A STRUCTURE THEOREM FOR SUBGROUPS OF $GL_n$ OVER COMPLETE LOCAL NOETHERIAN RINGS WITH LARGE RESIDUAL IMAGE

JAYANTA MANOHARMAYUM

Abstract. Given a complete local Noetherian ring $(A, m_A)$ with finite residue field and a subfield $k$ of $A/m_A$, we show that every closed subgroup $G$ of $GL_n(A)$ such that $G \mod m_A \supseteq SL_n(k)$ contains a conjugate of $SL_n(W(k)_A)$ under some small restrictions on $k$. Here $W(k)_A$ is the closed subring of $A$ generated by the Teichmüller lifts of elements of the subfield $k$.

1. Introduction

Let $k$ be a finite field of characteristic $p$ and let $W(k)$ be its Witt ring. Then, by the structure theorem for complete local rings (see Theorem 29.2 of [4]), every complete local ring with a residue field containing $k$ is naturally a $W$-algebra. More precisely, given a complete local ring $(A, m_A)$ with maximal ideal $m_A$ and a field homomorphism $\phi: k \to A/m_A$, there is a unique homomorphism $\phi: W(k) \to A$ of local rings which induces $\phi$ on residue fields. The homomorphism $\phi$ is completely determined by its action on Teichmüller lifts: if $x \in k$ and $\hat{x} \in W(k)$ is its Teichmüller, then $\phi(\hat{x})$ is the Teichmüller lift of $\phi(x)$.

In this article, we consider an analogous property for subgroups of $GL_n$ over complete local Noetherian rings. From here on, the index $n$ is fixed and assumed to be at least 2. First, a small bit of notation before we state our result formally: Given a complete local ring $(A, m_A)$ and a finite subfield $k$ of the residue field $A/m_A$, denote by $W(k)_A$ the image of the natural local homomorphism $W(k) \to A$ from the structure theorem. Alternatively, $W(k)_A$ is the smallest closed subring of $A$ containing the Teichmüller lifts of $k$.

Main Theorem. Let $(A, m_A)$ be a complete local Noetherian ring with maximal ideal $m_A$ and finite residue field $A/m_A$ of characteristic $p$. Suppose we are given a subfield $k$ of $A/m_A$ and a closed subgroup $G$ of $GL_n(A)$. Assume that:

- The cardinality of $k$ is at least 4. Furthermore, assume that $k \neq \mathbb{F}_5$ if $n = 2$ and that $k \neq \mathbb{F}_4$ if $n = 3$.
- $G \mod m_A \supseteq SL_n(k)$.

Then $G$ contains a conjugate of $SL_n(W(k)_A)$.

For an application, set $W_m := W(k)/p^m$ and $G := SL_n(W_m)$ with $k$ as in the above theorem. Then the above result implies that $W_m$, with the natural representation $\rho: G \to SL_n(W_m)$, is the universal deformation ring for deformations of...
\( \bar{p} := \rho \mod p : G \to SL_n(k) \) in the category of complete local Noetherian rings with residue field \( k \). (See Remark 1.5.)

We now outline the structure of this article (and introduce some notation along the way). If \( M \) is a module over a commutative ring \( A \), then \( \mathbb{M}(M) \), resp. \( \mathbb{M}_0(M) \), denotes the \( GL_n(A) \)-module of \( n \) by \( n \) matrices over \( M \), resp. \( n \) by \( n \) trace 0 matrices over \( M \), with \( GL_n(A) \) action given by conjugation. The bi-module structure on \( M \) is of course given by \( amb := abm \) for all \( a, b \in A, m \in M \). A typical application of this consideration is when \( B = A/J \) for some ideal \( J \) with \( J^2 = 0 \). Then \( GL_n(B) \) acts on \( \mathbb{M}(J) \) and \( \mathbb{M}_0(J) \), and this action is compatible with the action of \( GL_n(A) \).

Given \( A, B \) and \( J \) as above, we can understand subgroups of \( SL_n(A) \) if we know enough about extensions of \( SL_n(B) \) by \( \mathbb{M}_0(J) \). We give a brief description of the process involved (in terms of group extensions) in section 2. Determining extensions in general can be a complicated problem but, for the proof of the main theorem, we only need to look at extensions of \( SL_n(W(k)/p^m) \) by \( \mathbb{M}_0(k) \). To carry out the argument we need some control over \( H^1(SL_n(W(k)/p^m), \mathbb{M}_0(k)) \) and \( H^2(SL_n(W(k)/p^m), \mathbb{M}_0(k)) \). Some care is needed when \( p \) divides \( n \); the necessary calculations are carried out in section 3.

We remark that the condition on the residual image of \( G \) is necessary for the calculations used here to work. There are results due to Pink (see [9]) characterising closed subgroups of \( SL_2(A) \) when the complete local ring \( A \) has odd residue characteristic. (The proof depends on matrix/Lie algebra identities that only work when \( n = 2 \).) For explicit descriptions of some classes of subgroups of \( SL_2(A) \), see Böckle [1].

A different aspect of the size of closed subgroups of \( GL_n(A) \) with large residual image is studied by Boston in [7]. In a sense our result complements that of Boston: we give a lower bound for the size of closed subgroups assuming the image modulo \( m_A \) is big enough, while Boston’s result there, loc. cit, says such subgroups will contain \( SL_n(A) \) if the image modulo \( m_A^2 \) is big enough.

2. Twisted semi-direct products

Let \( G \) be a finite group. Given an \( \mathbb{F}_p[G] \)-module \( V \) and a normalised 2-cocycle \( x : G \times G \to V \), we can then form the twisted semi-direct product \( V \rtimes_x G \). Here, normalised means that \( x(g, e) = x(e, g) = 0 \) for all \( g \in G \) where we have denoted the identity of \( G \) by \( e \). Recall \( V \rtimes_x G \) has elements \( (v, g) \) with \( v \in V, g \in G \) and composition

\[
(v_1, g_1)(v_2, g_2) := (x(g_1, g_2) + v_1 + g_1v_2, g_1g_2),
\]

and that the cohomology class of \( x \) in \( H^2(G, V) \) represents the extension

\[
0 \to V \xrightarrow{(v, e)} V \rtimes_x G \xrightarrow{(v, g) \mapsto g} G \to 1.
\]

The conjugation action of \( V \rtimes_x G \) on \( V \) is the one given by the \( G \) action on \( V \), i.e.,

\[
(u, g)v := (u, g)(v, e)(u, g)^{-1} = (gv, e)
\]

holds for all \( u, v \in V, g \in G \).

We record the following result for use in the next section.

**Proposition 2.1.** With \( G, V \) and \( x : G \times G \to V \) as above, let \( \phi : V \rtimes_x e \to V \) be the map \( (v, e) \mapsto -v \). Then under the transgression map,

\[
\delta : Hom_G(V \rtimes_x e, V) = H^1(V \rtimes_x e, V)^G \to H^2(G, V),
\]

\( \delta(\phi) \) is the class of \( x \).
Proof. Let \( \pi : V \times_x G \to V \) be the map given by \( \pi(v, g) := -v \). Thus \( \pi|_{V \times_x e} = \phi \) and \( \pi(ab) = \pi(a) + a\pi(b)a^{-1} \) whenever \( a, b \) is in \( V \times_x e \). The map \( \partial \pi : G \times G \to V \) given by 
\[
\partial \pi(g_1, g_2) := \pi(a_1) + a_1\pi(a_2)a_1^{-1} - \pi(a_1a_2)
\]
where \( a_1, a_2 \in V \times_x G \) lifts \( g_i \) is then well defined and \( \delta(\phi) \) is the class of \( \partial \pi \). (See Proposition 1.6.5 in \([8]\).) Taking \( a_i := (0, g_i) \) we see that \( \partial \pi(g_1, g_2) = x(g_1, g_2) \). \( \square \)

For the remainder of this section, we assume that we are given an \( \mathbb{F}_p[G] \)-module \( M \) of finite cardinality and an \( \mathbb{F}_p[G] \)-submodule \( N \subseteq M \) such that the map

\[
H^2(G, N) \to H^2(G, M)
\]
is injective, and fix a normalised 2-cocycle \( x : G \times G \to N \). As we shall see, assumption 2.2 pretty much determines \( N \times_x G \) as a subgroup of \( M \times_x G \) up to conjugacy.

