FAITHFUL REPRESENTATIONS OF $SL_2$ OVER TRUNCATED WITT VECTORS

GEORGE J. MCNINCH

ABSTRACT. Let $\Gamma_2$ be the six dimensional linear algebraic $k$-group $SL_2(W_2)$, where $W_2$ is the ring of Witt vectors of length two over the algebraically closed field $k$ of characteristic $p > 2$. Then the minimal dimension of a faithful rational $k$-representation of $\Gamma_2$ is $p + 3$.

1. INTRODUCTION

Let $W = W(k)$ be the ring of Witt vectors over the algebraically closed field $k$ of characteristic $p > 0$. Let $W_n = W/p^nW$ be the ring of length $n$ Witt vectors. (See [Ser79, II.§6] for definitions and basic properties of Witt vectors, and see §3 below.) We regard $W_n$ as a “ring variety” over $k$, the underlying variety of which is $A^n_k$. If $n \geq 2$, the ring $W_n$ is not a $k$-algebra.

Let $\Gamma_n = SL_2(W_n)$ be the group of $2 \times 2$ matrices with entries in $W_n$ and with determinant 1. Then $\Gamma_n$ is a closed subvariety of the $4n$ dimensional affine space of $2 \times 2$ matrices over $W_n$; thus, it is an affine algebraic group over $k$. As such, it is a closed subgroup of $GL(V)$ for some finite dimensional $k$-vector space $V$, i.e. it has a faithful finite dimensional $k$-linear representation. Note that for $n \geq 2$, $W_n$ is not a vector space over $k$ in any natural way, so the natural action of $\Gamma_n$ on $W_n \oplus W_n$ is not a $k$-linear representation.

Let $H$ be any linear algebraic group over $k$. A rational $H$-module $(\rho, V)$ is said to be faithful if $\rho$ defines a closed embedding $H \to GL(V)$; this is equivalent to the condition: both $\rho$ and $d\rho$ are injective.

Theorem 1. If $(\rho, V)$ is a representation of $\Gamma_2$ with $\dim V \leq p + 2$, then $\rho(u^p) = 1_V$ for each unipotent element $u \in \Gamma_2$.

Theorem 2. If $p > 2$, the minimal dimension of a faithful rational representation of $\Gamma_2$ is $p + 3$.

With the same notation, if $p = 2$ then $\Gamma_2$ has a rational representation $(\rho, V)$ with $\dim V = p + 3 = 5$, and $\rho$ is abstractly faithful (i.e. injective on the closed points of $G$) but $\ker d\rho$ is the Lie algebra of a maximal torus of $\Gamma_2$.

After some preliminaries in §2 through §4, we construct in §5 a representation $(\rho, V)$ of $\Gamma_2$ of dimension $p + 3$ and show that $\rho$ is abstractly faithful; in §6 we show finally that $d\rho$ is injective when $p > 2$. Combined with Theorem 1 this proves Theorem 2.

In §7 we prove that the unipotent radical $R$ of $\Gamma_2$ acts trivially on any rational module with dimension $\leq p + 2$; this completes the verification of Theorem 2.
important tool in the proof is a result obtained in [1] concerning the weight spaces of a representation of the group $W_2 \rtimes k^\times$; this result is proved with the help of the algebra of distributions of the unipotent group $W_2$.

Finally, in [2], we prove the analogue of Theorem [2] for the finite groups $\Gamma_2(F_q)$ provided that $p > 2$ and $q \geq p^2$. In its outline, the proof is the same as in the algebraic case. In the finite case, we replaced the arguments concerning the algebra of distributions of $W_2$ in [2] with some more elementary arguments (see Proposition [3]). In fact, we could use these more elementary arguments in the “algebraic” case, but the techniques in [2] give more information and are therefore perhaps of independent interest. Note that the condition on $q$ is an artifact of the proof; I do not know if $\Gamma_2(F_p) = SL_2(Z/p^2Z)$ has a faithful $k$-representation of dimension $< p + 3$.

Thanks to Jens Carsten Jantzen and Jean-Pierre Serre for some helpful comments on this manuscript.

2. A NEGATIVE APPLICATION: UNIPOTENT ELEMENTS IN REDUCTIVE GROUPS.

Let $H$ be a connected reductive group over $k$, and let $u \in H$ be unipotent of order $p$. If $p$ is a good prime for $H$, there is a homomorphism $SL_2(k) \to H$ with $u$ in its image. This was proved by Testerman [Test95]; see also [McNb].

