + \lambda\mu(e_{ii} + e_{jj}) & -\lambda^2\mu(e_{ij} + e_{ji}) \\ \lambda\mu^2(e_{ij} + e_{ji}) & I - \lambda\mu(e_{ii} + e_{jj}) \end{pmatrix}$$

$$M_4 = \begin{pmatrix} I + \lambda\mu(1+\lambda\mu)(e_{ii} + e_{jj}) & -\lambda^2\mu(e_{ij} + e_{ji}) \\ \lambda\mu^2(e_{ij} + e_{ji}) & 1 - \lambda\mu(e_{ii} + e_{jj}) \end{pmatrix}.$$

Corollary 9.4.2. *Let k be the residue field of A then the group $SP_{2n}(A)$ is perfect provided the pair (n, k) is not one of: $(1, \mathbb{F}_2)$, $(1, \mathbb{F}_3)$ or $(2, \mathbb{F}_2)$.*

Although the conclusion in the case $(n, k) = (2, \mathbb{F}_2)$ is not immediately clear from the relations it follows from the exceptional isomorphism $SP_4(\mathbb{F}_2) \cong S_6$ where S_6 is the group of permutations of six letters. We remark that the commutator subgroup of S_6 is the alternating group A_6.

Next we state some simple implications of the form an arbitrary element $X \in M_{2n}(A)$ must take if it commutes with the generating elements of $SP_{2n}(A)$. These conditions will be particularly helpful when considering the image of the universal deformation.

Lemma 9.4.3. *Let $X \in M_{2n}(A)$. The following list shows the implications of the commutator relations on X:*

1. *If X commutes with $E_{i,m+i}(1)$ then*

$$\sum_a x_{ai}e_{a,m+i} = \sum_b x_{m+i,b}e_{ib}$$

2. *If X commutes with $E_{m+i,i}(1)$ then*

$$\sum_b x_{ib}e_{m+i,b} = \sum_a x_{a,m+i}e_{ai}$$

3. *If X commutes with $F_{ij}(1)$ then*

$$\sum_b x_{jb}e_{ib} - \sum_b x_{m+i,b}e_{m+j,b} = \sum_a x_{ai}e_{aj} - \sum_a x_{a.m+j}e_{a,m+i}$$

4. *If X commutes with $G_{i,j}(1)$ then*

$$\sum_b x_{m+j,b}e_{ib} + \sum_b x_{m+i,b}e_{jb} = \sum_a x_{ai}e_{a,m+j} + \sum_a x_{aj}e_{a,m+i}$$

5. *If X commutes with $H_{i,j}(1)$ then*

$$\sum_b x_{jb}e_{m+i,b} + \sum_b x_{ib}e_{m+j,b} = \sum_a x_{a,m+i}e_{aj} + \sum_a x_{a,m+j}e_{ai}.$$

Corollary 9.4.4. *The centraliser of $SP_{2n}(k)$ in $GL_{2n}(k)$ is the subgroup of invertible scalar matrices.*

Chapter 10

Skeleton of Proof in Symplectic Case

10.1 The Main Argument

In this section the main thrust of the argument proving Main Theorem 2 is presented, leaving the technical details of Main Theorem 3 until later. We begin by establishing the notation used.

Let k be a fixed choice of finite field, (A, m_A) a fixed element of $\mathcal{C}(k)$ and $n \geq 1$ and integer subject to the restrictions:

- If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$
- If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and p is coprime to n.

We then define $\Gamma = SP_{2n}(A)$, $\rho_A : \Gamma \xrightarrow{\cong} SP_{2n}(A)$ to be the identity representation (i.e. given by a fixed choice of isomorphism) and $\bar{\rho} : \Gamma \to GL_{2n}(k)$ to be componentwise reduction modulo m_A of ρ_A.

Lemma 10.1.1. *The residual representation $\bar{\rho}$ given above is absolutely irreducible.*

Proof. We begin by observing that for all $g \in SP_{2n}(k)$ there exists $\gamma \in SP_{2n}(A)$ such that $\bar{\rho}(\gamma) = g$.

Next, we show that $\bar{\rho}$ is irreducible. Let $v = (v_1, \ldots, v_{2n})$ be an arbitrary element of k^{2n}. Also let $1 \leq i, j \leq n$ be distinct integers and consider the action of $F_{ij}(1) = I + e_{ij} - e_{n+j,n+i}$ on v. If v is fixed by $F_{ij}(1)$ then equating this with v and looking at the i-th and $n + j$-th components implies $v_i = v_i + v_j$ and $v_{n+j} = v_{n+j} - v_{n+i}$. Therefore the components v_j and v_{n+i} must both be zero and continuing by running through all permissible values of i and j implies that k^{2n} has no non-trivial subspaces and the result follows.

Finally, recall that as $\bar{\rho} : \Gamma \to GL_n(k)$ is irreducible the condition of absolute irreducibility is equivalent to the centraliser of $\bar{\rho}(\Gamma)$ in $M_n(k)$ consisting of scalar matrices (see Theorem 9.2 of [17]). Therefore the result follows from Corollary 9.4.4. □

Therefore, invoking Theorem 1.1.6 we have proved the following.

Corollary 10.1.2. *For the deformation problem defined by Γ and $\bar{\rho}$ (as above) there exists an universal deformation ring R and a universal deformation ρ_R (see Theorem 1.1.6).*

Now we examine the images of the deformations introduced here.

Corollary 10.1.3. *For the deformation problem defined by Γ and $\bar{\rho}$ (as above) the following hold:*

(i) the image $\rho_R(\Gamma) \subseteq SL_{2n}(A)$.

(ii) the image $\bar{\rho}(\Gamma) \subseteq SP_{2n}(k)$.

Proof. Corollary 9.4.2 tells us that Γ is perfect therefore part (i) follows from Proposition 2.2.1. For part (ii) recall that all $g \in SP_{2n}(A)$ satisfy $g^T J g = J$, reducing this equality modulo m_A implies $\bar{g} = \bar{\rho}(g)$ also satisfies $\bar{g}^T \bar{J} \bar{g} = \bar{J}$. □

Recall from Theorem 1.1.6 the existence of a unique local ring homomorphism $\pi : R \to A$ for which $\pi \circ \rho_R$ is strictly equivalent to ρ_A and recall that $m : A \to k$ is componentwise reduction modulo m_A. We may summarise the relationships between the deformations $\bar{\rho}$, ρ_A and ρ_R in the commutative diagram below:

$$\begin{array}{ccc} & & SL_{2n}(R) \\ & \overset{\rho_R}{\nearrow} & \downarrow \pi \\ \Gamma & \xrightarrow{\rho_A} & SP_{2n}(A) \\ & \underset{\bar{\rho}}{\searrow} & \downarrow m \\ & & SP_{2n}(k). \end{array}$$

With an argument similar to that of Section 3.1 we will show that A together with ρ_A is the universal deformation ring for $\bar{\rho}$ by using a similar pattern of small steps.

Proof of Main Theorem 2. Step 1. Let $(R, \mathfrak{m}_R)$ together with $\rho_R : \Gamma \to SL_{2n}(R)$ be the universal deformation ring for $\overline{\rho} : \Gamma \to SP_{2n}(k)$. Note that ρ_R takes values in $SL_{2n}(R)$ by Corollary 2.2.1, and that $\rho_R(\Gamma) \mod \mathfrak{m}_R = SP_{2n}(k)$. Therefore, we may invoke Theorem 3 and upon replacement of ρ_R with a strictly equivalent representation we may assume that $\rho_R(\Gamma)$ contains a copy of $SP_{2n}(W_R)$.

Step 2. This is similar to the previous step 2 of Section 3.1 and culminates in the following observations

Proposition 10.1.4.

(i) $\rho_R : \Gamma \to SL_{2n}(R)$ is injective and $\pi : \rho_R(\Gamma) \to SP_{2n}(A)$ is an isomorphism.

(ii) The map $\pi : R \to A$ is surjective.

Proof. This follows immediately from the argument in Proposition 3.1.4. □

Step 3. To complete the outline of the proof we need the following result whose proof is given in the next section.

Proposition 10.1.5. *There exists a local ring homomorphism $s : A \to R$ which is a section to $\pi : R \to A$.*

To complete the proof of Main Theorem 2 we verify that $\rho_A : \Gamma \to SP_{2n}(A)$ is equivalent to the universal deformation. Recall that, by Corollary 9.1.4, the matrices $F(2n, A)$ generate $SP_{2n}(A)$. Therefore matrices of the form $E_{i,n+i}(s(a))$, $E_{n+i,i}(s(a))$, $F_{i,j}(s(a))$, $G_{ij}(s(a))$ and $H_{ij}(s(a))$ generate $\rho_R(\Gamma)$ where $s : A \to R$ is the section to $\pi : R \to A$ from Proposition 10.1.5.

As $\pi \circ s$ is the identity on A, we can now conclude that $s \circ \pi \circ \rho_R = \rho_R$. Hence, as before, we have shown that $A \cong R$.

□

10.2 Proof of Proposition 10.1.5

The method for constructing the section s resembles that of Section 3.2, although it is messier. This is because SP_{2n} has a more complicated set of generators than SL_n (see Corollary 2.1.3 and Corollary 9.1.4). The proof of the existence of the section $s : A \to R$ of Proposition 3.1.5 relies upon Main Theorem 3 which is stated again below for convenience.

Main Theorem 3. *Let (B, m_B) belong to $\mathcal{C}(k)$. Let $n \geq 1$ be an integer, p a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions:*

- *If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and p is coprime to n*

and let G be a closed subgroup of $SL_{2n}(B)$. If $G \bmod m_B = SP_{2n}(k)$, then there exists an $X \in GL_{2n}(B)$ satisfying $X \equiv I \bmod m_B$ such that $XGX^{-1} \supseteq SP_{2n}(W_B)$.

Similarly to the special linear case, the proof of Main Theorem 3 requires the background of chapters 11-12 and as such its proof is deferred until Chapter 13.

Proposition 10.2.1. *Let $\pi : R \to A$ be the unique local ring homomorphism which makes $\pi \circ \rho_R$ strictly equivalent to ρ_A. Then the restriction $\pi|_{W_R} : W_R \to W_A$ is an isomorphism.*

Proof. We note that $\rho_R(\Gamma) \bmod m_R = SP_{2n}(k)$ therefore Main Theorem 3 allows us to assume that $SP_{2n}(W_R)$ belongs to the image of a representative of the deformation class to which ρ_R belongs. The rest of the argument follows from Proposition 10.1.4 in a way which is in essence identical to that of the proof of Proposition 3.2.1. □

This allows us to again identify W_R and W_A. Henceforth, we will not differentiate between $\iota_R(x)$ and $\iota_A(x)$ for $x \in W$.

Next we investigate the local ring homomorphism π in further detail.

Proposition 10.2.2. *Let k be a fixed choice of finite field, (A, m_A) a fixed element of $\mathcal{C}(k)$ and $n \geq 1$ an integer subject to the restrictions:*

- *If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and p is coprime to n*

In addition let $a \in A$. The matrices $E_i(s(a))$, $E_{n+i}(s(a))$, $F_{ij}(s(a))$, $G_{ij}(s(a))$ and $H_{ij}(s(a))$ such that $1 \leq i, j \leq n$ are distinct (see Lemma 9.1.1 for their definitions) belong to $\rho_R(\Gamma)$ and are the unique pre-image under π of $E_i(s(a))$, $E_{n+i}(a)$, $F_{ij}(a)$, $G_{ij}(a)$ and $H_{ij}(a)$ respectively. Therefore the map $s : A \to R$ characterised by the following property is well defined:

> *If $a \in A$ then $s(a)$ is the unique element in R such that $\pi(s(a)) = a$ and that $E_i(s(a))$, $E_{n+i}(s(a))$, $F_{ij}(s(a))$, $G_{ij}(s(a))$ and $H_{ij}(s(a))$ belong to $\rho_R(\Gamma)$ for all $1 \leq i, j \leq n$ with $i \neq j$.*

Proof. Let $\pi(X_i) = E_i(a)$ then by Proposition 9.4.1 X_i must commute with: $E_j(1)$ for all $1 \leq j \leq n$, $G_{jk}(1)$ for all $1 \leq j, k \leq n$ and for all $j \neq i$ $E_{n+j}(1)$. Hence by Lemma (9.4.3) we obtain:

$$X_i = \lambda_i(I + x_i e_{i,m+i})$$

where $\lambda_i := \lambda_i(E_i(1))$ and $x_i := x_i(E_i(a))$ are elements of R. Let $\sigma(rs)$ denote image of the embedding of transpositions of the symmetric group S_n into $SP_{2n}(R)$, see the discussion around equation (9.2.3) for details. We may then conclude that $\lambda_i = \lambda_j$ and $x_i = x_j$ from the equality $\sigma(ij)E_i(a)\sigma(ij) = E_j(a)$. Therefore, we write $\lambda := \lambda_i$ and $x := x_i$. Now let $\pi((X_i')^{-1}) = E_{n+i}(-a)$ the relation $JE_i(a)J^{-1} = E_{n+i}(-a)$ implies $(X_i')^{-1} = \lambda(I - xe_{n+i,i})$.