Suppose we are given a subgroup \( H \) of \( M \times_x G \) extending \( G \) by \( N \), i.e., the sequence

\[
0 \longrightarrow N \longrightarrow H \xrightarrow{(m,g)\mapsto g} G \longrightarrow e
\]
is exact. By assumption 2.2, the extension \( 2.3 \) must correspond to \( x \) in \( H^2(G, N) \). Hence there is an isomomorphism \( \theta : N \times_x G \to H \) such that the diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & N \\
\downarrow & & \downarrow \theta \\
0 & \longrightarrow & N \times_x G & \longrightarrow & G & \longrightarrow & e
\end{array}
\]
commutes, and this allows us to define a map \( \xi : G \to M \) so that the relation \( \theta(0, g) = (\xi(g), g) \) holds for all \( g \in G \).

**Proposition 2.2.** With notation and assumptions as above, we have:

(i) \( \theta(n, g) = (n + \xi(g), g) \) for all \( n \in N, \ g \in G \).

(ii) The map \( \xi : G \to M \) is a 1-cocycle.

(iii) If \( H^1(G, M) = 0 \), then \( \theta \) is conjugation by \((m, e)\) for some \( m \in M \).

Proof. (i) This is a simple computation using the relation \( (n, g) = (n, e)(0, g) \).

(ii) Let \( g_1, g_2 \in G \). Using part (i), we get

\[
\theta((0, g_1)(0, g_2)) = \theta(x(g_1, g_2), g_1g_2) = (x(g_1, g_2) + \xi(g_1g_2), g_1g_2), \quad \text{and}
\]
\[
\theta((0, g_1)(0, g_2)) = (\xi(g_1), g_1)(\xi(g_2), g_2) = (x(g_1, g_2) + \xi(g_1) + g_1\xi(g_2), g_1g_2).
\]

Therefore we must have \( \xi(g_1g_2) = \xi(g_1) + g_1\xi(g_2) \).

(iii) If \( H^1(G, M) = 0 \), then there exists an \( m \in M \) such that \( \xi(g) = gm - m \) for all \( g \in G \). One then uses part (i) to check that

\[
(m, e)^{-1}(n, g)(m, e) = (n + gm - m, g) = \theta(n, g).
\]

We now give—with a view to motivating the calculations in the next section—a sketch of how we use the above proposition to prove a particular case of the main theorem. Suppose that we have an Artinian local ring \((A, m_A)\) with residue field \( k \), and suppose that we are given a subgroup \( G \leq SL_n(A) \) with \( \text{mod } m_A = SL_n(k) \). We’d like to know if a conjugate of \( G \) contains \( SL_n(W(k)_A) \).

Suppose that \( J \) is an ideal of \( A \) killed by \( m_A \). To simplify the discussion further, let’s assume that the quotient \( A/J \) is \( W_m := W(k)/p^m \), that \( W(k)_A = W(k)/p^{m+1} \), and that \( \text{mod } J = SL_n(W_m) \). The assumption that \( W(k)_A = W(k)/p^{m+1} \) gives us a choice \( k \subseteq J \), and we can set up an identification of
$SL_n(A)$ with a twisted semi-direct product $M_0(J) \rtimes_x SL_n(W_m)$ so that the subgroup $SL_n(W(k)_A)$ gets identified with $M_0(k) \rtimes_x SL_n(W_m)$. In order to apply Proposition 2.2 and conclude that $G$ is, up to conjugation, $M \rtimes_x SL_n(W_m)$ for some $F_p[SL_n(W_m)]$-submodule $M$ of $M_0(J)$, we need to verify that

- Assumption 2.2 holds for $F_p[SL_n(W_m)]$-submodules of $M_0(J)$ (Theorem 3.1);
- $H^1(SL_n(W_m), M_0(J)) = (0)$. This is a consequence of known results when $m = 1$ (Theorem 3.2 and Proposition 3.6) in “good” cases. Extra arguments (cf, for instance, Proposition 3.8) are needed when $p$ divides $n$.

We can then conclude that a conjugate of $G$ contains $SL_n(W(k)_A)$ provided $M_0(k) \subset M$. This is derived from the injectivity of $H^2$ (in particular Corollary 3.13; see claim 4.3 in section 4.

3. COHOMOLOGY OF $SL_n(W/p^m)$

We fix, as usual, a finite field $k$ of characteristic $p$ and set $W_m := W/p^m$ where $W := W(k)$ is the Witt ring of $k$. From here on we assume $n \geq 2$. Our aim is to verify that assumption 2.2 holds. More precisely, we have the following:

**Theorem 3.1.** Let $k$ be a finite field of characteristic $p$ and cardinality at least 4. Suppose $N \subseteq M$ are $F_p[SL_n(W_m)]$-submodules of $M_0(k)^r$ for some integer $r \geq 1$. Then the induced map on second cohomology $H^2(SL_n(W_m), N) \rightarrow H^2(SL_n(W_m), M)$ is injective.

The proof of Theorem 3.1 relies on knowledge of the first cohomology of $SL_n(W_m)$ with coefficients in $M_0(k)$. There are a couple more $SL_n(W_m)$ modules to consider when $p$ divides $n$, and we introduce these: Write $S$ for the subspace of scalar matrices in $M_0(k)$. Thus $S = (0)$ unless $p$ divides $n$ in which case $S = \{\lambda I : \lambda \in k\}$. If $p | n$ we define $V := M_0(k)/S$.

The first cohomology of $SL_n(W_m)$ with coefficients in $M_0(k)$ or $V$ is well understood when $m = 1$, and we refer to Cline, Parshall and Scott [3, Table 4.5] for the following result. (For results on $H^2(SL_n(k), M_0(k))$ see [2, 14].)

**Theorem 3.2.** Assume that the cardinality of $k$ is at least 4.

- Suppose $(n, p) = 1$. Then $H^1(SL_n(k), M_0(k))$ is always 0 except for $H^1(SL_2(F_5), M_0(k))$ which is a 1-dimensional $k$-vector space.
- Suppose $p | n$. Then $H^1(SL_n(k), V)$ is a 1-dimensional $k$-vector space.

Throughout this section, we will denote by $\Gamma$ the kernel of the mod $p^m$-reduction map $SL_n(W_{m+1}) \rightarrow SL_n(W_m)$. We have suppressed the dependence on $m$ in our notation; this shouldn’t create any great inconvenience. If $M \in M_0(W)$ is a trace 0, $n \times n$-matrix with coefficients in $W$, then $I + p^{m+1}M \mod p^{m+1}$ is in $\Gamma$, and this sets up a natural identification of $M_0(k)$ and $\Gamma$ compatible with $SL_n(W_m)$-action. The extension of Theorem 3.2 to the group $SL_n(W_m)$ for arbitrary $m$, carried out in subsections 3.2 and 3.3, then relies on the injectivity of transgression maps from $H^1(\Gamma, -)^{SL_n(W_m)}$ to $H^2(SL_n(W_m), -)$.