Now suppose that $u$ is a unipotent element in $H$ with order $p^n$, $n \geq 1$. Then there is a homomorphism $W_n = G_a(W_n) \to H$ with $u$ in its image. This was proved by Proud [Pro01]; see [McNa] for another proof when $H$ is classical.

In view of these results, one might wonder whether $u$ lies in the image of a homomorphism $\gamma : SL_2(W_n) \to H$. Theorem [3] shows that, in general, the answer is “no”.

Indeed, let $H$ be the reductive group $GL_{p+1}/k$. Then a regular unipotent element $u$ of $H$ has order $p^2$. On the other hand, if $f : SL_2(W_2) \to H$ is a homomorphism, the theorem shows that $u$ is not in the image of $f$.

3. WITT VECTORS

Elements of $W_n$ will be represented as tuples $(a_0, a_1, \ldots, a_{n-1})$ with $a_i \in k$. For $w = (a_0, a_1)$ and $w' = (b_0, b_1)$ in $W_2$, we have:

1. $w + w' = (a_0 + b_0, a_1 + b_1 + F(a_0, b_0))$ and $w \cdot w' = (a_0b_0, a_0b_1 + b_0a_1)$,

where $F(X, Y) = (X^p + Y^p - (X + Y)^p)/p \in Z[X, Y]$.

We have also the identity in $W_n$

2. $(t, 0, \cdots, 0) \cdot (a_0, a_1, \ldots, a_{n-1}) = (ta_0, t^pa_1, \ldots, t^{p^{n-1}}a_{n-1})$

for all $t \in k$ and $(a_0, \ldots, a_{n-1}) \in W_n$.

Let $\mathcal{X}_n : W_n = G_a(W_n) \to \Gamma_n$ and $\phi : k^\times \to \Gamma_n$ be the maps

$$\mathcal{X}_n(w) = \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \phi(t) = \begin{pmatrix} (t, 0, \ldots, 0) \\ 0 \\ 0 \\ (1/t, 0, \ldots, 0) \end{pmatrix}.$$  

Using (2), one observes the relation

3. $\text{Int}(\phi(t)) \mathcal{X}_n(a_0, a_1, \ldots, a_{n-1}) = \mathcal{X}_n(t^2a_0, t^2a_1, \ldots, t^{2^{p^{n-1}}-1}a_{n-1}).$

The element $\mathcal{X}_n(a_0, a_1, \ldots, a_{n-1})$ is unipotent; if $a_0 \neq 0$, it has order $p^n$.  

For \( n \geq 2 \), the map \((a_0, a_1, \ldots, a_{n-1}) \mapsto (a_0, \ldots, a_{n-2}) : W_n \to W_{n-1}\) induces a surjective homomorphism \( \Gamma_n \to \Gamma_{n-1} \)
whose kernel we denote by \( R_n \). Similarly, the residue map \((a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 : W_n \to k\) induces a surjective homomorphism \( \eta : \Gamma_n \to SL_2(k) \).

Concerning \( R_n \), we have the following:

**Lemma 3.** The group \( R_n \) is a connected, Abelian unipotent group of dimension 3. More precisely, there is a \( \Gamma_n \)-equivariant isomorphism of algebraic groups
\[
\gamma : R_n \to gl_2(k);
\]
the action of \( \Gamma_n \) on \( sl_2(k) \) is by \( Ad^{[n-1]} \circ \eta \), where \( Ad^{[n-1]} \) is the \((n-1)\)-st Frobenius twist of the adjoint representation of \( SL_2(k) \), and the action of \( \Gamma_n \) on \( R_n \) is by inner automorphisms.

The lemma follows from [DG70, II.§4.3]. Actually, the cited result is quite straightforward for \( SL_2 \).

The lemma shows that the kernel of \( \eta \) is a \( 3(n-1) \) dimensional unipotent group. In particular, \( \Gamma_n \) has dimension \( 3n \). Since \( \Gamma_n / \ker \eta \cong SL_2(k) \) is reductive, \( \ker \eta \) is the unipotent radical of \( \Gamma_n \). In particular, we see that the image of \( \phi \) is a maximal torus \( T \) of \( \Gamma_n \).