Similarly, let $\pi(Y_{rs}) = F_{rs}(a)$. This case is more complicated, to begin with observe that Y_{rs} must commute with: $E_i(1)$ for all $i \neq s$, $E_{n+j}(1)$ for all $j \neq r$ and $F_{ik}(1)$. This yields

$$Y_{rs} = \mu(I + ye_{rs} + ze_{n+s,n+r} + ue_{r,n+r} + ve_{n+s,s})$$

where: $\mu := \mu(F_{rs}(a))$, $y := y(F_{rs}(a))$, $z := z(F_{rs}(a))$, $u := u(F_{rs}(a))$ and $v := v(F_{rs}(a))$ are elements of R. The next step is to show that u and v are both zero. We show that as $p \neq 2$ this follows from the relations $[F_{rs}(a), G_{rs}(1)] = E_r(2a)$ and $[F_{rs}(a), H_{rs}(1)] = E_{n+s}(-2a)$. The first of these relations implies

$$Y_{rs}G_{rs}(-1) = X_r^2 G_{rs}(1)Y_{rs} \tag{10.2.1}$$

which itself yields that:

$$Y_{rs} + \mu(e_{r,n+s} + e_{s,n+r} + ye_{r,n+r} + ve_{n+s,n+r})$$

is equal to

$$\lambda^2 Y_{rs} + \lambda^2\mu(2xe_{r,n+r} + e_{r,n+s} + e_{s,n+r} + ze_{r,n+r} + ve_{rs}).$$

From which it is clear that $v = 0$, $\lambda^2 = 1$ and $y - z = 2x$. The second relation implies

$$Y_{rs}H_{rs}(1) = (X_i')^{-2}H_{rs}(1)Y_{rs}$$

which itself yields that

$$Y_{rs} + \mu(e_{n+r,s} + e_{n+s,r} + ze_{n+s,s} + ue_{rs})$$

is equal to

$$Y_{rs} + \mu(e_{n+r,s} + e_{n+s,r} - 2xe_{n+s,s} + ye_{n+s,s} + ue_{n+s,n+r}).$$

From which it is clear that $u = 0$. Considering conjugation by the elements $\sigma(rs)$ shows that the coefficients do not depend on the indices r and s. The relation $[E_r(a), H_{rs}(1)] = F_{rs}(a)E_{n+s}(a)$, or rather its equivalent:
$E_r(a)H_{rs}(1)E_r(-a) = F_{rs}(a)E_{n+s}(a)H_{rs}(1)$, implies that

$$I + e_{n+r,s} + e_{n+s,r} + x(e_{rs} - e_{n+s,n+r})$$

is equal to

$$\lambda^{-1}\mu(I + ye_{rs} + ze_{n+s,n+r} + xe_{n+s,s} + ze_{n+s,s} + e_{n+r,s} + e_{n+s,r}).$$

From which it is clear that $\lambda = \mu$, $y = x$ and $z = -x$. If $n \geq 3$ then the relations $[F_{rs}(a), F_{st}(1)] = F_{rt}(a)$ imply that $\mu = 1$, hence $\lambda = 1$ also. If $n = 2$ and $q \geq 7$ then the argument in the proof of Lemma 3.2.2 (ii) for $n = 2$ applied to the matrix $F_{12}(a)$ implies that $\mu = 1$. If $n = 2$, $q = 5$ and consider the pre-image of $F_{12}(3x)$, then an argument similar to that of Lemma 3.2.2 (ii) for $n = 2$ implies that $F_{12}(3s(x)) = \mu^3 F_{12}(3s(x))$. Therefore $\mu^3 = 1$ and considering cubic powers implies $\mu = 1$.

Let $\pi(Z_{kl}) = G_{kl}(a)$ and $\pi(Z'_{kl}) = H_{kl}(a)$ then the commutator relations:

$$[F_{ki}(a), G_{il}(1)] = G_{kl}(a)$$
$$[H_{il}(1), F_{ik}(a)] = H_{kl}(a)$$

imply that $Z_{kl} = I + x(e_{k,n+l} + e_{l,n+k})$ and $Z'_{kl} = I + x(e_{n+k,l} + e_{n+l,k})$ respectively. The proof is completed by setting $s(a) = x$. □

Corollary 10.2.3. *The map $s : A \to R$ defined in Proposition 10.2.2 is a local ring homomorphism which is a section for π.*

Proof. Everything carries over from the proof of Proposition 3.2.3. □

Chapter 11

Modules for $kSP_{2n}(W_r)$

The aims of this chapter are similar to those of Chapter 5. However the situation is more complicated than for special linear groups as we are now viewing $\mathfrak{M}_0 = \mathfrak{M}_0(2n)$ as a $kSP_{2n}(k)$-module. We begin by fixing the notation used.

Let k be a fixed choice of finite field, (A, m_A) a fixed ring in $\mathcal{C}(k)$ and $n \geq 1$ an integer. We then define $\rho_A : SP_{2n}(A) \xrightarrow{\cong} SL_{2n}(A)$ to be the identity representation and $\bar{\rho} : SP_{2n}(A) \to SP_{2n}(k)$ to be the componentwise reduction of ρ_A modulo m_A. As $SP_{2n}(A)$ is a subgroup of $SL_{2n}(A)$, the residual representation $\bar{\rho}$ defines an action of $SP_{2n}(A)$ on $\mathfrak{M}_0$ via:

$$\gamma \cdot M = \bar{\rho}(\gamma) M \bar{\rho}(\gamma)^{-1}$$

for all γ in $SP_{2n}(A)$ and M in $\mathfrak{M}_0$.

Similarly to the special linear case, we remark that a $SP_{2n}(A)$-module can be turned into a $kSP_{2n}(A)$-module.

11.1 $kSP_{2n}(k)$-modules

This section examines the $kSP_{2n}(k)$-submodule structure of $\mathfrak{M}_0$ which is more involved than that of $\mathfrak{M}_0$ as a $kSL_{2n}(k)$-module. In particular, we shall see that as a $kSP_{2n}(k)$-module $\mathfrak{M}_0$ has the form of a direct sum. With this in mind, we introduce the following subsets of $\mathfrak{M}_0$.

Definition 11.1.1. Let A, B and C be elements of $\mathfrak{M}(n)$ and define the following subsets of $\mathfrak{M}_0$:

$$\begin{aligned} \mathfrak{N} &:= \left\{ \begin{pmatrix} A & B \\ C & -A^T \end{pmatrix} \mid B^T = B,\ C^T = C \right\} \text{ and} \\ \mathfrak{P} &:= \left\{ \begin{pmatrix} A & B \\ C & A^T \end{pmatrix} \mid A \in \mathfrak{M}_0(n),\ B^T = -B,\ C^T = -C \right\}. \end{aligned}$$

Lemma 11.1.2. *The subsets $\mathfrak{N}$ and $\mathfrak{P}$ are $k\Gamma$-submodules of $\mathfrak{M}_0$. Furthermore, there is the direct sum decomposition*

$$\mathfrak{M}_0 = \mathfrak{N} \oplus \mathfrak{P}.$$

Proof. We begin by showing that both of these subsets are invariant under the action of $SP_{2n}(k)$. Let M, written in four $n \times n$ blocks A, B, C and D, be an element of $\mathfrak{N}$ or $\mathfrak{P}$ respectively. Firstly, suppose S is a symmetric $n \times n$ matrix this implies

$$\begin{aligned} \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \cdot M &= \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} A+SC & -AS-SCS+B+SD \\ C & -CS+D \end{pmatrix}. \end{aligned}$$

If M is in $\mathfrak{N}$ then

$$\begin{aligned} (-CS+D)^T &= (-CS-A^T)^T = (-SC-A) = -(A+SC) \\ (-AS-SCS+B-SA^T)^T &= -SA^T-SCS+B-AS \end{aligned}$$

which implies that:

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \cdot M$$

also belongs to $\mathfrak{N}$. If M is in $\mathfrak{P}$ then:

$$\begin{aligned} (-CS+D)^T &= (-CS+A^T)^T = (SC+A) \\ (-AS-SCS+B-SA^T)^T &= -SA^T-SCS-B+AS \end{aligned}$$

and we may conclude similarly.

Secondly, let g belong to $GL_n(k)$ then we have

$$\begin{pmatrix} g & 0 \\ 0 & g^{-t} \end{pmatrix} \cdot M = \begin{pmatrix} g & 0 \\ 0 & g^{-t} \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} gAg^{-1} & gBg^t \\ g^{-t}Cg^{-1} & g^{-t}Dg^t \end{pmatrix}$$

and the same conclusion may again be drawn.

Thirdly, the action of J on M is given by

$$J \cdot M = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix}$$

and once again $J \cdot M$ belongs to $\mathfrak{N}$ or $\mathfrak{P}$ respectively. Therefore both $\mathfrak{N}$ and $\mathfrak{P}$ are invariant under the action of $SP_{2n}(k)$ and hence are $kSP_{2n}(k)$-submodules of $\mathfrak{M}_0$.

Finally, we observe that as $p > 2$ the intersection of $\mathfrak{N}$ and $\mathfrak{P}$ is trivial. Therefore the proof of the direct sum decomposition is completed by comparing dimensions. $\mathfrak{M}_0(2n)$ has dimension $4n^2 - 1$; the restriction being on the final diagonal entry to ensure trace zero. We remark that the dimension of an $n \times n$ symmetric matrix, respectively skew-symmetric matrix, is $n(n+1)/2$ respectively $n(n-1)/2$. Therefore $\mathfrak{N}$ has dimension $2n^2 + n$, $\mathfrak{P}$ has dimension $2n^2 - n - 1$ and $\mathfrak{N} \oplus \mathfrak{P}$ has dimension $4n^2 - 1$. □

Our next objective is to examine the $kSP_{2n}(k)$-submodule structure of $\mathfrak{N}$ and $\mathfrak{P}$. For this, we require generating sets for both modules.

Lemma 11.1.3. *Let $1 \leq i, j \leq n$ be distinct integers.*

(i) $\mathfrak{N}$ is generated by:

- $\mathfrak{a}_i := e_{i,n+i}$
- $\mathfrak{b}_i := e_{n+i,i}$
- $\mathfrak{h}_i := e_{ii} - e_{n+i,n+i}$
- $\mathfrak{c}_{ij} := e_{i,n+j} + e_{j,n+i}$ *where* $i < j$
- $\mathfrak{d}_{ij} := e_{n+i,j} + e_{n+j,i}$ *where* $i < j$
- $\mathfrak{f}_{ij} := e_{ij} - e_{n+j,n+i}$.

(ii) $\mathfrak{P}$ is generated by:

- $\tilde{\mathfrak{h}}_i := e_{ii} - e_{i+1,i+1} + e_{n+i,n+i} - e_{n+i+1,n+i+1}$
- $\tilde{\mathfrak{c}}_{ij} := e_{i,n+j} - e_{j,n+i}$ *where* $i < j$
- $\tilde{\mathfrak{d}}_{ij} := e_{n+i,j} - e_{n+j,i}$ *where* $i < j$
- $\tilde{\mathfrak{f}}_{ij} := e_{ij} + e_{n+j,n+i}$.

Proof. For part (i), let B and C be the symmetric $n \times n$ matrices in the definition of $\mathfrak{N}$ (see Definition 11.1.1). B can be expressed uniquely as a linear combination of the $\mathfrak{a}_{ii}$ and $\mathfrak{c}_{ij}$; similarly C may be written uniquely in terms of $\mathfrak{b}_{ii}$ and $\mathfrak{d}_{ij}$. Analogously the elements $\mathfrak{h}_i$ and $\mathfrak{f}_{ij}$ are sufficient to uniquely express elements belonging to the two diagonal blocks.

Part (ii), we observe that the antisymmetric matrix B (respectively C) may be written uniquely as a linear combination of $\tilde{\mathfrak{c}}_{ij}$ (respectively $\tilde{\mathfrak{d}}_{ij}$) and elements belonging to the two diagonal blocks written in terms of $\tilde{\mathfrak{h}}_i$ and $\tilde{\mathfrak{f}}_{ij}$. □

This leads us to consider the irreducibility of these and related modules.

Proposition 11.1.4. *Let $p > 2$ be the characteristic of k.*

(1) $\mathfrak{N}$ is an irreducible $kSP_{2n}(k)$-module,

(2) If p does not divide n then $\mathfrak{P}$ is an irreducible $kSP_{2n}(k)$-module,

(3) If $p|n$ then $\mathfrak{S}$ is the unique $kSP_{2n}(k)$-submodule of $\mathfrak{P}$.