We end—before we go into the main computations of this section—by reviewing the structure of $M_0(k)$, and therefore of $\Gamma$, as an $F_p[SL_n(k)]$-module. For $1 \leq i, j \leq n$, $e_{ij}$ denotes the matrix unit which is 0 at all places except at the $(i, j)$-th place where it is 1.
Lemma 3.3. Assume that $k \neq \mathbb{F}_2$ if $n = 2$.

(i) If $X$ is an $F_p[SL_n(k)]$-submodule of $M_0(k)$, then either $X$ is a subspace of $S$, or $X = M_0(k)$. Thus $M_0(k)/S$ is a simple $F_p[SL_n(k)]$-module, and the sequence

$$0 \to S \to M_0(k) \to V \to 0$$

is non-split when $p|n$.

(ii) If $\phi : M_0(k) \to M_0(k)$ is a homomorphism of $F_p[SL_n(k)]$-modules, then there exists a $\lambda \in k$ such that $\phi(A) = \lambda A$ for all $A \in M_0(k)$.

(iii) Suppose $p|n$ and $\phi : M_0(k) \to V$ is a homomorphism of $F_p[SL_n(k)]$-modules. Then $\phi(S) = (0)$ and the induced map $\phi : V \to V$ is multiplication by a scalar in $k$.

Proof. Let $U$ be the subgroup $SL_n(k)$ consisting of upper triangular matrices with ones on the diagonal. As an $F_p[U]$-module the semi-simplification of $M_0(k)$ is a direct sum of copies of $F_p$ and $M_0(k)^U = S + ke_{1n}$. Therefore if the $F_p[SL_n(k)]$-submodule $X$ is not a subspace of $S$, then $X$ contains a matrix $aI + be_{1n}$ with $b \neq 0$.

Suppose first that $a = 0$. By considering the action of diagonal matrices, we see that $X$ must in fact contain the full $k$-span of $e_{1n}$. Conjugation by $SL_n(k)$ then implies that $X \supseteq ke_{ij}$ whenever $i \neq j$. Now, under the action of $SL_n(k)$, we can conjugate $e_{ij} + e_{ji}$ with $i \neq j$ to $e_{ii} - e_{jj}$ when $p$ is odd and to $e_{ii} - e_{jj} + e_{ij}$ when $p = 2$. In any case, we can conclude that $X \supseteq k(e_{ii} - e_{jj})$ whenever $i \neq j$. It follows that $X$ must be the whole space $M_0(k)$.

Suppose now $a \neq 0$. Thus $S \neq 0$ and $p$ divides $n$. When $n \geq 3$ the relation

$$(I + e_{21})(aI + be_{1n})(I - e_{21}) = aI + be_{1n} + be_{2n}$$

implies $be_{2n}$ and, consequently, $be_{1n}$ are in $X$, and so $X = M_0(k)$. When $n = 2$—so $p = 2$ and $k$ has at least 4 elements—we can find a $0 \neq \lambda \in k$ with $\lambda^2 \neq 1$. Conjugating by $F_p[SL_n(k)]$, we see that $aI + b\lambda^2 e_{1n} \in X$. This gives $0 \neq b(\lambda^2 - 1)e_{1n} \in X$ and so $X = M_0(k)$.

Now for part (ii). Since $\phi$ commutes with the action of $SL_n(k)$, the subspaces $M_0(k)^{SL_n(k)}$ and $M_0(k)^U$ are invariant under $\phi$. When $p$ divides $n$ the first of these gives $\phi S \subseteq S$; if $p$ does not divide $n$, then $M_0(k)^U = ke_{1n}$ and so we must have $\phi(e_{1n}) = \lambda e_{1n}$ for some $\lambda \in k$. In any case, we can find a $\lambda \in k$ such that the $F_p[SL_n(k)]$-module homomorphism $\phi - [\lambda] : M_0(k) \to M_0(k)$ given by $A \to \phi(A) - \lambda A$ has non-trivial kernel. We can then conclude, by part (i) and a simple dimension count, that the kernel has to be the whole space $M_0(k)$, and therefore $\phi$ must be multiplication by $\lambda$.

For part (iii), that $S \subseteq \ker \phi$ follows from part (i). The second part is proved along the same lines as the proof of part (ii) by considering $\phi(e_{1n})$. $\square$

3.1. **Determination of $H^1(SL_n(W_m), k)$**. Let $k$ have cardinality $p^d$. Our aim is to show that $H^1(SL_n(W_m), k)$ vanishes, subject to some mild restrictions on $k$. We do this inductively using inflation–restriction after dealing with the base case $m = 1$ by adapting Quillen’s result in the general linear group case (see section 11 of [10]).

To start off we impose no restrictions other than $n \geq 2$. Denote by $T$ the subgroup of diagonal matrices in $SL_n(k)$ and write $(t_1, t_\ldots, t_n)$ for the diagonal
matrix with \((i, i)\)-th entry \(t_i\). The image of the homomorphism \(T \to (k^\times)^{n-1}\) given by
\[
(t_1, \ldots, t_n) \mapsto (t_2/t_1, \ldots, t_n/t_{n-1})
\]
has index \(h := \text{hcf}(n, p^d - 1)\) in \((k^\times)^{n-1}\). Taking this into account and following the remark at the end of section 11 of [10], the proof covering the general linear group case only needs a small modification at one place\(^1\) to give the following:

**Theorem 3.4.** Let \(k\) be a finite field of characteristic \(p\) and cardinality \(p^d\). Then \(H^i(SL_n(k), \mathbb{F}_p) = 0\) for \(0 < i < d(p - 1)/h\) where \(h := \text{hcf}(n, p^d - 1)\).

For a fixed \(n\), Theorem 3.4 implies the vanishing of \(H^1(SL_n(k), k)\) and \(H^2(SL_n(k), k)\) for fields with sufficiently large cardinality. To get a stronger result for \(H^1\) and \(H^2\) covering fields with small cardinality, we will need to carry out a slightly more detailed analysis.

In order to show \(H^*(SL_n(k), \mathbb{F}_p) = 0\) it is enough to check that \(H^*(U, \mathbb{F}_p)^T = 0\) where \(U\) is the subgroup of upper triangular matrices with ones on the diagonal. Fix an algebraic closure \(\overline{\mathbb{F}}_p\) of \(\mathbb{F}_p\) containing \(k\). Since \(T\) is an abelian group of order prime to \(p\), the \(\overline{\mathbb{F}}_p[T]\)-module \(H^*(U, \mathbb{F}_p) \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p\) is isomorphic to a direct sum of characters; we will then have to check that none of these can be the trivial character.