We now consider the case \( n = 2 \); we write \( \mathcal{Z} \) for \( R_2 \). Let \( \mathcal{Z} : G_a(k) \to R < G \) be the homomorphism
\[
(5) \quad \mathcal{Z}(s) = \begin{pmatrix} 1, s & 0 \\ 0 & (1, -s) \end{pmatrix}.
\]
An easy matrix calculation yields:
\[
(6) \quad \text{Int}(\phi(t))\mathcal{Z}(s) = \mathcal{Z}(s) \quad \text{for each } t \in k^\times \text{ and } s \in k.
\]
Recall that any non-0 nilpotent element of \( sl_2(k) \) is a cyclic generator as a \( \Gamma_2 \)-module, and any non-0 semisimple element of \( sl_2(k) \) generates the socle of this module. (These remarks are trivial for \( p > 2 \) since in that case \( sl_2(k) \) is a simple \( SL_2(k) \)-module; the assertions in characteristic 2 are well known and anyhow easy to verify.) We thus obtain the following:

**Lemma 4.** There are no proper \( \Gamma_2 \)-invariant subgroups of \( R \) containing \( \mathcal{Z}(0, 1) \). Any non-trivial \( \Gamma_2 \)-invariant subgroup of \( R \) contains \( \mathcal{Z}(1) \).

**Remark 5.** J. Humphreys pointed out that \( \Gamma_n \) provides an example of a linear algebraic group in characteristic \( p \) with no Levi decomposition. Here is an argument for his observation using the main result of this paper.

First, since \( \Gamma_2 \) is a quotient of \( \Gamma_n \), the above observation follows from:

- The group \( \Gamma_2 \) has no Levi decomposition.

Let \( H = (Ad^{[1]}, sl_2(k)) \rtimes SL_2(k) \). If we know that \( H \) has a representation \((\mu, V)\) such that \( \dim V < p + 3 \) and \( \ker \mu \) is finite, then Theorem 4 implies that \( \Gamma_2 \) is not isomorphic to \( H \), hence that \( \Gamma_2 \) has no Levi decomposition.

If \((\lambda, V)\) is a rational representation of a linear algebraic group \( A \), we may form the semidirect product \( \hat{A} = (\lambda, V) \rtimes A \). There is a rational representation \((\lambda, V \oplus k)\)
of \( \hat{\lambda} \) given by \( \hat{\lambda}(v,a)(w,\alpha) = (\lambda(a)w + \alpha v, \alpha) \) for \((v,a) \in \hat{A} \) and \((w,\alpha) \in V \oplus k\). A straightforward check yields
\[
\ker \hat{\lambda} = \{(0, a) \mid a \in \ker \lambda \}.
\]

Applying this construction with \( A = \text{SL}_2(k) \), \((\lambda, V) = (\text{Ad}^{[1]}, \mathfrak{sl}_2(k))\), \( \hat{A} = H \), we find a representation
\[
(\text{Ad}^{[1]}, \mathfrak{sl}_2(k) \oplus k)
\]
with dimension \( 4 < p + 3 \) and finite kernel \( \{(0, \pm 1)\} \leq H \), as required.

For a different proof of this observation (when \( p \geq 5 \)) see \cite{Ser68}, IV.23.

Remark 6. One can list all normal subgroups \( N \) of \( \Gamma_2 \). If \( p > 2 \), \( N \cap R \) must be either 1 or \( R \). Since the only proper, non-trivial normal subgroup of \( \text{SL}_2(k) = \Gamma_2/R \) is \( \{\pm 1\} \), we see that \( N \) is one of
\[
\Gamma_2, \quad R, \quad \{\pm 1\}, \quad R \cdot \{\pm 1\}, \quad 1
\]
In this case \( \{\pm 1\} \) is the center of \( \Gamma_2 \).

If \( p = 2 \), \( N \cap R \) is either 1, \( R \), or \( Z \), the inverse image under \( \gamma \) of the 1 dimensional center of \( \mathfrak{sl}_2(k) \). The group \( \text{SL}_2(k) = \Gamma_2/R \) is (abstractly) a simple group. Let \( N \lhd \Gamma_2 \) satisfy \( N \cap R = Z \). Then \( \eta(N) \) is either trivial or equal to \( \text{SL}_2(k) \). If \( \eta(N) \neq 1 \), there is an extension
\[
1 \to Z \to N \to \text{SL}_2(k) \to 1.
\]
We have \( H^2(\text{SL}_2(k), Z) = H^2(\text{SL}_2(k), k) = 0 \) by \cite{Jan87}, Proposition II.4.13], so such an extension must be split. But a splitting would yield a Levi decomposition for \( \Gamma_2 \), contrary to our observations in Remark 5. Thus \( \eta(N) = 1 \) so \( N = Z \). [Note that the argument we just gave depends on Theorem 4; we will not use it in proving this theorem.]