Proof. Let v be an arbitrary element of $\mathfrak{M}_0$ written in $n \times n$ blocks as

$$v = \sum_{x,y=1}^{n} a_{xy}e_{xy} + \sum_{x,y=1}^{n} b_{xy}e_{x,n+y} + \sum_{x,y=1}^{n} c_{xy}e_{n+x,y} + \sum_{x,y=1}^{n} d_{xy}e_{n+x,n+y} \quad (11.1.1)$$

and observe the identities:

(i) $(2E_{n+i}(1) - E_{n+i}(2) - I) \cdot v = 2b_{ii}e_{n+i,i}$

(ii) $(E_{n+i}(1) + E_{n+j}(1) - E_{n+j}(1)E_{n+i}(1) - I) \cdot v = b_{ij}e_{n+i,j} + b_{ji}e_{n+j,i}$

(iii) $(I - E_{n+j}(1)) \cdot (E_i(1) \cdot v) - (I - E_{n+j}(1)) \cdot v = d_{ij}e_{ij} + a_{ji}e_{n+j,n+i}$

(iv) If v is diagonal then $F_{ij}(1) \cdot v - v = (a_{jj} - a_{ii})e_{ij} + (d_{jj} - d_{ii})e_{n+j,n+i}$.

Firstly assume v is a non-zero element of a submodule $\mathcal{N}$ of $\mathfrak{N}$. If b_{ii} is non-zero, then identity (i) implies that $2b_{ii}e_{n+i,i} = 2b_{ii}\mathfrak{b}_i$ belongs to $\mathcal{N}$ and thus the equation

$$-(J + J\sigma(ij) - JF_{ij}(1)) \cdot \mathfrak{b}_i = \mathfrak{c}_{ij}$$

$$\mathfrak{b}_i + (\sigma(ij) - F_{ij}(1)) \cdot \mathfrak{b}_i = \mathfrak{c}_{ij}$$

allows us to assume $\mathfrak{c}_{ij}$ is in $\mathcal{N}$. If $b_{ij} = b_{ji}$ is non-zero then identity (ii) implies that $b_{ij}(e_{n+i,j} + e_{n+j,i}) = b_{ij}\mathfrak{c}_{ij}$ belongs to $\mathcal{N}$. If c_{ii}, respectively c_{ij}, is non-zero then taking $J \cdot v$ allows us to assume b_{ii}, respectively b_{ij}, is non-zero, and so in either case we may assume $\mathfrak{c}_{ij}$ is in $\mathcal{N}$. If $a_{ji} = -d_{ij}$ is non-zero then identity (iii) implies that $a_{ji}(e_{n+j,n+i} - e_{ij}) = -a_{ji}\mathfrak{f}_{ij}$ belongs to $\mathcal{N}$ and the equation

$$(I - E_j(1)) \cdot \mathfrak{f}_{ij} = \mathfrak{c}_{ij} \tag{11.1.2}$$

implies that $\mathfrak{c}_{ij}$ also belongs to $\mathcal{N}$. If v is not covered by one of the previous cases then it must be diagonal. If v has the form $v = \lambda \sum_i (e_{ii} - e_{n+i,n+i})$ then

$$(I - G_{ij}(1)) \cdot v = 2\lambda(e_{ij} + e_{ji}) = 2\lambda\mathfrak{c}_{ij}.$$

If not, then $a_{jj} \neq a_{ii}$ for some pair i and j, hence identity (iv) implies that

$$(a_{jj} - a_{ii})e_{ij} - (a_{jj} - a_{ii})e_{n+j,n+i} = (a_{jj} - a_{ii})\mathfrak{f}_{ij}$$

belongs to $\mathcal{N}$. Equation (11.1.2) then implies that $\mathfrak{c}_{ij}$ belongs to $\mathcal{N}$ as well. Therefore in each case we may assume that an element $\mathfrak{c}_{ij}$ belongs to $\mathcal{N}$.

Secondly assume v is a non-zero element of a submodule $\mathcal{P}$ of $\mathfrak{P}$ and proceed in a similar fashion. If $b_{ij} = -b_{ji}$ is non-zero then identity (ii) implies $b_{ij}\tilde{\mathfrak{c}}_{ij}$ belongs to $\mathcal{P}$ and if $c_{ij} = -c_{ji}$ is non-zero taking $J \cdot v$ also allows us to assume $\tilde{\mathfrak{c}}_{ij}$ to be in $\mathcal{P}$. If $a_{ji} = d_{ij}$ is non-zero then identity (iii) and the equality

$$(I - E_j(1)) \cdot \tilde{\mathfrak{f}_{ij}} = \tilde{\mathfrak{c}}_{ij}$$

implies that $\tilde{c}_{ij}$ belongs to $\mathcal{P}$. All that remains is the case when v is diagonal. If $p|n$ then the scalar matrices $\mathfrak{S}$ have trace zero and form a submodule of $\mathfrak{P}$. If v is not a scalar then $a_{ii} \neq a_{jj}$ for some i and j. Then identity (iv) implies that $(a_{jj} - a_{ii})\tilde{\mathfrak{f}}_{ij}$, hence $\tilde{\mathfrak{c}}_{ij}$, is in $\mathcal{P}$. Therefore, if $\mathcal{P}$ is not $\mathfrak{S}$, we may assume $\tilde{\mathfrak{c}}_{ij}$ belongs to $\mathcal{P}$.

To complete the proof we show that $\mathfrak{c}_{ij}$ (respectively $\tilde{\mathfrak{c}}_{ij}$) may be conjugated to each of the other generators of $\mathfrak{N}$ (respectively $\mathfrak{P}$). This is listed below; the expressions without square brackets around refer to $\mathcal{N}$ and those with to $\mathcal{P}$

- $\sigma(ik) \cdot \mathfrak{c}_{ij} = \mathfrak{c}_{kj}$ and $[\sigma(ik) \cdot \tilde{\mathfrak{c}}_{ij} = \tilde{\mathfrak{c}}_{kj}]$
- $\sigma(jk) \cdot \mathfrak{c}_{ij} = \mathfrak{c}_{ik}$ and $[\sigma(jk) \cdot \tilde{\mathfrak{c}}_{ij} = \tilde{\mathfrak{c}}_{ik}]$

- $(F_{ij}(1) - I) \cdot \mathfrak{c}_{ij} = 2\mathfrak{a}_i$
- $-J \cdot \mathfrak{c}_{ij} = \mathfrak{d}_{ij}$ and $[-J \cdot \tilde{\mathfrak{c}}_{ij} = \tilde{\mathfrak{d}}_{ij}]$
- $-J \cdot \mathfrak{a}_i = \mathfrak{b}_i$
- $(I - E_{n+i}(1)) \cdot \mathfrak{a}_i - \mathfrak{b}_i = \mathfrak{h}_i$ and $[(H_{i,i+1}(-1) - I) \cdot \tilde{\mathfrak{c}}_{i,i+1} - \tilde{\mathfrak{d}}_{i,i+1} = \tilde{\mathfrak{h}}_i]$
- $(F_{ij}(1) - I) \cdot \mathfrak{h}_j = \mathfrak{f}_{ij}$ and $[(F_{ij}(1) - I) \cdot \tilde{\mathfrak{h}}_j = \tilde{\mathfrak{f}}_{ij}]$.

The irreducibility of $\mathfrak{P}/\mathfrak{S}$ follows immediately from the argument for $\mathfrak{P}$. □

In the following corollary recall that $\mathfrak{V} = \mathfrak{M}_0/\mathfrak{S}$.

Corollary 11.1.5. *If p is coprime to n then $\mathfrak{N}$ and $\mathfrak{P}$ are the only non trivial $kS_{2n}(k)$-submodules of $\mathfrak{M}_0$. If $p|n$ then $\mathfrak{S}$ and $\mathfrak{N} \oplus \mathfrak{S}$, in addition to $\mathfrak{N}$ and $\mathfrak{P}$, are $kSP_{2n}(k)$-submodules of $\mathfrak{M}_0$.*

The following sequences of $kSP_{2n}(k)$-modules are exact:

1. $0 \to \mathfrak{N} \to \mathfrak{M}_0 \to \mathfrak{P} \to 0$
2. $0 \to \mathfrak{P} \to \mathfrak{M}_0 \to \mathfrak{N} \to 0$
3. *if $p|n$,* $0 \to \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{V} \to 0$
4. *if $p|n$,* $0 \to \mathfrak{N} \oplus \mathfrak{S} \to \mathfrak{M}_0 \to \mathfrak{P}/\mathfrak{S} \to 0$.

Proof. These sequences easily follow from Lemma 11.1.2 and Proposition 11.1.4. In the fourth sequence we have made the identification

$$\frac{\mathfrak{M}_0}{\mathfrak{N} \oplus \mathfrak{S}} \cong \frac{\mathfrak{N} \oplus \mathfrak{P}}{\mathfrak{N} \oplus \mathfrak{S}} \cong \frac{\mathfrak{P}}{\mathfrak{S}}.$$

□

11.2 $kSP_{2n}(W_r)$-modules

Recall that $\bar{\rho} : SP_{2n}(A) \to SP_{2n}(k)$ gives $\mathfrak{M}_0$ the structure of a $kSP_{2n}(A)$-module, in this section we investigate the structure of $kSP_{2n}(W_r)$-modules.

Recall the definition of the subgroup N of $SP_{2n}(W_r)$ from Definition 9.2.2, it consists of matrices of the form:

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$$

where $S \in M_n(W_r)$ is a symmetric matrix. We note that $SP_{2n}(W_r)$-modules are naturally N-modules as well. In preparation for the cohomological calculations in Chapter 12 we begin by considering the action of N on the modules introduced in the previous section.

Lemma 11.2.1. *Recall that $\mathfrak{M}(n)$ is the set of $n \times n$ over k and define:*

$$\mathcal{B} := \left\{ \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \mid B \in \mathfrak{M}(n) \right\}$$

Then

$$\mathfrak{M}_0{}^N = \begin{cases} \mathcal{B} \oplus \mathfrak{S} & \text{if } p|n \\ \mathcal{B} & \text{if not.} \end{cases}$$

Proof. Let S be an $n \times n$ symmetric matrix and let the four $n \times n$ blocks A, B, C and D constitute an arbitrary element of $\mathfrak{M}_0$ then we must have the equality

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 1 & -S \\ 0 & 1 \end{pmatrix}$$

which implies the equality:

$$\begin{pmatrix} SC & -AS - SCS + SD \\ 0 & -CS \end{pmatrix} = 0 \tag{11.2.1}$$

Looking at the top left-hand block, we see that $SC = 0$. We write $C = \sum_{xy} c_{xy} e_{xy}$ then if $S = e_{ii}$ this implies that $\sum_y c_{iy} e_{iy} = 0$ which by running through all values of i shows that $C = 0$.

Focusing on the top right-hand block, we see that $AS = SD$. Again if $S = e_{ii}$ and $A = \sum_{xy} a_{xy} e_{xy}$ and $D = \sum_{x,y} d_{xy} e_{xy}$ we see that

$$\sum_x a_{xi} e_{xi} = \sum_y d_{iy} e_{iy}$$

which shows that $a_{ii} = d_{ii}$ for i and that all entries off the diagonals of A and D are zero. Now let $S = e_{rs} + e_{sr}$ then this implies

$$a_{rr} e_{rs} + a_{ss} e_{sr} = a_{ss} e_{rs} + a_{rr} e_{sr}$$

i.e. that all the diagonal entries of A are equal. If p does not divide n then A must equal the zero matrix. If $p|n$ we remark that the action of G clearly fixes $\mathfrak{S}$ and G also fixes $\mathcal{B}$ as shown by

$$\begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix} \cdot \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & gBg^T \\ 0 & 0 \end{pmatrix}.$$

Therefore, as their intersection is obviously 0, the direct sum decomposition follows. □

Corollary 11.2.2. *Let $\mathcal{B}$ be defined by Lemma 11.2.1. Then the following hold:*

(1)

$$\mathfrak{N}^N = \left\{ B \in \mathcal{B} \mid B^T = B \right\}$$

(2)

$$\mathfrak{P}^N = \begin{cases} \{B \in \mathcal{B} \mid B^T = -B\} & \text{if } p \text{ does not divide } n \\ \{B \in \mathcal{B} \mid B^T = -B\} \oplus \mathfrak{S} & \text{if } p|n. \end{cases}$$

Proof. The results follows from the observations $\mathfrak{N}^N = \mathcal{B} \bigcap \mathfrak{N}$ and $\mathfrak{P}^N = \mathcal{B} \bigcap \mathfrak{P}$. □

Corollary 11.2.3. *Recall that $\mathfrak{V} = \mathfrak{M}_0/\mathfrak{S}$, thus:*

$$\mathfrak{V}^N = \left\{ \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} + \mathfrak{S} \mid B \in \mathfrak{M}(n) \right\}.$$

Proof. We adopt the block notation to that used in the proof of Lemma 11.2.1. The analogue to equation (11.2.1) is that

$$\begin{pmatrix} SC & -AS - SCS + SD \\ 0 & -CS \end{pmatrix} \in \mathfrak{S}.$$

If we set $S = e_{ii}$ the top left-hand block implies that $\sum_{xy} c_{xy} e_{xy}$ is a scalar matrix, hence we may assume $C = 0$. The rest of the proof follows exactly as in the lemma. □

The results obtained so far, i.e. modules fixed by N, are extended to calculate the modules fixed by $SP_{2n}(k)$.