Let \(\Delta^+\) be the set of characters \(a_{ij} : T \to k^\times\) given by \(a_{ij}(t_1, \ldots, t_n) := t_i/t_j\) where \(1 \leq i < j \leq n\). The analysis in [10] section 11 shows that the Poincaré series of \(H^*(U)\) as a representation of \(T\), denoted by \(P.S.(H^*(U))\), satisfies the bound

\[
P.S.(H^*(U)) := \sum_{i \geq 0} \text{cl}(H^i(U, \mathbb{F}_p) \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p)z^i \ll \prod_{a \in \Delta^+} \prod_{b=0}^{d-1} \frac{1 + a^{-p^b}z}{1 - a^{-p^b}z^2}
\]
in \(R_{\overline{\mathbb{F}}_p}(T)[[z]]\). Here \(R_{\overline{\mathbb{F}}_p}(T)\) is the Grothendieck group for representations of \(T\) over \(\overline{\mathbb{F}}_p\), and \(\text{cl}(V)\) is the class of a \(\overline{\mathbb{F}}_p[T]\)-module \(V\) in \(R_{\overline{\mathbb{F}}_p}(T)\); given \(\overline{\mathbb{F}}_p[T]\)-modules \(V_0, V_1, V_2, \ldots\) and \(W_0, W_1, W_2, \ldots\), the bound

\[
\sum_{i \geq 0} \text{cl}(W_i)z^i \ll \sum_{i \geq 0} \text{cl}(V_i)z^i
\]
in \(R_{\overline{\mathbb{F}}_p}(T)[[z]]\) expresses the property that \(W_i\) is isomorphic to an \(\overline{\mathbb{F}}_p[T]\)-submodule of \(V_i\) for every integer \(i \geq 0\). Thus the right hand side of (3.2) tells us which characters might occur in the decomposition of the \(\overline{\mathbb{F}}_p[T]\)-module \(H^*(U, \mathbb{F}_p) \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p\).

Note that our choice of a positive root system \(\Delta^+\) is different from the one in [10]; the choice made there leads to a sign discrepancy in the upper bound (3.2) (but doesn’t affect any of the results derived from it). If we use the ordering on \(\Delta^+\) given by \((i', j') \leq (i, j)\) if either \(i' < i\), or \(i' = i\) and \(j \leq j'\), then with notation as in [10] we have a central extension

\[
0 \to k_a \to U/U_a \to U/U_a' \to 1,
\]
with \(T\)-action and the argument in [10] carries through verbatim.

---

\(^1\) The congruence just before Lemma 16 changes to a congruence modulo \((p^d - 1)/h\).
It is then straightforward to work out the coefficients of \( z \) and \( z^2 \) on the right hand side of (3.2) and we can conclude the following: If \( \chi : T \to \mathbb{F}_p^\times \) is a character occurring in \( \text{cl}(H^1(U, \mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_p), i = 1, 2 \), then \( \chi^{-1} \) is either

- a Galois conjugate of a positive root, i.e., \( \chi^{-1} = a^{p^b} \) for some positive root \( a \in \Delta \) and integer \( 0 \leq b < d \), or
- a product \( \alpha \alpha' \) where \( \alpha, \alpha' \) are Galois conjugates of positive roots and \( \alpha \neq \alpha' \). (This case happens only when \( i = 2 \).)

Thus, taking Galois conjugates as needed, we need to determine when \( a_{ij} \) or \( a_{ij}p_{kl}^{pb} \) is the trivial character, where \( a_{ij}, a_{kl} \in \Delta^+ \) and \( 0 < b < d \) in the case \((i, j) = (k, l)\). The first case is immediate: \( a_{ij} \) is never the trivial character except when \( k = \mathbb{F}_2 \), or \( n = 2 \) and \( k = \mathbb{F}_3 \).

Now for the second case. We now have integers \( 1 \leq i < j \leq n \), \( 1 \leq k < l \leq n \), \( 0 \leq b < d \) with \( b \neq 0 \) if \((i, j) = (k, l)\) such that the following relation holds:

\[
(3.3) \quad \frac{t_i}{t_j} (\frac{t_k}{t_l})^{p^b} = 1 \quad \text{for all } (t_1, \ldots, t_n) \in T.
\]

We will determine for which fields the above relation holds by specialising suitably. We exclude \( k = \mathbb{F}_2 \) in what follows.

Firstly, let’s consider the case when \( i, j, k, l \) are distinct. Thus \( n \geq 4 \). We can specialise (3.3) to \( t_k = t_l = 1 \) and \( t_i = t_j^{-1} = t \) for \( t \in k^\times \). We then get \( t^2 = 1 \) for all \( t \in k^\times \)—which implies \( k \) can only be \( \mathbb{F}_3 \). Furthermore, if \( n \geq 5 \) we have an even better specialisation: we can choose \( t_j = t_k = t_l = 1 \) and \( t_i \) freely, and conclude (3.3) never holds.

Next, suppose the cardinality \( \{i, j, k, l\} \) is 3. If we suppose \( \{i, j, k, l\} = \{i, k, l\} \) (the case \( \{i, j, k, l\} = \{j, k, l\} \) is similar), then specialisation to \( t_j = t_k = t_l = t^{-1} \) and \( t_i = 2^3 \) implies that \( t^3 = 1 \) for all \( t \in k^\times \), i.e., \( k \) is a subfield of \( \mathbb{F}_4 \). If in addition \( n \geq 4 \) we can take \( t_k = t_l = 1 \) and then there is a free choice for either \( t_i \), so (3.3) cannot hold.

Finally consider the case when the cardinality of \( \{i, j, k, l\} \) is 2. We must then have \( i = k \), \( j = l \) and \( 1 \leq b < d \). Taking \( t_i = t_j^{-1} \), we get \( t^{2(1+p^b)} = 1 \) for all \( t \in k^\times \), and so \( 2(1+p^b) = p^d - 1 \). This only works when \( k = \mathbb{F}_9 \). Moreover, when \( n \geq 3 \), we can set \( t_j = 1 \) and then the relation (3.3) implies \( t^{p^b+1} = 1 \) for all \( t \in k^\times \). So \( p^b + 1 = p^d - 1 \) and \( k \) is necessarily \( \mathbb{F}_4 \). Therefore in the case \((i, j) = (k, l)\) the relation (3.3) holds only when \( n = 2 \) and \( k = \mathbb{F}_9 \).

We have thus proved the first part of the following:

**Theorem 3.5.** Let \( k \neq \mathbb{F}_2 \) be a finite field of characteristic \( p \) and let \( n \geq 2 \) be an integer. Further, assume that

- if \( n = 4 \), then \( k \) is not \( \mathbb{F}_3 \);
- if \( n = 3 \), then \( k \neq \mathbb{F}_4 \);
- if \( n = 2 \), then \( k \) is not \( \mathbb{F}_3 \) or \( \mathbb{F}_9 \).

Then \( H^1(SL_n(k), \mathbb{F}_p) \) and \( H^2(SL_n(k), \mathbb{F}_p) \) are both trivial. Furthermore, under the same assumptions on \( k \), we have \( H^1(SL_n(W_m), k) = (0) \) for all integers \( m \geq 1 \).
The second part is proved by induction using inflation-restriction and the vanishing of $H^1(SL_n(k), k)$ from the first part. With $\Gamma = \ker(SL_n(W_{m+1}) \to SL_n(W_m))$ we have

$$0 \to H^1(SL_n(W_m), k) \to H^1(SL_n(W_{m+1}), k) \to H^1(\Gamma, k)^{SL_n(W_m)}.$$ 

Now the natural identification of $\mathbb{M}_0(k)$ with $\Gamma$ compatible with $SL_n(W_m)$-actions sets up an isomorphism between $H^1(\Gamma, k)^{SL_n(W_m)}$ and $\text{Hom}_{\mathbb{F}_p}[SL_n(k)](\mathbb{M}_0(k), k)$. The latter vector space is easily seen to be $(0)$ by a dimension count using Lemma 3.3 and the theorem follows.

3.2. Determination of $H^1(SL_n(W_m), \mathbb{M}_0(k))$. The result here is that all cohomology classes come from $H^1(SL_n(k), \mathbb{M}_0(k))$. More precisely:

**Proposition 3.6.** Suppose that $k$ has cardinality at least 4 and that $k \neq \mathbb{F}_4$ when $n = 3$. The inflation map $H^1(SL_n(W_m), \mathbb{M}_0(k)) \to H^1(SL_n(W_{m+1}), \mathbb{M}_0(k))$ is then an isomorphism for all integers $m \geq 1$.