To summarize, the possibilities for \( N \) are:
\[
\Gamma_2, \quad R, \quad Z, \quad 1
\]
The group \( Z \) is the center of \( G \). It is equal to the image \( \mathcal{P}(k) \).

4. UNIPOTENT RADICALS AND REPRESENTATIONS

Let \( A \) be a linear algebraic group over \( k \), and let \( R \) denote its unipotent radical. If \((\rho, V) \) is a rational finite dimensional \( A \)-representation (with \( V \neq 0 \)), then the space \( V^R \) of \( R \)-fixed points is a non-0 \( A \)-subrepresentation (the fact that it is non-0 follows from the Lie-Kolchin Theorem \cite{Spr98}, Theorem 6.3.1). This implies that there is a filtration of \( V \) by \( A \)-subrepresentations
\[
V = \mathcal{R}^0 V \supset \mathcal{R}^1 V \supset \mathcal{R}^2 V \supset \cdots \supset \mathcal{R}^n V = 0
\]
with the properties: \( (\rho(x) - 1)\mathcal{R}^i V \subset \mathcal{R}^{i+1} V \) for each \( x \in R \) and each \( i \), and each quotient \( \mathcal{R}^i V/\mathcal{R}^{i+1} V \) is a non-0 representation for the reductive group \( A/R \).

We see in particular that the simple \( A \)-modules are precisely the simple \( A/R \)-modules inflated to \( A \).

All this applies especially for \( A = \Gamma_n, n \geq 1 \). We identify the simple \( \text{SL}_2(k) \) modules and the simple \( \Gamma_n \)-modules; for \( a \geq 0 \), there is thus a simple \( \Gamma_n \)-module \( L(a) \) with highest weight \( a \). If \( 0 \leq a \leq p - 1 \), \( \dim L(a) = a + 1 \). If \( a \) has \( p \)-adic
expansion \( a = \sum a_i p^i \) where \( 0 \leq a_i \leq p - 1 \) for each \( i \), then Steinberg’s tensor product theorem \([\text{Jan87}, \text{II.3.17}]\) yields
\[
L(a) \simeq L(a_0) \otimes L(a_1)^{[1]} \otimes L(a_1)^{[2]} \otimes \cdots
\]
where \( V^{[i]} \) denotes the \( i \)-th Frobenius twist of the \( \Gamma_n \) module \( V \).

5. A FAITHFUL G-REPRESENTATION

In this section, we consider the group \( G = \Gamma_2 = \text{SL}_2(W_2) \). We recall the homomorphisms \( \mathscr{X}_2 : W_2 \to G \) and \( \mathscr{X} : k \to R \); we write \( \mathscr{X} \) for \( \mathscr{X}_2 \).

**Lemma 7.** Let \( (\rho, V) \) be a rational finite dimensional \( G \)-representation. Then \( \rho \) is abstractly faithful (i.e. injective on the closed points of \( G \)) if and only if (i) \( (\rho|_T, V) \) is an abstractly faithful \( T \)-representation, and (ii) \( u = \rho(\mathscr{X}(1)) \neq 1_V \).

**Proof.** The necessity of conditions (i) and (ii) is clear, so suppose these conditions hold and let \( K \) be the kernel of \( \rho \). Let \( \text{gr}(V) \) denote the associated graded space for any filtration as in \([\text{1}]\). Then \( \text{gr}(V) \) is a module for \( \Gamma_2/R = \text{SL}_2(k) \). Condition (i) implies that \( \text{gr}(V) \) acts as a group of automorphisms on the 4 dimensional affine coordinate ring \( k[A_0, A_1, B_0, B_1] \).

There is a linear representation \( \lambda \) of \( k^x \) on \( \mathscr{X} \) given by \( (\lambda(t)f)(w) = f((t,0),w) \) for \( t \in k^x \), \( f \in \mathscr{X} \), \( w \in W_2 \oplus W_2 \). One checks easily that \( \lambda(t)A_0 = tA_0 \), and that \( \lambda(t)A_1 = t^pA_1 \) for \( t \in k^x \), with similar statements for \( B_0 \) and \( B_1 \).

For \( \nu \in \mathbb{Z} \), let \( \mathscr{X}_\nu \) be the space of all functions \( f \in \mathscr{X} \) for which \( \lambda(t)f = t^\nu f \) for all \( t \in k^x \) (i.e. the \( \nu \)-weight space for the torus action \( \lambda \)). Then we have a decomposition \( \mathscr{X} = \bigoplus_{\nu \in \mathbb{Z}} \mathscr{X}_\nu \) as a \( \lambda(k^x) \)-representation.