Corollary 11.2.4. *The submodules fixed by the action of $SP_{2n}(k)$ are given by:*

1. ${\mathfrak{M}_0}^{SP_{2n}(k)} = \begin{cases} \mathfrak{S} & \text{if } p|n \\ 0 & \text{if not} \end{cases}$
2. $\mathfrak{N}^{SP_{2n}(k)} = 0$
3. $\mathfrak{P}^{SP_{2n}(k)} = \begin{cases} \mathfrak{S} & \text{if } p|n \\ 0 & \text{if not.} \end{cases}$

Proof. We note that $SP_{2n}(k)$ clearly fixes $\mathfrak{S}$. Therefore result follows immediately from Lemma 11.2.1 and the equality:

$$\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} = J. \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -B & 0 \end{pmatrix}.$$

□

Now we investigate $kSP_{2n}(W_r)$-module homomorphisms.

Proposition 11.2.5. *If $n \geq 2$ be an integer and $\mathcal{M}$ represent each of the $kSP_{2n}(W_r)$-modules: $\mathfrak{N}$, $\mathfrak{P}$ and $\mathfrak{P}/\mathfrak{S}$; then*

$$\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathcal{M}, \mathcal{M}) \cong k.$$

Proof. These homomorphism groups are found by considering the restriction that the fixed action of G imposes, see equation (5.1.1).

Firstly, let $\mathcal{M} = \mathfrak{N}$ and consider the image of $\mathfrak{a}_i$ under ϕ in $\mathrm{Hom}_{kG}(\mathfrak{N}, \mathfrak{N})$. Specify the image of $\mathfrak{a}_i$ in the form $\phi(\mathfrak{a}_i) = \sum_{x,y} a_{xy} e_{xy}$. As $E_j(1)$ fixes $\mathfrak{a}_i$ for all j equation (5.1.1) implies that $E_i \cdot \phi(\mathfrak{a}_i) = \phi(\mathfrak{a}_i)$ which yields:

$$\begin{cases} a_{xj} = 0 & \text{for every } x \neq j \\ a_{m+j,y} = 0 & \text{for every } y \neq n+j \\ a_{jj} = a_{n+j,n+j}. \end{cases} \tag{11.2.2}$$

The action of $G_{rs}(1)$, which also fixes α, on $\phi(\alpha)$ implies

$$\sum_y (a_{n+s,y} e_{ry} + a_{n+r,y} e_{sy}) - \sum_x (a_{xr} e_{x,n+s} + a_{xs} e_{x,n+r}) = 0. \tag{11.2.3}$$

A comparison of coefficients of $e_{r,n+s}$ implies $a_{n+s,n+s} = a_{rr}$. By varying r and s we conclude that all diagonal entries of $\phi(\mathfrak{a}_i)$ are equal. Thus, as ϕ takes values in $\mathfrak{N}$ the diagonal entries are zero. So far we have shown that the only possible non-zero entries of $\phi(\mathfrak{a}_i)$ are those in the top right-hand $n \times n$ block. Let $j \neq i$ then the element $F_{ij}(1)$ fixes $\mathfrak{a}_i$ hence

$$\sum_y a_{j,n+y} e_{i,n+y} + \sum_x a_{x,n+j} e_{x,n+i} + a_{j,n+j} e_{i,n+i} = 0.$$

This implies that

$$\begin{cases} a_{j,n+y} = 0 & \text{for every } y \neq i \\ a_{x,n+j} = 0 & \text{for every } x \neq i \\ a_{j,n+i} + a_{i,n+j} = 0. \end{cases} \tag{11.2.4}$$

The third restriction implies that $a_{j,n+i} = -a_{i,n+j}$ which as ϕ takes values in $\mathfrak{N}$ implies that $a_{j,n+i} = 0$. Varying j over all its possible values makes it clear that the only possible non-zero entry is the $(1, n+1)$-th. Therefore it follows that we may write $\phi(\mathfrak{a}_i) = \lambda \mathfrak{a}_i$ for some $\lambda := \lambda(\mathfrak{N})$ in k.

Secondly, consider the image of $\tilde{\mathfrak{c}}_{rs}$ under ϕ in $\mathrm{Hom}_G(\mathfrak{P}, \mathfrak{P})$. We write $\phi(\tilde{\mathfrak{c}}_{rs}) = \sum_{x,y} b_{xy} e_{xy}$. As in the previous case the elements $E_i(1)$ and $G_{ij}(1)$ fix $\tilde{\mathfrak{c}}_{rs}$ hence the diagonal entries of $\phi(\tilde{\mathfrak{c}}_{rs})$ are equal and the only other possible non-zero entries are in the top right-hand $n \times n$ block.

If p does not divide n then the diagonal entries are all zero. The group elements $F_{rs}(1)$ and $F_{sr}(1)$ also fix $\tilde{\mathfrak{c}}_{rs}$ which in turn imply:

- $\begin{cases} b_{s,n+y} = 0 & \text{for each } y \neq r \\ b_{x,n+s} = 0 & \text{for each } x \neq r \\ b_{s,n+r} + b_{r,n+s} = 0 \end{cases}$
- $\begin{cases} b_{r,n+y} = 0 & \text{for each } y \neq s \\ b_{x,n+r} = 0 & \text{for each } x \neq s \end{cases}$.

If $n = 2$ then this is sufficient to conclude that $\phi(\tilde{\mathfrak{c}}_{rs}) = \lambda\tilde{\mathfrak{c}}_{rs}$ for some $\lambda := \lambda(\mathfrak{P})$ in k. If $n \geq 3$ then take $j \neq r$, s and observe that $F_{rj}(1)$ fixes $\tilde{\mathfrak{c}}_{rs}$ which implies

- $\begin{cases} b_{j,n+y} = 0 & \text{for each } y \neq r \\ b_{x,n+j} = 0 & \text{for each } x \neq r \end{cases}$.

Running through all possible values of j allows us to again conclude that $\phi(\tilde{\mathfrak{c}}_{rs}) = \lambda\tilde{\mathfrak{c}}_{rs}$. Corollary 11.2.4 implies that if $p|n$ the image $\phi(\mathfrak{S}) \subseteq \mathfrak{S}$.

Thirdly, let $\mathcal{M} = \mathfrak{P}/\mathfrak{S}$ and β denote the image of $\mathfrak{c}_{rs}$ in $\mathcal{M}$. Then the argument for $\tilde{\mathfrak{c}}_{rs}$ in $\mathfrak{P}$ hold modulo $\mathfrak{S}$. Therefore for ϕ in $\mathrm{Hom}_{kG}(\mathcal{M}, \mathcal{M})$ we may conclude that $\phi(\beta) = \lambda\beta$.

For each $\mathcal{M}$ the map $f : \mathcal{M} \to \mathcal{M}$ defined as $f(m) = \phi(m) - \lambda m$ has non trivial kernel. As each $\mathfrak{N}$ and $\mathfrak{P}/\mathfrak{S}$ have no non trivial $kSP_{2n}(W_r)$-submodules the kernel of ϕ in these cases must equate to the totality of the module in question. If p does not divide n then for $\mathfrak{P}$ we may conclude similarly. If $p|n$ then $\mathfrak{S} \subset ker(f)$ and the first isomorphism theorem for modules implies that there are two $kSP_{2n}(W_r)$-submodules of $\mathfrak{P}$ one isomorphic to $ker(f)$ and the other isomorphic to $im(f) \cong \mathfrak{P}/ker(f)$. However as $\mathfrak{S}$ is the only non-trivial $kSP_{2n}(W_r)$-submodule of $\mathfrak{P}$ we must have $ker(f) = \mathfrak{P}$. Therefore in each case $ker(f) = \mathcal{M}$ and thus ϕ is multiplication by a scalar. □

Corollary 11.2.6. *If p does not divide n then* $\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathfrak{N}, \mathfrak{P}) = 0$. *If $p|n$ then* $\mathrm{Hom}_{kSP_{2m}(W_r)}(\mathfrak{N}, \mathfrak{P}/\mathfrak{S}) = 0$.

Proof. Suppose p does not divide n. Consider the image of $\mathfrak{a}_1$ under ϕ in $\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathfrak{N}, \mathfrak{P})$. The relations from equations (11.2.2), (11.2.3) and (11.2.4) hold and imply that

$$\phi(\mathfrak{a}_1) = \sum_{j=2}^{n} a_{j,n+1}(e_{j,n+1} - e_{1,n+j}).$$

If $n \geq 3$ choose two distinct indices r and s both of which are also not equal to 1. Then $F_{rs}(1) \cdot \mathfrak{a}_1 = \mathfrak{a}_1$ and hence

$$\begin{aligned} \phi(\mathfrak{a}_1) &= F_{rs}(1) \cdot \phi(\mathfrak{a}_1) \\ &= \phi(\mathfrak{a}_1) + a_{s,n+1}(e_{r,n+1} - e_{1,n+r}) \end{aligned}$$

which implies that $a_{s,n+1} = 0$. Running through all suitable choices of r and s completes the proof. If $n = 2$ then $\phi(e_{1,3}) = a(e_{1,4} - e_{2,3})$ and acting on $\phi(e_{1,3})$ with $\sigma(12)$ implies that $\phi(e_{2,4}) = -a(e_{1,4} - e_{2,3})$. Therefore $\phi(e_{1,3} + e_{2,4}) = 0$ and as $\mathfrak{P}$ has no non trivial submodules ϕ is the zero map. The case $p|n$ clearly follows from this argument. □

Chapter 12

Cohomology of $SP_{2n}(W_r)$-modules

In this chapter the objective is to make the calculations necessary to prove Main Theorem 3 in the next chapter. The principal results here are summarised in the Theorem 12.0.7.

Theorem 12.0.7. *Let $n \geq 1$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

- *If $n = 1$ then $q = 4$ or $q \geq 7$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p.*

Then the following hold:

(i) $H^1(SP_{2n}(W_r), \mathfrak{M}_0) = (0)$.

(ii) *the map* $H^2(SP_{2n}(W_r), \mathfrak{N}) \to H^2(SP_{2n}(W_r), \mathfrak{M}_0)$ *induced from inclusion is injective.*

(iii) *the map* $H^2(SP_{2n}(W_r), \mathfrak{P}) \to H^2(SP_{2n}(W_r), \mathfrak{M}_0)$ *induced from inclusion is injective.*

As we shall see in Section 12.2, the proof of the above theorem is derived from the following proposition (whose proof is calculated from first principles in Section 12.1).

Prior to stating the proposition we recall the subgroup Ω of $SP_{2n}(k)$ from Definition 9.2.4. $\Omega = N \rtimes G$ where N is the abelian subgroup of Ω from Definition 9.2.2 and G is the subgroup isomorphic to $GL_n(k)$ from Definition 9.2.4, i.e. we have the following exact sequence:

$$I \to N \to \Omega = N \rtimes G \to G \to I. \tag{12.0.1}$$

The restriction of $\bar{\rho}$ to Ω, G, N defines an action of these subgroups on the $SP_{2n}(k)$-modules $\mathfrak{N}$, $\mathfrak{P}$ and $\mathfrak{M}_0$.

The application of (inflation-restriction) to the sequence (12.0.1) produces the exact sequence beginning

$$0 \to H^1(G, \mathcal{M}^N) \to H^1(\Omega, \mathcal{M}) \to H^1(N, \mathcal{M})^G \to \dots \tag{12.0.2}$$

Proposition 12.0.8. *Let $n \geq 1$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. Recall the subgroups G and N of $SP_{2n}(k)$ given in Definition 9.2.4 and Definition 9.2.2 respectively. We make the following restrictions on n and k:*

(i) If $n = 1$ then $q = 4$ or $q \geq 7$

(ii) If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p

then following hold:

1. $H^1(G, \mathfrak{N}^N) = (0)$
2. $H^1(G, \mathfrak{P}^N) = (0)$.
3. $H^1(N, \mathfrak{N})^G = (0)$.
4. $H^1(N, \mathfrak{P})^G = (0)$.