By the inflation–restriction exact sequence, the above proposition follows if we can show that the transgression map

$$\delta : H^1(\Gamma, \mathbb{M}_0(k))^{SL_n(W_m)} \to H^2(SL_n(W_m), \mathbb{M}_0(k))$$

is injective. Since $H^1(\Gamma, \mathbb{M}_0(k))^{SL_n(W_m)}$ has dimension 1 as a $k$-vector space by Lemma 3.3, we just need to check that $\delta$ is not the zero map.

Recall that we have a natural identification of $\Gamma$ with $\mathbb{M}_0(k)$ given by $\phi(I + p^m A) := A \mod p$. Hence by Proposition 2.1 we see that $\delta(-\phi)$ must be the class of the extension

$$I \to \Gamma \to SL_n(W_{m+1}) \to SL_n(W_m) \to I.$$ 

Therefore the required conclusion follows if the above extension is non-split, and we address this below.

**Proposition 3.7.** Assume that $k$ has cardinality at least 4 and that if $n = 3$, then $k \neq \mathbb{F}_4$. Then the extension

$$(3.4) \quad I \to \Gamma \to SL_n(W_{m+1}) \to SL_n(W_m) \to I$$

does not split for any integer $m \geq 1$.

**Proof.** This should be well known, but it is hard to find a reference in the form we need. We therefore sketch a proof for completeness. The case when $n = 2$ and $p \geq 5$ is discussed in [13]. For the non-splitting of the above sequence when $k = \mathbb{F}_p$ see [11]; for non-splitting in the $GL_n$ case see [12].

If $R$ is a commutative ring and $r \in R$, then we write $N(r)$ for the elementary nilpotent $n \times n$ matrix in $M(R)$ with zeroes in all places except at the $(1,2)$-th entry where it is $r$. Note that $N(r)^2 = 0$ and that

$$(I + N(r))^k = I + kN(r) = I + krN(1)$$

for every integer $k$.

Suppose there is a homomorphism $\theta : SL_n(W_m) \to SL_n(W_{m+1})$ which splits the above exact sequence [3.4]. We fix a section $s : W_m \to W_{m+1}$ that sends Teichmüller lifts to Teichmüller lifts. For instance, if we think in terms of Witt vectors of finite length then we can take $s$ to be the map $(a_1, \ldots, a_m) \to (a_1, \ldots, a_m, 0)$. Finally, take the map $A : W_m \to \mathbb{M}_0(k)$ so that the relation

$$\theta(I + N(x)) = (I + p^m A(x))(I + N(s(x)))$$
holds for all \( x \in W_m \) (and we have abused notation and identified \( p^mW_{m+1} \) with \( p^mk \)).

Now \( \theta(I + N(x)) \) has order dividing \( p^m \) in \( SL_n(W/p^{m+1}) \) for any \( x \in W_m \).

Writing \( N \) and \( A \) in lieu of \( N(s(x)) \) and \( A(x) \), we have

\[
(I + N)^k(I + p^m A)(I + N)^{-k} = I + p^m(A + kNA - kAN - k^2NAN)
\]

for any integer \( k \), and a small calculation yields

\[
\theta(I + N(x))p^m = (I + \alpha p^m(NA - AN) - \beta p^mNAN)(I + p^mN).
\]

where \( \alpha = p^m(p^m - 1)/2 \) and \( \beta = p^m(p^m - 1)(2p^m - 1)/6 \). Hence if either \( p \geq 5 \), or \( p \) divides 6 and \( m \geq 2 \), then \( \theta(I + N(1)) \) cannot have order \( p^m \)—a contradiction.

From here on \( p \) divides 6 and \( m = 1 \); so \( \theta : SL_n(k) \to SL_n(W/p^2) \) and \( s(x) = \hat{x} \).

Applying \( \theta \) to \( (I + N(x))(I + N(y)) = I + N(x + y) \) and multiplying by \( N(1) \) on the left and right then gives \( N(1)A(x)N(1) + N(1)A(y)N(1) = N(1)A(x + y)N(1) \), and therefore,

\[
a_{21}(x + y) = a_{21}(x) + a_{21}(y)
\]

for all \( x, y \in k \).

Suppose now \( p = 3 \). The expression \( 3.5 \) for \( \theta(I + N(x))^p \) then becomes

\[
I + pxN(1) + px^2N(1)A(x)N(1) = I.
\]

Comparing the (1, 2)-th entries on both sides we get \( x^2a_{21}(x) + x = 0 \) for all \( x \in k \). Thus for \( x \neq 0 \) we have \( a_{21}(x) = -x^{-1} \). This contradicts the linearity of \( a_{21} \) if \( k \neq \mathbb{F}_3 \).

Before we consider the case \( p = 2 \) specifically, we make some relevant simplifications by considering the action of \( \Gamma \), the subgroup of diagonal matrices in \( SL_n(k) \). For \( t = (t_1, \ldots, t_n) \in SL_n(k) \) we define \( \hat{t} := (\hat{t}_1, \ldots, \hat{t}_n) \in SL_n(W/p^2) \). We must then have \( \theta(t) = B(t)\hat{t} \) where \( B : \Gamma \to \Gamma \) is a 1-cocycle. Since \( H^1(\Gamma, \Gamma) = 0 \) we can assume, after conjugation by a matrix in \( \Gamma \) if necessary, that \( \theta(t) = \hat{t} \). The homomorphism condition applied to \( \theta(t(I + N(x))t^{-1}) \) then gives

\[
(I + pA(t_1x/t_2))(I + (t_1x/t_2)N(1)) = (I + ptA(x)t^{-1})(I + \hat{t}xN(1)\hat{t}^{-1})
\]

where \( t = (t_1, \ldots, t_n) \). Hence \( A(t_1x/t_2) = tA(x)t^{-1} \) for all \( t \in T \) and \( x \in k \). By considering specialisations \( t_1 = t_2 = 1 \) for \( n \geq 4 \) and \( t = (\lambda, \lambda, \lambda^{-2}) \) when \( n = 3 \), we conclude that \( a_{ij}(x) = 0 \) if \( i \neq j \) and \( i \geq 3 \) or \( j \geq 3 \) provided \( k \) has cardinality at least 4 and \( k \neq \mathbb{F}_4 \) when \( n = 3 \).

We now go back to assuming \( p = 2 \) and \( m = 1 \). Relation \( 3.5 \) then becomes

\[
I + px(N(1)A(x) + A(x)N(1)) + px^2N(1)A(x)N(1) + pxN(1) = I,
\]

and we get \( a_{21}(x) = 0 \) and \( a_{11}(x) + a_{22}(x) = 1 \) whenever \( x \neq 0 \). Hence if \( k \) has cardinality at least 4 and \( k \neq \mathbb{F}_4 \) when \( n = 3 \), then \( \theta(I + N(x)) \) is an upper-triangular matrix and so \( a_{ii}(x + y) = a_{ii}(x) + a_{ii}(y) \) for \( i = 1, \ldots, n \) and \( x, y \in k \).

Since \( k \) has at least 4 elements we can choose \( x, y \in k \) with \( xy(x+y) \neq 0 \), and this gives

\[
1 = a_{11}(x + y) + a_{22}(x + y) = (a_{11}(x) + a_{11}(y)) + (a_{22}(x) + a_{22}(y)) = 1 + 1
\]

—a contradiction.
3.3. $H^1$ when $n$ and $p$ are not coprime. Suppose now that $p$ divides $n$. Thus $\mathbb{M}_0(k)$ is reducible and we have the exact sequence

$$0 \to S \xrightarrow{i} \mathbb{M}_0(k) \xrightarrow{\pi} V \to 0.$$  

We then have the following analogue of Proposition 3.6.