Since \( G \) acts “\( W_2 \)-linearly” on \( W_2 \oplus W_2 \), \( \lambda(k^x) \) centralizes \( \rho(G) \); thus each \( \mathscr{X}_\nu \) is a \( G \)-subrepresentation of \( \mathscr{X} \). We consider the \( G \)-representation \((\rho_\nu, \mathscr{X}_\nu)\). One sees that \( \mathscr{X}_\nu \) is spanned by all \( A_i^0B_j^0 \) with \( i + j = p \) and \( i, j \geq 0 \), together with \( A_1 \) and \( B_1 \). Thus \( \dim \mathscr{X}_\nu = p + 3 \).

Using \([\text{1}]\), one checks for each \( s \in k \) that
\[
\rho_\nu(\mathscr{X}(s))A_1 = A_1 + sA_0^p,
\]
so that \( \rho_\nu(\mathscr{X}(1)) \neq 1_V \). Since \( A_1 \) has \( T \)-weight \( p \), \( \mathscr{X}_\nu \) is an abstractly faithful representation of \( T \); thus the lemma shows that \((\rho_\nu, \mathscr{X}_\nu)\) is an abstractly faithful \( G \)-representation.

**Remarks 9.**

(a) It is straightforward to see that \((\rho_\nu, \mathscr{X}_\nu)\) has length three, and that its composition factors are \( L(p-2) \) together with two copies of \( L(p) = L(1)^{[1]} \).

(b) The representation \( \rho_p \) is defined over the prime field \( \mathbb{F}_p \). In particular, the finite group \( \text{SL}_2(\mathbb{Z}/p^2\mathbb{Z}) \) has a faithful representation on a \( p + 3 \) dimensional \( \mathbb{F}_p \)-vector space. More generally, the finite group \( \text{SL}_2(W_2(\mathbb{F}_q)) \) has
a faithful representation on a \( p + 3 \) dimensional \( \mathbf{F}_q \)-vector space for each \( q = p^q \).

(c) We will show in [8] that the representation \((\rho_p, \mathcal{A}_p)\) is actually faithful provided that \( p > 2 \).

6. ALGEBRAS OF DISTRIBUTIONS

Let \( H \) be a linear algebraic \( k \)-group, and let \( \text{Dist}(H) \) be the algebra of distributions on \( H \) supported at the identity; see [Jan87, I.7] for the definitions. Recall that elements of \( \text{Dist}(H) \) are certain linear forms on the coordinate algebra \( k[H] \).

The algebra structure of \( \text{Dist}(H) \) is determined by the comultiplication \( \Delta \) of \( k[H] \); the product of \( \mu, \nu \in \text{Dist}(H) \) is given by

\[
\mu \cdot \nu : k[H] \xrightarrow{\Delta} k[H] \otimes_k k[H] \xrightarrow{\mu \otimes \nu} k \otimes_k k = k.
\]

We immediately see the following:

\begin{equation}
(8) \quad \text{If } H \text{ is Abelian, then } \text{Dist}(H) \text{ is a commutative } k\text{-algebra.}
\end{equation}

Now consider the case \( H = W_2 \). As a variety, \( W_2 \) identifies with \( A^2_1 \). We write \( k[W_2] = k[A_0, A_1] \) as before. As a vector space \( \text{Dist}(W_2) \) has a basis \( \{\gamma_{i,j} \mid i, j \geq 0\} \) where \( \gamma_{i,j}(A_0 A_1^t) = \delta_{i,s} \delta_{j,t}; \) see [Jan87, I.7.3].

Let \((\rho, V)\) be a \( W_2 \)-representation. This is determined by a comodule map

\[
\Delta_V : V \to V \otimes_k k[W_2];
\]

for \( v \in V \) we have \( \Delta_V(v) = \sum_{i,j \geq 0} \psi_{i,j}(v) \otimes A_0^i A_1^j \) where \( \psi_{i,j} \in \text{End}_k(V) \).

The \( W_2 \)-module \((\rho, V)\) becomes a \( \text{Dist}(W_2) \)-module by the recipe given in [Jan87, I.7.11]. A look at that recipe shows that the basis elements \( \gamma_{i,j} \in \text{Dist}(W_2) \) act on \( V \) as multiplication by \( \psi_{i,j} \). Since \( W_2 \) is Abelian, we deduce that the linear maps \( \{\psi_{i,j} \mid i, j \geq 0\} \) pairwise commute.