12.1 Proof of Proposition 12.0.8

The first and second parts of the proposition are proved simultaneously. This is achieved by showing that the group $H^1(G, {\mathfrak{M}_0}^N) = (0)$ and then illustrating how the separate parts of the proposition follow.

Before continuing we make a simple general observation. If g and h are two elements which commute of a group H, $\mathcal{M}$ be a H-module and $f \in H^1(H, \mathcal{M})$; then we have the equality:

$$f(g) - h \cdot f(g) = f(h) - g \cdot f(h). \tag{12.1.1}$$

This equation will be referenced many times in the current section.

Recall that Lemma 11.2.1 implies that if p is coprime to n then ${\mathfrak{M}_0}^N = \mathcal{B}$. If $g \in GL_n(k)$ then the action of G on $\mathcal{B}$ is described by:

$$\begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix} \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \begin{pmatrix} g^{-1} & 0 \\ 0 & g^T \end{pmatrix} = \begin{pmatrix} 0 & gBg^T \\ 0 & 0 \end{pmatrix} \tag{12.1.2}$$

Therefore if we define an action of $\gamma \in GL_n(k)$ on $M \in \mathfrak{M}_n$ by $\gamma \cdot M = \gamma M \gamma^T$ we obtain the following isomorphism

$$H^1(G, {\mathfrak{M}_0}^N) \cong H^1(GL_n(k), \mathfrak{M}(n))$$

Lemma 12.1.1. *With the restrictions:*

- *if $n = 1$ then $q = 4$ or $q \geq 7$*

- *if $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p*

we have that $H^1(SP_{2n}(k), \mathfrak{M}(n)) = (0)$.

Proof. If $n = 1$ then $SP_2(k) = SL_2(k)$ and has already been examined in Theorem 6.0.3. Therefore let $n \geq 2$ and note that the restrictions $p \geq 3$ and $q \geq 5$ ensure the existence of an element $u \in k^*$ satisfying $\mu^2 - 1 \neq 0$

Let f be an arbitrary 1-cocycle in $H^1(G, \mathfrak{M}(n))$ we consider the images of the elements of G and show that this defines a 1-coboundary.

Step (i). Fix an element μ in k^* satisfying $\mu^2 - 1 \neq 0$ and denote the image of μI under f as $f(\mu I) = \sum_{x,y} a_{xy} e_{xy}$. Let λ be a non-zero element of k. The group element $D_r(\lambda)$ commutes with μI. Equation (12.1.1) implies

$$\begin{aligned} \mu I \cdot f(D_r(\lambda)) - f(D_r(\lambda)) &= (\mu^2 - 1) f(D_r(\lambda)) \\ &= D_r(\lambda) \cdot f(\mu I) - f(\mu I) \\ &= (\lambda - 1)[\sum_{x \neq r} a_{xr} e_{xr} + \sum_{y \neq r} a_{ry} e_{ry}] + (\lambda^2 - 1) a_{rr} e_{rr}. \end{aligned}$$

We fix $\theta := (\mu^2 - 1)^{-1}$ and the equation above simplifies to give:

$$f(D_r(\lambda)) = \theta[(\lambda - 1)(\sum_{x \neq r} a_{xr} e_{xr} + \sum_{y \neq r} a_{ry} e_{ry}) + (\lambda^2 - 1) a_{rr} e_{rr}].$$

Step (ii). Similarly to the first step, here we specify $f(E_{ij}(\tau))$ using the fact that it commutes with μI. Equation (12.1.1) tells us that

$$\begin{aligned} (\mu^2 - 1) f(E_{ij}(\tau)) &= E_{ij}(\tau).f(\mu I) - f(\mu I) \\ &= \tau(\sum_x a_{xj} e_{xi} + \sum_y a_{jy} e_{iy} + \tau a_{jj} e_{ii}). \end{aligned}$$

Therefore the image of $E_{ij}(\tau)$ is given by

$$f(E_{ij}(\tau)) = \theta\tau(\sum_x a_{xj} e_{xi} + \sum_y a_{jy} e_{iy} + \tau a_{jj} e_{ii}).$$

Step (iii). All that remains is to verify that f is a 1-coboundary. To this end, set $X = \theta f(\mu I)$; to complete the proof we will show that $f(g) = g \cdot X - X$. Then firstly it is clear that:

$$\mu I \cdot \theta f(\mu I) - f(\mu I) = (\mu^2 - 1)\theta f(\mu I) = f(\mu I).$$

In step (i), when finding the image of $D_r(\lambda)$ under f, we essentially showed that:

$$\theta^{-1} f(D_r(\lambda)) = \theta^{-1}(D_r(\lambda) \cdot X - X).$$

This is clearly equivalent to $f(D_r(\lambda))$ satisfying the 1-coboundary condition. The argument in step (ii) analogously shows that:

$$\theta^{-1} f(E_{ij}(\tau)) = \theta^{-1}(E_{ij}(\tau) \cdot f(\mu I) - f(\mu I)).$$

□

Proof of Proposition 12.0.8, 1 and 2. From this proof we return to the proof of Proposition 12.0.8 parts 1 and 2. These results follow easily as we now observe. If f belongs to $H^1(G, \mathfrak{N}^N)$ or $H^1(G, \mathfrak{P}^N)$ then to complete the proof we must show that the matrix X of step (iii) belongs to $\mathfrak{N}$, respectively $\mathfrak{P}$. As X is defined as a scalar multiple of an element in the image of f, this is clear. □

Now we focus on Proposition 12.0.8 parts 3 and 4. In a manner akin to the proof of 1 and 2 we calculate $H^1(N, \mathfrak{M}_0)$ and use this to prove parts 3 and 4 separately.

Lemma 12.1.2. *If $p \geq 3$ and $n \geq 2$ then $H^1(N, \mathfrak{M}_0)^G = (0)$.*

Proof of Lemma 12.1.2 . Let f be an element of $H^1(N, \mathfrak{M}_0)^G$ we observe that for all g in G and $n \in N$ we have:

$$f(n) = g \cdot f(g^{-1}ng). \tag{12.1.3}$$

Step 1. Let us consider the image of $E_i(1)$ under f which we write in $n \times n$-block matrix form:

$$f(E_i(1)) = \begin{pmatrix} A^i & B^i \\ C^i & D^i \end{pmatrix}.$$

As $E_i(1)$ commutes with $E_j(1)$ for all j, we investigate the restrictions that equation (12.1.1) places on $f(E_i(1))$. Before we continue, we remark that if $j = i$ then the condition on the cocycles are vacuous. Equation (12.1.1) implies that the following matrix is zero

$$\begin{pmatrix} [-e_{ii}C^j] + [e_{jj}C^i] & [A^j e_{ii} + e_{ii}C^j e_{ii} - e_{ii}D^j] - [A^i e_{jj} + e_{jj}C^i e_{jj} - e_{jj}D^i] \\ 0 & [C^j e_{ii}] - [C^i e_{jj}] \end{pmatrix}. \tag{12.1.4}$$

Write $C^i = \sum_{x,y} c^i_{xy} e_{xy}$, then the top left and bottom right entry blocks give us respectively:

$$-\sum_x c^j_{ix} e_{ix} + \sum_y c^i_{jy} e_{jy} = 0 \tag{12.1.5}$$

$$\sum_x c^j_{xi} e_{xi} - \sum_y c^i_{yj} e_{yj} = 0 \tag{12.1.6}$$

This implies that the j-th row and j-th column of C^i are zero. Therefore the only possible non-zero entry of C^i is the (i,i)-th.

Let us now examine the top right entry, begining by observing that $e_{jj}C^i e_{jj} = 0$. Writing $A^i = \sum_{x,y} a^i_{xy} e_{xy}$ and $D^i = \sum_{x,y} d^i_{xy} e_{xy}$ this implies that:

$$\sum_x a^j_{xi} e_{xi} - \sum_y d^j_{iy} e_{iy} = \sum_x a^i_{xj} e_{xj} - \sum_y d^i_{jy} e_{jy}.$$

This means that, with the possible exceptions of $a^i_{jj} = d^i_{jj}$ and $a^i_{ij} = -d^j_{ij}$, the entries of the j-th column of A^i are zero. Similarly with these two possible exceptions the entries of the j-th row of D^i are zero.

Step 2. Next define D_r to be the diagonal matrix with -1 in both its (r,r)-th and $(n+r,n+r)$-th entries and 1s elsewhere on the diagonal. We remark that D_r is its own inverse. As D_r commutes with $E_i(1)$, equation (12.1.3) implies that

$$D_r f(E_{i,n+i}(1))D_r = f(E_{i,n+i}(1)). \tag{12.1.7}$$

Running through all $1 \leq r \leq n$ implies that the only possible non-zero entries of $f(E_i(1))$ are on the diagonals of A^i, B^i, C^i and D^i. Combining all of what we have so far gives:

$$\begin{array}{ll} A^i = \sum_x a^i_{xx} e_{xx} & B^i = \sum_x b^i_{xx} e_{xx} \\ C^i = \lambda^i e_{ii} & D^i = \sum_{x \neq i} a^i_{xx} e_{xx} + d^i_{ii} e_{ii} \end{array} \tag{12.1.8}$$

Step 3. Let us introduce the images under f of the $G_{rs}(1)$ to the discussion, which we write as

$$f(G_{rs}(1)) = \begin{pmatrix} X^{rs} & Y^{rs} \\ W^{rs} & Z^{rs} \end{pmatrix}.$$

As $G_{rs}(1)$ commutes with $E_i(1)$ equation (12.1.1) implies that for all i the matrix

$$\begin{pmatrix} -e_{ii}W^{rs} & X^{rs}e_{ii} + e_{ii}W^{rs}e_{ii} - e_{ii}Z^{rs} \\ 0 & W^{rs}e_{ii} \end{pmatrix} \tag{12.1.9}$$

is equal to

$$\begin{pmatrix} -(e_{rs}+e_{sr})C^i & A^i(e_{rs}+e_{sr}) + (e_{rs}+e_{sr})C^i(e_{rs}+e_{sr}) - (e_{rs}+e_{sr})D^i \\ 0 & C^i(e_{rs}+e_{sr}) \end{pmatrix}. \tag{12.1.10}$$

We write $W^{rs} = \sum_{a,b} w_{ab} e_{ab}$ and then set $i = r$. Comparing the top left hand blocks of the two matrices immediately above gives

$$\lambda^r e_{sr} = \sum_a w^{rs}_{ra} e_{ra}.$$

Noting $s \neq i$, this equality firstly implies that $\lambda^r = 0$ thus $C^r = 0$. Secondly, it also implies that the r-th row of W^{rs} consists of zeros. As $\lambda^i = 0$ for all i, if $i = s$ or $i \neq r$, s the top left hand blocks imply that i-th rows consist of zeros. Therefore, the block W^{rs} is zero.

Step 4. F_{is} commutes with $E_{i,n+i}(1)$ for each permissable value of s. Equation (12.1.3) then implies that $F_{is} f(E_i(1)) F_{is}^{-1} = f(E_i(1))$. Consequently

$$f(E_i(1)) = \begin{pmatrix} E_{is}(1)A^i E_{is}(-1) & E_{is}(1)B^i E_{si}(1) \\ 0 & E_{si}(-1)D^i E_{si}(1) \end{pmatrix} \tag{12.1.11}$$

Comparing top left hand blocks implies that $a^i_{ss} = a^i_{ii}$. Similarly, comparing bottom right hand blocks implies that $d^i_{ii} = a^i_{ii}$. Examining the top right hand block implies that $b^i_{ss}(e_{is} + e_{si} + e_{ii})$, hence $b^i_{ss} = 0$. Allowing s to take all permissable values implies that we may write the image of $E_i(1)$ under f in the form:

$$f(E_i(1)) = a^i I + b^i e_{i,n+i}$$

As $\sigma(ij)$ belongs to G and $\sigma(ij)E_i(1)\sigma(ij) = E_j(1)$, equation (12.1.3) implies $f(E_i(1)) = \sigma(ij)f(E_j(1))\sigma(ij)$. Therefore $a^i = a^j := a$ and $b^i = b^j := b$ and we may write

$$f(E_i(1)) = aI + be_{i,n+i}.$$

Step 5. We switch back to examining the restrictions placed on f from the fact that $E_i(1)$ and $G_{rs}(1)$ commute, i.e. re-examining the implications of the equality of equations (12.1.9) and (12.1.10), we see that the top right hand block of equation (12.1.10) is zero. If we set $i = r$ we have

$$\sum_a x_{ar}e_{ar} - \sum_b z_{rb}e_{rb} = 0$$

which implies that $x_{ar} = 0$ if $a \neq r$, $z_{rb} = 0$ if $b \neq r$ and that $x_{rr} = z_{rr}$. Similarly, setting $i = s$ gives that $x_{as} = 0$ if $a \neq s$, $z_{sb} = 0$ if $b \neq s$ and that $x_{ss} = z_{ss}$. If $n \geq 3$ then set $i \neq r$, s and analogously this implies that $x_{ai} = 0$ if $a \neq i$, $z_{ib} = 0$ if $b \neq i$ and that $x_{ii} = z_{ii}$. In summary we write the image of $G_{rs}(1)$ under f in the form:

$$\begin{pmatrix} D^{rs} & M^{rs} \\ 0 & D^{rs} \end{pmatrix}$$

where D^{rs} is a diagonal matrix.