**Proposition 3.8.** Assume that $p$ divides $n$ and that the cardinality of $k$ is at least 4. The inflation map $H^1(SL_n(W_m), V) \to H^1(SL_n(W_{m+1}), V)$ is then an isomorphism for all integers $m \geq 1$.

Denote by $Z$ the subgroup of $\Gamma$ consisting of the scalar matrices $(1+p^m\lambda)I$. We then have an exact sequence

$$I \to \Gamma/Z \to SL_n(W_{m+1})/Z \xrightarrow{\mod p^m} SL_n(W_m) \to I.$$  

Under the natural identification $\phi : \Gamma \to \mathbb{M}_0(k)$ given by $\phi(I+p^m A) := A \mod p$ of $\Gamma$ with $\mathbb{M}_0(k)$, the groups $Z$, resp. $\Gamma/Z$, correspond to $S$, resp. $V$. If we set $\psi : \Gamma/Z \to V$ to be the map induced by $\phi \mod S$, then Proposition 2.1 shows that $\delta = (\psi^*)^{-1}$ is the cohomology class of the extension 3.7 under the transgression map

$$\delta : H^1(\Gamma/Z, V)^{SL_n(W_m)} \to H^2(\Gamma, V)^{SL_n(W_m)}.$$  

Now, by Lemma 3.3, the map

$$H^1(\Gamma/Z, V)^{SL_n(W_m)} \to H^1(\Gamma, V)^{SL_n(W_m)}$$  

is an isomorphism of 1-dimensional $k$-vector spaces. Thus the conclusion of Proposition 3.8 holds exactly when the extension 3.7 is non-split.

In many cases the required non-splitting follows from a simple modification of the proof of Proposition 3.7. More precisely, we have the following:

**Lemma 3.9.** Suppose $p|n$, and assume that either $p \geq 5$ or $m \geq 2$. Then the extension

$$I \to \Gamma/Z \to SL_n(W_{m+1})/Z \to SL_n(W_m) \to I$$  

does not split.

**Proof.** We give a sketch: Suppose $\theta : SL_n(W_m) \to SL_n(W_{m+1})$ is a section. Then, with $N(1)$ the elementary nilpotent matrix described in the proof of Proposition 3.7 we have $\theta(I+N(1)) = (I+p^m A)(I+N(1))$ modulo $Z$ for some $A \in \mathbb{M}_0(k)$. Because elements in $Z$ are central, relation 3.5 holds modulo $Z$ and the lemma easily follows. \qed

We now deal with the case $m = 1$ and complete the proof of Proposition 3.8. Consider the commutative diagram

$$\begin{array}{cccccc}
H^1(\Gamma, \mathbb{M}_0(k))^{SL_n(W_m)} & \xrightarrow{\delta} & H^2(SL_n(W_m), \mathbb{M}_0(k)) \\
\downarrow \pi^* & & \downarrow \pi^* \\
H^1(\Gamma, V)^{SL_n(W_m)} & \xrightarrow{\delta} & H^2(SL_n(W_m), V)
\end{array}$$

where $\pi^*$ is the map induced by the projection $\pi : \mathbb{M}_0(k) \to V$. Now, the map $\pi^*$ on the left hand side of the square is an isomorphism by Lemma 3.3. Since the cardinality of $k$ is at least 4 (and remembering that we are also assuming $p|n$), the top row of the square 3.8 is an injection by Proposition 3.6. Furthermore, Theorem 4.5 implies $H^2(SL_n(W_m), k) = (0)$ and therefore the map $\pi^*$ on the right hand
side of the square is an injection. Hence the bottom row of the square \(3.8\) is also an injection and we can conclude the proposition.

\textbf{Remark 3.10.} As we saw in course of the proof, Proposition \(3.8\) implies the following extension of Lemma \(3.9\):

\textbf{Corollary 3.11.} Assume that \(p\) divides \(n\) and \(k\) has cardinality at least 4. Then the sequence

\[ I \to \Gamma/Z \to SL_n(W_{m+1})/Z \to SL_n(W_m) \to I \]

does not split for any integer \(m \geq 1\).

We end this subsection with a description of the relations between the cohomology groups with coefficients \(\mathbb{M}_0(k), S\) and \(V\):

\textbf{Proposition 3.12.} Suppose that \(p\) divides \(n\) and that \(k\) has at least 4 elements. Then, with \(i\) and \(\pi\) as in the exact sequence \(3.6\) the map \(H^1(SL_n(W_m), \mathbb{M}_0(k)) \xrightarrow{\pi^*} H^1(SL_n(W_m), V)\) is an isomorphism and

\[ 0 \to H^2(SL_n(W_m), S) \xrightarrow{i^*} H^2(SL_n(W_m), \mathbb{M}_0(k)) \xrightarrow{\pi^*} H^2(SL_n(W_m), V) \]

is exact.

\textbf{Proof.} The long exact sequence obtained from \(3.6\) shows that we just need to check \(H^1(SL_n(W_m), \mathbb{M}_0(k)) \xrightarrow{\pi^*} H^1(SL_n(W_m), V)\) is an isomorphism. This holds when \(m = 1\) because both \(H^1(SL_n(k), S)\) and \(H^2(SL_n(k), S)\) are 0 by Theorem \(3.5\). For general \(m\) we can use induction because in the commutative diagram

\[ \begin{array}{ccc}
H^1(SL_n(W_m), \mathbb{M}_0(k)) & \xrightarrow{\pi^*} & H^1(SL_n(W_m), V) \\
\downarrow & & \downarrow \\
H^1(SL_n(W_{m+1}), \mathbb{M}_0(k)) & \xrightarrow{\pi^*} & H^1(SL_n(W_{m+1}), V)
\end{array} \]

the vertical inflation maps are isomorphisms by Proposition \(3.6\) and Proposition \(3.8\). \(\square\)

\textbf{3.4. Proof of Theorem 3.1} Recall that we want to show the injectivity of \(H^2(SL_n(W_m), N) \to H^2(SL_n(W_m), M)\) whenever \(N \subseteq M\) are \(\mathbb{F}_p[SL_n(W_m)]\)-submodules of \(\mathbb{M}_0(k)r\) for some integer \(r \geq 1\).

We will write \(H^*(X)\) to mean \(H^*(SL_n(W_m), X)\). Note that it is enough to show that \(H^2(M) \to H^2(\mathbb{M}_0(k)r)\) is injective for all \(\mathbb{F}_p[SL_n(W_m)]\)-submodules \(M\) of \(\mathbb{M}_0(k)r\). If \((n, p) = 1\) then \(\mathbb{M}_0(k)r\) is semi-simple and the desired injectivity is immediate. So we will suppose \(p\) divides \(n\) from here on.

Consider the commutative diagram

\[ \begin{array}{ccccccc}
0 & \to & M \cap S^r & \xrightarrow{i} & M & \xrightarrow{\pi} & M/(M \cap S^r) & \to & 0 \\
0 & \to & S^r & \xrightarrow{i} & \mathbb{M}_0(k)r & \xrightarrow{\pi} & V^r & \to & 0
\end{array} \quad (3.9) \]
where the is are inclusions. Thus \( j \) is necessarily an injection. Taking cohomology and using Proposition 3.12, we get a commutative diagram

\[
\begin{array}{c}
H^2(M \cap S^r) \\
\downarrow i^* \\
H^2(S^r) \\
\downarrow j^*
\end{array} \quad \begin{array}{c}
H^2(M) \\
\downarrow i^* \\
H^2(M/(M \cap S^r)) \\
\downarrow j^*
\end{array}
\]

(3.10)

\[
0 \longrightarrow H^2(S^r) \longrightarrow H^2(M_0(k)^r) \longrightarrow H^2(V^r)
\]

in which the horizontal rows are exact. Now the maps \( H^2(M \cap S^r) \longrightarrow H^2(S^r) \) and \( H^2(M/(M \cap S^r)) \longrightarrow H^2(S^r) \) are injective since \( S^r \) and \( V^r \) are semi-simple and \( i, j \) are injections. A straightforward diagram chase then shows that \( i^* : H^2(M) \to H^2(M_0(k)^r) \) is an injection, and this completes the proof of Theorem 3.13. \( \square \)

As a consequence, we have the following:

**Corollary 3.13.** Let \( k \) be a finite field of characteristic \( p \) and cardinality at least 4, and let \( M, N \) be two \( \mathbb{F}_p[SL_n(W_m)] \)-submodules of \( M_0(k)^r \) for some integer \( r \geq 1 \). Suppose we are given \( x \in H^2(SL_n(W_m), M) \) and \( y \in H^2(SL_n(W_m), N) \) such that \( x \) and \( y \) represent the same cohomology class in \( H^2(SL_n(W_m), M_0(k)^r) \). Then there exists a \( z \in H^2(SL_n(W_m), M \cap N) \) such that \( x = z \), resp. \( y = z \), holds in \( H^2(SL_n(W_m), M) \), resp. \( H^2(SL_n(W_m), M) \).

**Proof.** Consider the exact sequence

\[
0 \to M \cap N \xrightarrow{m \mapsto m \oplus m} M \oplus N \xrightarrow{m \oplus n \mapsto m - n} M + N \to 0.
\]

By Theorem 3.13 we get a short exact sequence

\[
0 \to H^2(M \cap N) \to H^2(M) \oplus H^2(N) \to H^2(M + N).
\]

Since \( H^2(M + N) \to H^2(M_0(k)^r) \) is injective, it follows that \( x \oplus y \) is zero in \( H^2(M + N) \) and therefore must be in the image of \( H^2(M \cap N) \). \( \square \)

4. **Proof of the main theorem**

From here on, we assume that we are given finite fields \( k \subseteq k' \) of characteristic \( p \). Let \( C \) be the category of complete local Noetherian rings \( (A, m_A) \) with residue field \( A/m_A = k' \) and with morphisms required to be identity on \( k' \). We will abbreviate \( W(k) \) and \( W(k)_A \) for \( A \) an object in \( C \) to \( W \) and \( W_A \) respectively. Recall that \( W_A \) is the closed subring of \( A \) generated by the Teichmüller lifts of elements of \( k \); it is not an object in \( C \) unless \( k = k' \). Throughout this section we assume that the finite field \( k \) satisfies the hypothesis of the main theorem:

**Assumption 4.1.** The cardinality of \( k \) is at least 4. Furthermore, \( k \neq \mathbb{F}_5 \) if \( n = 2 \) and that \( k \neq \mathbb{F}_4 \) if \( n = 3 \).

Suppose we are given a local ring \( (A, m_A) \) in \( C \) and a closed subgroup \( G \) of \( GL_n(A) \) such that \( G \mod m_A \supseteq SL_n(k) \). We want to show that \( G \) contains a conjugate of \( SL_n(W_A) \). Now, without any loss of generality, we may assume that \( G \mod m_A = SL_n(k) \). The quotient \( G/(G \cap SL_n(A)) \) is then pro-\( p \). This implies that \( G \cap SL_n(A) \mod m_A \) is a normal subgroup of \( SL_n(k) \) with index a power of \( p \). Now \( PSL_n(k) \) is simple since the cardinality of \( k \) is at least 4. Consequently we must have \( G \cap SL_n(A) \mod m_A = SL_n(k) \). Along with the fact that \( A \) is the
inductive limit of Artinian quotients $A/m_A^n$, we see that the main theorem follows
from the following proposition:

**Proposition 4.2.** Let $\pi: (A, m_A) \to (B, m_B)$ be a surjection of Artinian local
rings in $C$ with $m_A \ker \pi = 0$, and let $H$ be a subgroup of $SL_n(A)$ such that $\pi H =
SL_n(W_B)$. Assume that $k$ satisfies assumption 4.1 Then we can find a $u \in GL_n(A)$ such that $\pi u = I$ and $uH u^{-1} \supseteq SL_n(W_A)$.

For the proof of the above proposition, let’s set $G := \pi^{-1}SL_n(W_B) \cap SL_n(A)$
where $\pi^{-1}SL_n(W_B)$ is the pre-image of $SL_n(W_B)$ under the map $\pi : GL_n(A) \to
GL_n(B)$. We then have an exact sequence

$$(4.1) \quad 0 \to M(\ker \pi) \to \pi^{-1}SL_n(W_B) \to SL_n(W_B) \to I$$

with $j(v) = I + v$ for $v \in M(\ker \pi)$, and this restricts to

$$(4.2) \quad 0 \to M_0(\ker \pi) \to G \to SL_n(W_B) \to I.$$

Note that $M(\ker \pi) \cong M(k) \otimes_k \ker \pi$ and $M_0(\ker \pi) \cong M_0(k) \otimes_k \ker \pi$
as $k[SL_n(W_B)]$-modules.

In what follows we will abbreviate $H^*(SL_n(W_B), M)$ to simply $H^*(M)$. For $X \subseteq SL_n(A)$, we set $M_0(X)$ to be the set of matrices $v \in M_0(\ker \pi)$ such that $j(v) \in X$. We then have the following:

**Claim 4.3.** $M_0(SL_n(W_A)) \subseteq M_0(H)$.

Let’s assume the above claim and carry on with the proof of Proposition 4.2.

Fix a section $s : SL_n(W_B) \to SL_n(W_A)$ that sends identity to identity and set $x : SL_n(W_B) \times SL_n(W_B) \to M_0(SL_n(W_A))$ to be the resulting 2-cocycle representing the extension

$$(4.3) \quad 0 \to M_0(SL_n(W_A)) \to SL_n(W_A) \to SL_n(W_B) \to I.$$

The section $s$ and cocyle $x$ thus set up an identification

$$\varphi : \pi^{-1}SL_n(W_B) \to M_0 \times_x SL_n(W_B),$$

and we have the following commutative diagram (cf. diagram 4.4)

$$0 \quad \longrightarrow \quad M_0(H) \quad \longrightarrow \quad M_0(H) \times_x SL_n(W_B) \quad \longrightarrow \quad SL_n(W_B) \quad \longrightarrow \quad I$$

and

$$0 \quad \longrightarrow \quad M_0(H) \quad \longrightarrow \quad \varphi H \quad \longrightarrow \quad SL_n(W_B) \quad \longrightarrow \quad I.$$

Suppose first that $(p, n) = 1$. Our assumptions on $k$ imply that we can combine
Theorem 3.2 and Proposition 3.6 to conclude that $H^1(M_0(k)) = (0)$. Consequently,
we get $H^1(M_0(\ker \pi)) = (0)$. Furthermore, $H^2(M_0(H)) \to H^2(M_0(\ker \pi))$ is an
injection by Theorem 3.1. Hence we can apply Proposition 2.2 and conclude that $M_0(H) \times_x SL_n(W_B) = \varphi u H u^{-1}$ for some $u \in G$ (cf. sequence 4.2) with $\pi(u) = I$.