Step 6. Observe that $D_rG_{rs}(1)D_r = G_{rs}(1)^{-1} = D_sG_{rs}(1)D_s$. As D_r and D_s both belong to G equation (12.1.3) implies

$$f(G_{rs}(1)) = D_rf(G_{rs}(1)^{-1})D_r = -D_rG_{rs}(1)^{-1}f(G_{rs}(1))G_{rs}(1)D_r \qquad (12.1.12)$$

where the second equality follows from the definition of a 1-cocycle via the observation $0 = f(g^{-1}g) = f(g^{-1}) + g^{-1} \cdot f(g)$. Now we examine the implications of equation (12.1.12).

$$\begin{pmatrix} D^{rs} & M^{rs} \\ 0 & D^{rs} \end{pmatrix} = -\begin{pmatrix} D_rD^{rs}D_r & M' \\ 0 & D_rD^{rs}D_r \end{pmatrix} \qquad (12.1.13)$$

where

$$M' = D_rD^{rs}(e_{rs} + e_{sr})D_r + D_rM^{rs}D_r - D_r(e_{rs} + e_{sr})D^{rs}D_r.$$

Looking at the top left hand block we restate that since both D_r and D^{rs} are diagonal matrices they commute and hence $D^{rs} = 0$. This also implies that

$$M' = D_rM^{rs}D_r$$

and from a comparison of the top right hand blocks it is clear that the only possible non-zero entries of M^{rs} are m_{ra} for all $a \neq r$ and m_{br} for all $b \neq r$. Combining this with the analogous condition deriving from D_s implies that

$$M^{rs} = m_{rs}e_{rs} + m_{sr}e_{sr}$$

Note that $\sigma(rs)G_{rs}(1)\sigma(rs) = G_{rs}(1)$ and hence that

$$f(G_{rs}(1)) = \sigma(rs)f(G_{rs}(1))\sigma(rs).$$

This clearly implies that $m_{rs}e_{rs} + m_{sr}e_{sr} = m_{sr}e_{rs} + m_{rs}e_{sr}$ i.e that $m_{rs} = m_{sr} := m^{rs}$. Therefore we have shown

$$f(G_{rs}(1)) = m^{rs}(e_{r,n+s} + e_{s,n+r})$$

If $n = 2$, $G_{12}(1)$ is the only element of this form and we may write $f(G_{12}(1)) = m(e_{12} + e_{21})$. This may also be done when $n \geq 3$. The equalities

$$\begin{aligned} \sigma(xr) \cdot G_{rs}(1) = &\quad G_{xs}(1) \\ \sigma(sy) \cdot G_{xs}(1) = &\quad G_{xy}(1) \end{aligned}$$

imply the equalities

$$f(G_{rs}(1)) = m^{rs}(e_{rs} + e_{sr}) = \sigma(xr) \cdot G_{xs}(1) = m^{xs}(e_{rs} + e_{sr}) \quad (12.1.14)$$

$$f(G_{xs}(1)) = m^{xs}(e_{xs} + e_{sx}) = \sigma(sy) \cdot f(G_{xy}(1)) = m^{xy}(e_{xs} + e_{sx}). \quad (12.1.15)$$

Therefore m^{rs} does not depend on either r or s and we may write:

$$f(G_{rs}(1)) = m(e_{r,n+s} + e_{s,n+r}).$$

Step 7. In reference to the images of $G_{rs}(1)$ and $E_i(1)$, we will now show that $b = m$ and $a = 0$. To this end, observe that $F_{rs}(1) \cdot G_{rs}(1) = E_r(2)G_{rs}(1)$ which implies

$$f(G_{rs}(1)) = F_{rs}(1)^{-1} \cdot [f(E_r(2)) + E_r(2).f(G_{rs}(1))] \quad (12.1.16)$$

and we set about calculating the left hand side of this equality. Remarking that both $E_i(1)$ and $G_{rs}(1)$ commute with both of their images, the observation

$$F_{rs}(1)^{-1} \cdot [E_r(2).f(G_{rs}(1))] = m(e_{r,n+s} + e_{s,n+r} - 2e_{r,n+r})$$

implies that collecting all this together implies that equation (12.1.16) is equivalent to

$$m(e_{r,n+s} + e_{s,n+r}) = 2(aI + be_{r,n+r}) + m(e_{r,n+s} + e_{s,n+r} - 2e_{r,n+r}).$$

As the characteristic of k is not equal to 2, $a = 0$ and $b = m$. In summary the images have the forms:

$$f(E_r(1)) = be_{r,n+r}, \qquad f(G_{rs}(1)) = b(e_{r,n+s} + e_{s,n+r}).$$

Step 8. In conjunction with the final step, the calculations made so far are sufficient if $k = \mathbb{F}_p$ but for general k we require a supplementary argument. Let x be an arbitrary element of k. Then define $D_r(x)$ to be the diagonal matrix with x in the (r, r)-th entry, x^{-1} in the $(n+r, n+r)$-th entry and $1s$ on the other diagonals. Then by equation (12.1.3), the equality $D_r(x) \cdot G_{rs}(1) = G_{rs}(x)$ implies

$$f(G_{rs}(x)) = D_r(x) \cdot f(G_{rs}(1)) = xf(G_{rs}(1)).$$

For the images of $E_i(x)$ recall the third relation of 11 in Proposition 9.4.1. If $\lambda = x$ and $\mu = 2^{-1}$ then this relation implies $F_{rs}(x)G_{rs}(2^{-1})F_{rs}(-x) = E_r(x)G_{rs}(2^{-1})$. Utilising equation (12.1.3) again yields the equality:

$$\begin{aligned} f(E_r(x)) &= F_{rs}(x) \cdot f(G_{rs}(2^{-1}) - f(G_{rs}(2^{-1}))) \\ &= xf(E_r(1)). \end{aligned}$$

Step 9. We conclude by showing that f is a coboundary. Define a matrix in $\mathfrak{M}_0$ by

$$X = 2^{-1}b\sum_{a=1}^{n}(e_{n+a,n+a} - e_{a,a}).$$

Then the calculations

$$\begin{aligned} (1 + xe_{i,n+i}) \cdot X &= X + bxe_{i,n+i} \\ (1 + xe_{r,n+s} + xe_{s,n+r}) \cdot X &= X + bx(e_{r,n+s} + e_{s,n+r}) \end{aligned}$$

imply that f is indeed a coboundary.

□

Proof of Proposition 12.0.8, 3 and 4. Consider f in $H^1(N, \mathfrak{N})$: in the proof of Lemma 12.1.2 above we showed that for $f \in H^1(N, \mathfrak{M}_0)^G$ the image of f in fact belongs to $\mathfrak{N}$. Moreover, in step 9 of the proof above the element X, which is used to show that f is a coboundary, is an element of $\mathfrak{N}$. Thus it is clear that $H^1(N, \mathfrak{N})^G = (0)$.

Now suppose that f belongs to $H^1(N, \mathfrak{P})^G$. As the top right hand $n \times n$ block of elements of $\mathfrak{P}$ are skew symmetric steps 7 and 8 of the proof of Lemma 12.1.2 above imply that $f(E_i(x)) = 0$ and $f(G_{rs}(x)) = 0$. Therefore, $H^1(N, \mathfrak{P})^G = (0)$ and step 9 is not required. □

12.2 Proof of Theorem 12.0.7

Now we use Proposition 12.0.8 to complete the proof of Theorem 12.0.7. These calculations are greatly simplified using standard cohomological results as is now demonstrated. The following is Proposition 6 in Chapter VII of [30].

Proposition 12.2.1. *If $\Omega < \Gamma$ are two groups and $\mathcal{M}$ a Γ-module, then the composition*

$$H^1(\Gamma, \mathcal{M}) \xrightarrow{res} H^1(\Omega, \mathcal{M}) \xrightarrow{cores} H^1(\Gamma, \mathcal{M}) \tag{12.2.1}$$

is multiplication by the index $[\Gamma : \Omega]$.

Corollary 12.2.2. *If $[\Gamma : \Omega]$ is coprime to p then the composite map $cores \circ res$ is injective. Therefore, the map*

$$res : H^1(\Gamma, \mathcal{M}) \to H^1(\Omega, \mathcal{M}) \tag{12.2.2}$$

is injective.

For further details of the results above see [30] or [21]. We apply this result to our context. To this end, fix $\Gamma = SP_{2n}(k)$ and the subgroup Ω to be its namesake defined in 9.2.4. As remarked previously Ω contains the p-sylow subgroup of $SP_{2n}(k)$ hence the index $[SP_{2n}(k) : \Omega]$ is coprime to p. Therefore for an arbitrary $kSP_{2n}(k)$-module $\mathcal{M}$ Corollary 12.2.2 implies there is an injection:

$$H^1(SP_{2n}(k), \mathcal{M}) \to H^1(\Omega, \mathcal{M}).$$

Thus if $H^1(\Omega, \mathcal{M}) = (0)$ we may conclude that $H^1(SP_{2n}(k), \mathcal{M})$ is also trivial.

In fact the calculation can be simplified even further. Recall the group extension (12.0.1) specified by $\Omega = N \rtimes G$ and the exact cohomology sequence given in equation 12.0.2 which we restate below:

$$0 \to H^1(G, \mathcal{M}^N) \to H^1(\Omega, \mathcal{M}) \to H^1(N, \mathcal{M})^G \to \dots$$

From this, we obtain the following criterion for determining $H^1(SP_{2n}(k), \mathcal{M})$.

Corollary 12.2.3. *Let Ω, G and N be the subgroups of $SP_{2n}(k)$ given in Definitions 9.2.4 and 9.2.2. If $H^1(G, \mathcal{M}^N) = H^1(N, \mathcal{M})^G = (0)$ then $H^1(\Omega, \mathcal{M}) = H^1(SP_{2n}(k), \mathcal{M}) = (0)$.*

Corollary 12.2.4. *Let $n \geq 1$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n and k:*

(i) If $n = 1$ then $q = 4$ or $q \geq 7$

(ii) If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p

then following hold:

(1) $H^1(SP_{2n}(k), \mathfrak{N}) = (0)$

(2) $H^1(SP_{2n}(k), \mathfrak{P}) = (0)$.

Proof. After invoking Corollary 12.2.3 the result follows immediately from Proposition 12.0.8. □

Recall the map $\varepsilon : \mathfrak{M}_0 \to K_r$ from equation (5.2.4). Its restriction to the submodule $\mathfrak{N}$ defines an isomorphism $\varepsilon|_{\mathfrak{N}} : \mathfrak{N} \to K_r(\mathfrak{N})$ where the latter is given by

$$K_r(\mathfrak{N}) := \{I + p^r n \mid n \in \mathfrak{N}\}. \tag{12.2.3}$$

Similarly recall that ε is a one-sided inverse to the map $\phi|_{K(\mathfrak{N})} : K(\mathfrak{N}) \to \mathfrak{N}$ given by $\phi(I + p^r n) = n \bmod p^r$. We remark that $K_r(\mathfrak{P})$, $\varepsilon|_{\mathfrak{P}}$ and $\phi|_{K_r(\mathfrak{P})}$ are defined similarly. The next result is analogous to Proposition 6.1.2 and Lemma 6.2.1.

Proposition 12.2.5. *Let $n \geq 1$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions:*

- *If $n = 1$ then $q = 4$ or $q \geq 7$*

- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p.*

Let $\pi : SP_{2n}(W_{r+1}) \to SP_{2n}(W_r)$ be componentwise reduction modulo p^r.

(1) The following sequence does not split

$$I \to K_r(\mathfrak{N}) \to SP_{2n}(W_{r+1}) \xrightarrow{\pi} SP_{2n}(W_r) \to I. \tag{12.2.4}$$

(2) If E be a subgroup of $SL_{2n}(W_{r+1})$ which fits into the exact sequence

$$I \to K(\mathfrak{M}_0)/K(\mathfrak{P}) \to E/K(\mathfrak{P}) \xrightarrow{\pi'} SP_{2n}(W_r) \to I \tag{12.2.5}$$

where π' is induced from the reduction modulo p^r map $SP_{2n}(W_{r+1}) \to SP_{2n}(W_r)$, then the exact sequence above does not split.

Proof. We remark that if $n = 1$ then $SP_2(W_r) = SL_2(W_r)$ and so the proof is covered in Chapter 6. Therefore, assume $n \geq 2$.

For Part (1): suppose that this sequence splits. Thus there is a group homomorphism $s : SP_{2n}(W_r) \to SP_{2n}(W_{r+1})$ such that $\pi \circ s = id$. We consider the image of the element $E_1(x)$ of $SP_{2n}(W_r)$ under the map s, which must be of the form

$$s(E_1(x)) = E_1(t) + p^r\mu$$

where $t := t(x)$ is a lifting of x to W_{r+1} and $\mu := \mu(i,j)$ belongs to $M_{2n}(W_{r+1})$ then $\pi(\mu) = 0$. The condition on μ implies that it is annihilated by p. We write $g = E_1(t)$, $\lambda = p^r$ and calculate

$$\begin{aligned} s(g)^\lambda &= g^\lambda + \sum_{z=0}^{\lambda-1} g^{\lambda-1-z}\mu g^z \\ &= E_1(\lambda t) + M \end{aligned}$$

where the matrix M has the form

$$\sum_{z=0}^{\lambda}\left[\mu + t(\lambda-1-z)\sum_b \mu_{n+1,b}e_{1b} + zt\sum_a \mu_{a1}e_{a,n+1} + t^2(\lambda-1-z)z\mu_{n+1,1}e_{1,n+1}\right].$$

As λ annihilates the entries of μ the summation over z of the bracketed term above may be simplified to:

$$t\frac{\alpha}{2}\left(\sum_a \mu_{a1}e_{aj} - \sum_b \mu_{n+1,b}e_{1b}\right) + t^2\left(\frac{\beta}{2} - \frac{\delta}{6}\right)\mu_{n+1,1}e_{1,n+1} \tag{12.2.6}$$

where $\alpha = \lambda(\lambda-1)$, $\beta = \lambda(\lambda-1)^2$ and $\delta = \lambda(\lambda-1)(2\lambda-1)$. Therefore if either $p > 3$ (and so does not divide 6) or $r > 1$ (and so p divides $\alpha/2$, $\beta/2$ and $\delta/6$) the sum of the bracket is zero. This implies that in these cases $s(E_1(x))^{p^r} = E_1(p^r t)$. If x is a unit in W_r then t must be a unit in W_{r+1} and as such is not annihilated by p^r. This is a contradiction to the existence of the section s.

If $p = 3$ then define a map $m : W_r \to k$ by $m(x) = \mu_{n+1,1}$ where $p^r W_{r+1}$ has been identified with k. The equality

$$e_{1,n+1}s(E_1(x_1 + x_2))e_{1,n+1} = e_{1,n+1}s(E_1(x_1))s(E_1(x_2))e_{1,n+1}$$

implies that $m(x_1 + x_2) = m(x_1) + m(x_2)$. Equation (12.2.6) implies that $m(x) = -t^{-1}$ for all $t \in k$. If $k \neq \mathbb{F}_3$, then this is a contradiction.

For Part (2): let x be a unit in $SP_{2n}(W_r)$. If s be a section for π then from the proof of Proposition 6.1.2 the image of $E_i(x)$ must belong to the identity coset in $E/K(\mathfrak{P})$. However equation (12.2.6) clearly implies that this is not the case. □

Proposition 12.2.6. *Let $n \geq 1$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions:*

- *If $n = 1$ then $q = 4$ or $q \geq 7$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and n is coprime to p.*

1. *The inflation map $H^1(SP_{2n}(W_r), \mathfrak{N}) \to H^1(SP_{2n}(W_{r+1}), \mathfrak{N})$ is an isomorphism. Therefore $H^1(SP_{2n}(W_r), \mathfrak{N}) = (0)$ for all r.*
2. *The inflation map $H^1(SP_{2n}(W_r), \mathfrak{P}) \to H^1(SP_{2n}(W_{r+1}), \mathfrak{P})$ is an isomorphism. Therefore $H^1(SP_{2n}(W_r), \mathfrak{P}) = (0)$ for all r.*

Proof. Let $\mathcal{M} = \mathfrak{N}, \mathfrak{P}$ and observe the exact sequence

$$0 \to \mathfrak{N} \xrightarrow{\epsilon|_{\mathfrak{N}}} SP_{2n}(W_{r+1}) \to SP_{2n}(W_r) \to I \tag{12.2.7}$$

Then invoking Proposition 4.1.6 (inflation-restriction) yields the exact cohomology sequence

$$0 \to H^1(SP_{2n}(W_r), \mathcal{M}) \to H^1(SP_{2n}(W_{r+1}), \mathcal{M}) \to H^1(K(\mathfrak{N}), \mathcal{M})^{SP_{2n}(W_r)} \xrightarrow{\delta} H^2(SP_{2n}(W_r), \mathcal{M}) \to$$

where we have noted that $K(\mathfrak{N})$ acts trivially on $\mathcal{M}$,

If $\mathcal{M} = \mathfrak{N}$ then by Proposition 11.2.5 $\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathfrak{N}, \mathfrak{N}) \cong k$ and by an argument similar to that in Proposition 5.2.1 $\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathfrak{N}, \mathfrak{N}) \cong H^1(K(\mathfrak{N}), \mathfrak{N})^{SP_{2n}(W_r)}$. Therefore we must show that δ is injective to complete the proof. By Proposition 12.2.5 the sequence (12.2.4) does not split. Writing the extension additively as

$$0 \to \mathfrak{N} \xrightarrow{\epsilon} \mathfrak{N} \rtimes_x SP_{2n}(W_r) \xrightarrow{\pi} SP_{2n}(W_r) \to I$$

where the map ϵ is a one-sided inverse to ϕ, it is clear that Proposition 4.3.1 implies that δ maps $-\phi$ to the class of x in $H^2(SL_n(W_r), \mathfrak{N})$. Hence the inflation map is an isomorphism and by Corollary 12.2.4:

$$H^1(SP_{2n}(W_{r+1}), \mathfrak{N}) \cong H^1(SP_{2n}(k), \mathfrak{N}) = (0).$$

If p does not divide n and if $\mathcal{M} = \mathfrak{P}$ then $\mathrm{Hom}_{kSP_{2n}(W_r)}(\mathfrak{N}, \mathfrak{P}) \cong H^1(K(\mathfrak{N}), \mathfrak{P}) = (0)$ by Corollary 11.2.6. Thus the inflation-restriction sequence above in conjunction with Corollary 12.2.4 implies

$$H^1(SP_{2n}(W_r), \mathfrak{P}) \cong H^1(SP_{2n}(k), \mathfrak{P}) = (0).$$

□

Proof of Theorem 12.0.7. For Part (i) we apply the long exact cohomology sequence (Proposition 6.0.4) to following exact sequence of $SP_{2n}(W_r)$-modules:

$$0 \to \mathfrak{N} \to \mathfrak{M}_0 \to \mathfrak{P} \to 0.$$

This yields the following excerpt of an exact cohomology sequence

$$\to H^1(SP_{2n}(W_r), \mathfrak{N}) \to H^1(SP_{2n}(W_r), \mathfrak{M}_0) \to H^1(SP_{2n}(W_r), \mathfrak{P}) \to . \quad (12.2.8)$$

Proposition 12.2.6 implies that both $H^1(SP_{2n}(W_r), \mathfrak{N})$ and $H^1(SP_{2n}(W_r), \mathfrak{P})$ are (0), hence part (i) follows. which from the preceding parts of this proof clearly implies that $H^1(SP_{2n}(W_r), \mathfrak{M}_0) = (0)$.

For Part (ii), note that the exact cohomology sequence in equation (12.2.8) continues to

$$\to H^1(SP_{2n}(W_r), \mathfrak{P}) \to H^2(SP_{2n}(W_r), \mathfrak{N}) \xrightarrow{f} H^2(SP_{2n}(W_r), \mathfrak{M}_0) \to .$$

As $H^1(SP_{2n}(W_r), \mathfrak{P}) = (0)$ the map f is clearly injective.

Part (iii) follows similarly by considering the sequence $0 \to \mathfrak{P} \to \mathfrak{M}_0 \to \mathfrak{N}$ and recalling that $H^1(SP_{2n}(W_r), \mathfrak{N}) = (0)$.

□

Chapter 13

Proof of Main Theorem 3

The proof of Main Theorem 3 has the same form as that of Theorem 1.2.5 relying on the artinian case covered in Proposition 13.0.7. The extension of Proposition 13.0.7 to Main Theorem 3 is exactly similar to the way Theorem 1.2.5 follows from Proposition 7.0.5, namely by defining a refinement of the chain of ideals:

$$m_A \supseteq m_A^2 \supseteq m_A^3 \supseteq \dots$$

and inductive limit.

Therefore all that remains is to prove the following result.

Proposition 13.0.7. *Let n be a positive integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the following restrictions on n, p and q:*

- *If $n = 1$ then $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$*
- *If $n \geq 2$ then $p \geq 3$, $q \geq 5$ and p is coprime to n.*

Let (A, m_A) be an artinian ring in $\mathcal{C}(k)$ and $t \in A$ be a non-zero element such that $tm_A = 0$. If G be a subgroup of $SL_{2n}(A)$ with the property $G \bmod t = SP_{2n}(W_B)$ where $B = A/(t)$, then there exists $X \in SL_{2n}(A)$ with $X \equiv I \bmod t$ such that $SP_{2n}(W_A) \subseteq XGX^{-1}$.

Proof. Let $\pi : A \to B$ be reduction modulo t. Recall the map $\varepsilon|_{\mathfrak{N}} : \mathfrak{N} \to SP_{2n}(A)$. Thus, there is an exact sequence

$$0 \to \mathfrak{N} \xrightarrow{\varepsilon|_{\mathfrak{N}}} SP_{2n}(A) \xrightarrow{\pi} SP_{2n}(B) \to 1 \tag{13.0.1}$$

Let $\tilde{G}$ denote the pre-image under π of $SP_{2n}(W_B)$ in $SL_{2n}(A)$ this defines the following exact sequence:

$$0 \to \mathfrak{M}_0 \xrightarrow{\varepsilon|_{\mathfrak{N}}} \tilde{G} \xrightarrow{\pi} SP_{2n}(W_B) \to 1. \tag{13.0.2}$$

We observe that both G and $SP_{2n}(W_A)$ are subgroups of $\tilde{G}$ and examine the possible subgroup structures relating these three. There are four cases to investigate.

(1) $G = \tilde{G}$, in which case $SP_{2n}(A) \subseteq G$ and we are finished.

(2) $\pi : G \to SP_{2n}(W_B)$ is an isomorphism.

(3) G fits into an exact sequence

$$0 \to \mathfrak{N} \to G \to SP_{2n}(W_B) \to I \tag{13.0.3}$$

(4) G fits into an exact sequence

$$0 \to \mathfrak{P} \to G \to SP_{2n}(W_B) \to I. \tag{13.0.4}$$

Let's investigate case (2). As $\pi : G \to SP_{2n}(W_B)$ is an isomorphism the sequence (13.0.2) splits. This implies that $\widetilde{G} = \mathfrak{M}_0 \rtimes SP_{2n}(W_B)$ and that $SP_{2n}(W_A) = \mathcal{M} \rtimes SP_{2n}(W_B)$ where $\mathcal{M}$ is either 0 or $\mathfrak{N}$. As $H^2(SP_{2n}(W_B), \mathfrak{N}) \to H^2(SP_{2n}(W_B), \mathfrak{M}_0)$ is injective any extension $E = \mathfrak{N} \rtimes_x SP_{2n}(W_B)$ must also split hence by Proposition 12.2.5 we must have $SP_{2n}(W_A) \cong SP_{2n}(W_B)$. Therefore G is a twist of $SP_{2n}(W_A)$ by an element of $H^1(SP_{2n}(W_B), \mathfrak{M}_0)$. Theorem 12.0.7 (i) implies $H^1(SP_{2n}(W_B), \mathfrak{M}_0) = (0)$ and thus Proposition 4.3.3 (3) implies that there exists $X \in SL_{2n}(A)$ with $\pi(X) = I$ such that $XGX^{-1} \supseteq SP_{2n}(W_A)$.

In case (3) G contains a subgroup which is a twist of $SP_{2n}(W_A)$ by an element of $H^1(SP_{2n}(W_B), \mathfrak{N})$ and as $H^1(SP_{2n}(W_B), \mathfrak{M}_0) = (0)$ as above this case may be concluded.