Suppose now $p$ divides $n$. Since $H^1(k) = 0$ by Theorem 3.3 we get the following
the exact sequence

$$0 \to k \to H^1(M_0(k)) \to H^1(M(k)) \to 0 \to H^2(M_0(k)) \to H^2(M(k))$$

from $0 \to M_0(k) \to M(k) \to k \to 0$. Now since $\dim_k H^1(V) = 1$ by Theorem 3.2
and Proposition 3.8 we must also have $\dim_k H^1(M_0(k)) = 1$ by Proposition 3.12. Hence $H^1(M(k)) = 0$ and, consequently, $H^1(M(\ker \pi)) = 0$. Along with Theorem
The above exact sequence also shows that $H^2(M_0(H)) \to H^2(M(\ker \pi))$ is an injection. Hence $M_0(H) \times_x S L_n(W_B) = \varphi u H u^{-1}$ for some $u \in \pi^{-1} S L_n(W_B)$ (cf. sequence 4.11) with $\pi(u) = I$ by Proposition 22.12.

In any case, we have found a $u \in G L_n(A)$ with $\pi(u) = I$ and $\varphi u H u^{-1} = M_0(H) \times_x S L_n(W_B)$. Finally,

$$\varphi S L_n(W_A) = M_0(S L_n(W_A)) \times_x S L_n(W_B) \subseteq M_0(H) \times_x S L_n(W_B)$$

as $M_0(S L_n(W_A)) \subseteq M_0(H)$ by our claim 4.3 and the proposition follows.

We now establish the claim to complete the argument.

Proof of Claim 4.3 There is nothing to prove if $W_A \twoheadrightarrow W_B$ is an injection (as $M_0(S L_n(W_A))$ is then 0). Therefore we may suppose that we have a natural identification of $W_A \twoheadrightarrow W_B$ with $W_{m+1} \to W_m$ for some integer $m \geq 1$, and consequently an identification of $M_0(S L_n(W_A))$ with $M_0(k)$. We will freely use these identifications in what follows.

As in the proof of the proposition, let $x \in H^2(M_0(k))$ represent the extension 4.3 and let $y \in H^2(M_0(H))$ represent the extension

$$0 \to M_0(H) \xrightarrow{\cdot 2} H \to S L_n(W_B) \to I.$$ 

Then $x$ and $y$ represent the same cohomology class in $H^2(M_0(k) \cap M_0(H))$. By Corollary 3.13 there is a $z \in H^2(M_0(k) \cap M_0(H))$ such that $x$ and $z$ (resp. $y$ and $z$) represent the same cohomology class in $H^2(M_0(k))$ (resp. $H^2(M_0(H))$).

Suppose the claim $M_0(k) \subseteq M_0(H)$ is false. Then we must have $M_0(k) \cap M_0(H) \subseteq S$ by Lemma 3.3. Now, if $M_0(k) \cap M_0(H) = 0$ then $x$ will be zero, contradicting non-splitting of the extension 4.3.

Thus $M_0(k) \cap M_0(H)$ must be a non-zero submodule of $S$, and we must therefore have $p$ dividing $n$. Now the image of $x$ in $H^2(M_0(k)/S)$ represents the extension

$$0 \to M_0(k)/S \xrightarrow{\cdot 2} S L_n(W_{m+1})/Z \xrightarrow{\text{mod } p^m} S L_n(W_m) \to I.$$ 

Since this is non-split by Corollary 3.11 the image of $x$ in $H^2(V)$ is not 0. This contradicts the fact that $x$ is itself in the image of $H^2(S) \to H^2(M_0(k))$. □

Remark 4.4. It is well known that the mod-$p$ reduction map $S L_2(\mathbb{Z}/p^2 \mathbb{Z}) \to S L_2(\mathbb{Z}/p \mathbb{Z})$ has a homomorphic section when $p$ is 2 or 3. (See the exercises at the end of Chapter IV(3).) Thus the conclusion of the main theorem fails when $n = 2$ and $k$ is $\mathbb{F}_2$ or $\mathbb{F}_3$.

The main theorem also fails when $n = 2$ and $k = \mathbb{F}_5$. To see this, choose $0 \neq \xi \in H^1(S L_2(\mathbb{F}_5), M_0(\mathbb{F}_5))$ and consider the subgroup

$$G := \{(I + \epsilon \xi(A)) A \mid A \in S L_2(\mathbb{F}_5)\}$$

of $S L_2(\mathbb{F}_5[\epsilon])$ where $\mathbb{F}_5[\epsilon]$ is the ring of dual numbers (so $\epsilon^2 = 0$). Clearly, $G \mod \epsilon = S L_2(\mathbb{F}_5)$. If $G$ can be conjugated to $S L_2(\mathbb{F}_3)$ in $G L_2(\mathbb{F}_5[\epsilon])$, then the cocycle $\xi$ must vanish in $H^1(S L_2(\mathbb{F}_5), M(\mathbb{F}_5))$. This cannot happen as the sequence

$$0 \to M_0(\mathbb{F}_5) \to M(\mathbb{F}_5) \to \mathbb{F}_5 \to 0$$

splits. □

Remark 4.5. Fix a finite field $k$ satisfying assumption 4.11 and an integer $m \geq 1$. The main theorem then determines the universal deformation ring for $G := S L_n(W_m)$ with standard representation completely. (See [5, 6] for background on deformation of representations.)
To describe this fully, let $\rho: G \to SL_n(W_m)$ be the natural representation and set $\overline{\rho} := \rho \mod \rho$. We work inside the category of complete local Noetherian rings with residue field $k$ from here on. Let $R$ be the universal deformation ring for deformations of $(G, \overline{\rho})$ in this category and let $\rho_R: G \to GL_n(R)$ be the universal representation.

By universality, there is a morphism $\pi: R \to W_m$ such that $\pi \circ \rho_R$ is strictly equivalent to $\rho$. By our main theorem $X\rho_R(G)X^{-1} \supseteq SL_n(W_R)$ for some $X$ in $GL_n(R)$; here, we can insist that $X$ reduces to the identity modulo $m_R$. Now $\pi|_{W_R}: W_R \to W_m$ along with

$$|SL_n(W_m)| = |G| \geq |\rho_R(G)| \geq |SL_n(W_R)| \geq |SL_n(W_m)|$$

implies that $\pi|_{W_R}: W_R \to W_m$ is an isomorphism and that $X\rho_R(G)X^{-1} = SL_n(W_R)$. Replacing $\rho_R$ with the strictly equivalent representation $X\rho_RX^{-1}$ if necessary, we can then assume that $\rho_R: G \to GL_n(R)$ takes values in $SL_n(W_R)$. Writing $i: W_m \to W_R$ for the inverse to $\pi|_{W_R}$, we conclude that $i \circ \rho$ is strictly equivalent to $\rho_R$.

We will now verify that $\rho: G \to SL_n(W_m)$ is the universal deformation. So given a lifting $\rho_A: G \to GL_n(A)$ of $\overline{\rho}: G \to SL_n(k)$, we need to show that there is a unique morphism $i_A: W_m \to A$ such that $i \circ \rho$ is strictly equivalent to $\rho_A$. Uniqueness comes for free (it has to send 1 to 1). For existence, note that by universality there is a morphism $\pi_A: R \to A$ such that $\pi_A \circ \rho_R$ is strictly equivalent to $\rho_A$. It is then an easy check to see that $i_A := \pi_A \circ i$ works.

**Acknowledgements**

The author thanks the referee for bringing to attention the work of Boston in [7] and other helpful comments.

**References**


School of Mathematics and Statistics, University of Sheffield, Sheffield S3 7RH, United Kingdom

E-mail address: J.Manoharmayum@sheffield.ac.uk