Finally, we consider case (4). Theorem 12.0.7 states that the map

$$H^2(SP_{2n}(W_B), \mathfrak{P}) \to H^2(SP_{2n}(W_B), \mathfrak{M}_0)$$

induced from inclusion is injective. The sequence (13.0.4) defines an isomorphism

$$f : SP_{2n}(W_B) \to G/K(\mathfrak{P}).$$

If we assume $W_A = W_{r+1}$ and $W_B = W_r$ for some natural number r then $\iota \circ f$ is a section for π in the sequence (12.2.5). However, this contradicts Proposition 12.2.5 (2). Therefore $SP_{2n}(W_A) \cong SP_{2n}(W_B)$ and, as the map $H^2(SP_{2n}(W_B), \mathfrak{P}) \to H^2(SP_{2n}(W_B), \mathfrak{M}_0)$ induced from inclusion is injective, the result follows using $H^1(SP_{2n}(W_B), \mathfrak{M}_0)$ as above. □

Chapter 14

Symplectic Deformations

In this chapter we consider another generalisation of the SL_2 deformation problem, i.e. residual representations of the form $\rho : SL_2(A) \to SL_2(k)$. As observed previously $SL_2(A) = SP_2(A)$ and this time we are lead to a different deformation problem. The results of this chapter prove Main Theorem 4 (described below in Section 14.1), hence giving an affirmative answer to the inverse symplectic deformation problem (also in Section 14.1) for all rings in $\mathcal{C}(k)$, provided k is not $\mathbb{F}_2$ or $\mathbb{F}_3$.

14.1 Symplectic Deformation Problem

Let k be a finite field and let Γ be a profinite group. Suppose there is a residual representation

$$\bar{\rho} : \Gamma \to SP_{2n}(k)$$

and consider *symplectic deformations* by which we mean a deformation of the form

$$\rho : \Gamma \to SP_{2n}(A)$$

where A belongs to $\mathcal{C}(k)$. Now set to $\Gamma = SP_{2n}(A)$ and the residual representation to

$$\bar{\rho} : \Gamma \to SP_{2n}(k),$$

where $\bar{\rho}$ is reduction modulo m_A. We observe that $\bar{\rho}$ is surjective and therefore that the centraliser of the image of $\bar{\rho}$ coincides with the centre of $SP_{2n}(k)$.

This leads to the question of whether or not there is the notion of a universal deformation and universal deformation ring in this setting. The following result, an extension of Theorem 1.1.6, is a paraphrasing of Theorem 2.2 in [7] and confirms that this is the case.

Theorem 14.1.1. *Let Γ be a profinite group with the property that for every open subgroup $\Gamma_0 < \Gamma$ of finite index the number of continuous homomorphisms from Γ_0 to $\mathbb{F}_p$ is finite and let $\bar{\rho} : \Gamma \to SP_{2n}(k)$ be a continuous representation.*

If $\bar{\rho}$ is absolutely irreducible and the centraliser of the image of $\bar{\rho}$ is contained in the centre of $SP_{2n}(k)$, then there exists a universal deformation ring $R := R(\bar{\rho})$

and a universal deformation $\rho_R : \Gamma \to SP_{2n}(R)$, i.e. for each deformation $\rho : \Gamma \to SP_{2n}(A)$ there is a local ring homomorphism $h : R \to A$ such that $h \circ \rho_R$ is equivalent to ρ.

Returning to the symplectic deformation problem it is clear from our discussions that $\Gamma = SP_{2n}(A)$ and $\bar{\rho} : \Gamma \to SP_{2n}(k)$ as above satisfy the conditions of the theorem and consequently the existence of a universal deformation ring is confirmed. This brings us to state the following.

Main Theorem 4. *Let $k = \mathbb{F}_q$ where the characteristic of k is p. If $q \geq 4$ then every element of $\mathcal{C}(k)$ is a universal deformation ring of the residual representation $\bar{\rho} : SP_{2n}(A) \to SP_{2n}(k)$ given by reducing the standard representation $\rho_A : SP_{2n}(A) \to SP_{2n}(A)$ modulo m_A.*

More precisely, for the symplectic deformation problem we show that A is the universal deformation ring in the following cases:

1. *$n = 1$ and $q \neq 2$, 3 or 5*
2. *$n \geq 2$, $p \geq 3$ and $q \geq 5$.*

14.2 Structure of Symplectic Deformations

Similarly to the previous cases we require the following structure result for subroups of $SP_{2n}(A)$.

Theorem 14.2.1. *Let $n = 1$ or $n \geq 3$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the additional restrictions:*

- *If $n = 1$ then $q \neq 2, 3, 5$*
- *If $n \geq 2$ then $p > 2$ and $q \neq 3$.*

Let (A, m_A) belong to $\mathcal{C}(k)$. If G is a closed subgroup of $SP_{2n}(A)$ satisfying $G \bmod m_A = SP_{2n}(k)$, then there exists an $X \in SP_{2n}(A)$ with $X \cong I \bmod m_A$ such that $SP_{2n}(W_A) \subseteq XGX^{-1}$.

Just as in the two previous occasions this theorem follows from the following artinian case. We recall that Proposition 11.1.4 implies $\mathfrak{N}$ is a simple $kSP_{2n}(k)$-module.

Proposition 14.2.2. *Let $n = 1$ or $n \geq 3$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the additional restrictions:*

- *If $n = 1$ then $q \neq 2, 3, 5$*
- *If $n \geq 2$ then $p > 2$ and $q \neq 3$.*

Let (A, m_A) belong to $\mathcal{C}(k)$, t be a non zero element of A satisfying $tm_A = 0$, and $B = A/(t)$. If G is subgroup of $SP_{2n}(A)$ satisfying $G \bmod t = SP_{2n}(W_B)$, then there exists an $X \in SP_{2n}(A)$ with $X \cong I \bmod t$ such that $SP_{2n}(W_A) \subseteq XGX^{-1}$.

Proof. The notation is taken to be the same as that in Proposition 13.0.7. The first difference comes to at point where the pre-image of $SP_{2n}(W_B)$ is necessarily specified as a subgroup $SP_{2n}(A)$. Thus $\tilde{G}$ fits into the exact sequence

$$0 \to \mathfrak{N} \to \tilde{G} \xrightarrow{\pi} SP_{2n}(W_B) \to I. \tag{14.2.1}$$

As before both G and $SP_{2n}(W_A)$ are subgroups of $\tilde{G}$. This time there are only two cases:

1. $G = \tilde{G}$
2. $\pi : G \to SP_{2n}(W_B)$ is an isomorphism

The conclusion in case 1 is trivial. For case 2 the argument is similar to that of Proposition 13.0.7. As $\pi : G \to SP_{2n}(W_B)$ is an isomorphism the sequence (14.2.1) splits and $\tilde{G} = \mathfrak{N} \rtimes SP_{2n}(W_B)$. Therefore as $\mathfrak{N}$ is simple we have trivially that for all submodules $\mathcal{N} \leq \mathfrak{N}$ the maps $H^2(G, \mathcal{N}) \to H^2(G, \mathfrak{N})$ are injective. This implies that G is a twist of $SP_{2n}(W_A)$ by an element of $H^1(SP_{2n}(W_B), \mathfrak{N})$ and by Theorem 12.0.7 this cohomology group is trivial. □

14.3 Symplectic Deformation Ring Calculations

Let $n = 1$ or $n \geq 3$ be an integer, p be a prime and $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. We make the additional restrictions:

- If $n = 1$ then $q \neq 2, 3, 5$
- If $n \geq 2$ then $p > 2$ and $q \neq 3$.

Consider the symplectic deformation problem defined in Section 14.1. Main Theorem 14.2.1 again allows us to assume that $SP_{2n}(W_R)$ belongs to a lifting in the equivalence class of the universal deformation. We continue to show that the conclusion: ρ_A is the universal deformation ring for $\bar{\rho}$; follows easily from the argument in Chapter 10.

Step 1. Let (R, m_R) together with $\rho_R : \Gamma \to SP_{2n}(R)$ be the universal deformation ring for $\overline{\rho} : \Gamma \to SP_{2n}(k)$. Note that $\rho_R(\Gamma) \mod m_R = SP_{2n}(k)$. Therefore, we may invoke Theorem 14.2.1 and upon replacement of ρ_R with a strictly equivalent representation we may assume that $\rho_R(\Gamma)$ contains a copy of $SP_{2n}(W_R)$.

Step 2 and Step 3. Follow similarly to the proof of Main Theorem 2 in Section 10.1.

Bibliography

[1] J. Alperin and R. Bell. *Groups and Representations.* Graduate Texts in Mathematics, 162. Springer-Verlag, New York, 1995.

[2] G. Berhuy. *An Introduction to Galois Cohomology and its Applications.* London Mathematical Society Lecture Note Series, 377. Cambridge University Press, Cambridge, 2010.

[3] F. Bleher and T. Chinburg. Universal deformation rings need not be complete intersections. C. R. Math. Acad. Sci. Paris 342 (2006), 229-232.

[4] F. Bleher and T. Chinburg. Universal deformation rings need not be complete intersections. Math. Ann. 337 (2007), no. 4, 739767.

[5] F. Bleher, T. Chinburg, and B. De Smit. Deformation rings which are not local complete intersections, March 2010. `arXiv:1003.3143 [math.NT]`.

[6] F. Bleher, T. Chinburg, and B. De Smit. Inverse problems for deformation rings, April 2012. `arXiv:1012.1290v3 [math.NT]`. To appear in Trans. Amer. Math. Soc.

[7] G. Böckle. Presentations of Universal Deformations, February 2007.

[8] K. Brown. *Cohomology of groups.* Graduate Texts in Mathematics, 87. Springer-Verlag, New York-Berlin, 1982.

[9] T. Chinburg. Can deformations rings of group representations not be local complete intersections? In *Problems from the workshop on automorphisms of curves.* Edited by Gunther Cornelissen and Frans Oort, with contributions by I. Bouw, T. Chinburg, Cornelissen, C. Gasbarri, D. Glass, C. Lehr, M. Matignon, Oort, R. Pries and S. Wewers. Sem. Mat. Univ. Padova 113 (2005), 129-177.

[10] E. Cline, B. Parshall, and L. Scott. Cohomology of finite groups of Lie type, I. *Inst. Hautes Études Sci. Publ. Math.*, 45:169–191, 1975.

[11] K. Dorobisz. The Inverse Problem for Universal Deformation Rings and the Special Linear Group, December 2013. `arXiv: 1308.1346v2 [math.RT]`

[12] T. Eardley and J. Manoharmayum. The Inverse Deformation Problem, August 2013. `arXiv: 1307.8356v2 [math.RA]`.

[13] A. Hahn and O. O'Meara. *The Classical Groups and K-theory*, volume 291 of *Grundlehren der Mathematischen Wissenschaften* Springer-Verlag, Berlin Heidelberg, 1989.

[14] W. Jones. Cohomology of finite groups of Lie type. Doctoral Thesis, University of Minnesota, 1975.

[15] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin Heidelberg New York, revised third edition, 2005.

[16] J. Manoharmayum. A structure theorem for subgroups of GL_n over complete local noetherian rings with large residual image, April 2013. `arXiv:1304.1196v1 [math.RA]`. To appear in Proc. Amer. Math. Soc.

[17] I. Martin Isaacs. Character Theory of Finite Groups, volume 69 of *Pure and applied mathematics a series of monographs and textbooks*. Academic Press Inc, London, 1976.

[18] B. Mazur. Deforming Galois representations. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 385–437. Springer, New York, 1989.

[19] B. Mazur. Deformation theory of Galois representations. In *Modular Forms and Galois Representations*. Eds G. Cornell, J. H. Silverman, G. Stevens. Springer, New York, 1997.

[20] J. Milnor. *Introduction to Algebraic K-theory*, volume 72 of *Annals of Mathematics Studies*. Princeton University Press, 1971.

[21] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[22] O. O'Meara. *Symplectic Groups*, volume 16 of *Mathematical Surveys*. American Mathematical Society, Rhode Island, 1978.

[23] D. Quillen. On the cohomology and K-theory of the general linear groups over a finite field. *Ann. of Math.*, 96(3):552–586, 1972.

[24] R. Rainone. On the inverse problem for deformation rings of representations. Master's Thesis, Universiteit Leiden, Thesis Advisor: Bart de Smit, June 2010.

[25] L. Ribes and P. Zalesskii. *Profinite Groups*, volume 40 of *A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin Heidelberg, 2000.

[26] J. Rosenberg *Algebraic K -theory and its applications.* Graduate Texts in Mathematics, 147. Springer-Verlag, New York, 1994.

[27] C-H. Sah. Cohomology of split group extensions. *J. Algebra*, 29(2):255–302, 1974.

[28] C-H. Sah. Cohomology of split group extensions, II. *J. Algebra*, 45(1):17–68, 1977.

[29] M. Schlessinger. Functors on Artin Rings. *Trans AMS 130*:208-222, 1968.

[30] J.-P. Serre. *Local Fields,* Graduate Texts in Mathematics, 67. Springer-Verlag, New York, 1979.

[31] V. Srinivas. *Algebraic K Theory.* Reprint of the 1996 second edition. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2008.

[32] R.Wilson et al. Atlas of finite groups,
http://brauer.maths.qmul.ac.uk/Atlas/v3/matrep/2A8G1-Z4r4aB0.