In view of the commutativity, we obtain

\[
1_V = \rho(a, b)p^2 = \left( \sum_{i,j \geq 0} a^i b^j \psi_{i,j} \right) p^2 = \sum_{i,j \geq 0} a^i b^j p^2 \psi_{i,j}^p,
\]

identically in \( a, b \); thus \( \psi_{0,0} = 1_V \) and \( \psi_{i,j}^p = 0 \) if \( i > 0 \) or \( j > 0 \).

Now let \( H \) be the subgroup of \( G = \text{SL}_2(W_2) \) generated by the maximal torus \( T \) together with the image of \( \mathcal{X}_2 : W_2 \to G \). Thus \( H \) is a semidirect product \( \mathcal{X}_2(W_2) \rtimes T \).

Let \((\rho, V)\) be an \( H \)-representation. The \( T \)-module structure on \( V \) yields a \( T \)-module structure on \( \text{End}_k(V) \); for a weight \( \mu \) of \( T \) we have \( \psi \in \text{End}_k(V)_\mu \) if and only if \( \psi(v) \in V_{\lambda + \mu} \) for all weights \( \lambda \) and all \( v \in V_\lambda \).

Fix a weight vector \( v \in V_\lambda \). Then

\[
\rho(\mathcal{X}_2(a, b))v = \sum_{i,j \geq 0} a^i b^j \psi_{i,j}(v),
\]

where the \( \psi_{i,j} \) are determined as before by the comodule map for the \( W_2 \)-module \( V \). A look at [8] shows that \( \psi_{i,j}(v) \in V_{\lambda + 2i + 2pj} \). It follows that \( \psi_{i,j} \in \text{End}_k(V)_{2i + 2pj} \).

**Proposition 10.** Let \((\rho, V)\) be a representation of \( H = \mathcal{X}_2(W_2) \rtimes T \). Suppose that \( \rho(\mathcal{X}_2(0, 1)) \neq 1_V \). Then \( T \) has at least \( p + 1 \) distinct weights on \( V \). More precisely, there are weights \( s \in \mathbf{Z}_{\geq 0} \) and \( \lambda \in \mathbf{Z} \) such that \( V_{\lambda + 2sj} \neq 0 \) for \( 0 \leq j \leq p \).
Proof. We have \( \mathcal{X}_2(0,1) = \mathcal{X}_2(1,0)^p \). With notation as above, our hypothesis means that
\[
1_V \neq \rho(\mathcal{X}_2(1,0))^p = \left( \sum_{i \geq 0} \psi_{i,0} \right)^p = \sum_{i \geq 0} \psi_{i,0}^p.
\]
Thus there is some \( s > 0 \) for which \( \psi_{s,0}^p \neq 0 \). Write \( \psi = \psi_{s,0} \). Recall that \( \psi \) has \( T \)-weight \( 2s \). We may find a weight \( \lambda \in \mathbb{Z} \) and \( v \in V_{\lambda} \) for which \( \psi^p(v) \neq 0 \). But then \( v, \psi(v), \ldots, \psi^p(v) \) are all non-0, and have respective weights \( \lambda, \lambda + 2s, \ldots, \lambda + 2sp \). The proposition follows.

Remark 11. The following analogue of the proposition for \( H_n = \mathcal{X}_n(W_n) \cdot T \leq \Gamma_n \) may be proved by the same method: if \( (\rho, V) \) is an \( H_n \) module such that \( \rho(\mathcal{X}_n(0, \ldots, 0, 1)) \neq 1_V \), then there are weights \( s \in \mathbb{Z}_{>0} \) and \( \lambda \in \mathbb{Z} \) such that \( V_{\lambda + 2sj} \neq 0 \) for \( 0 \leq j \leq p^{n-1} \). In particular, \( T \) has at least \( p^{n-1} + 1 \) distinct weight spaces on \( V \).

7. Minimality of \( p + 3 \)

In this section, \( G \) again denotes the group \( \Gamma_2 = \text{SL}_2(W_2) \), and \( \mathcal{X} = \mathcal{X}_2 \).

Lemma 12. Let \( (\rho, V) \) be a \( G \)-representation with \( \rho(\mathcal{X}(1)) \neq 1_V \). For some \( \nu \in \mathbb{Z} \), the \( T \)-weight space \( V_{\nu} \) must satisfy \( \dim V_{\nu} \geq 2 \).

Proof. We may find \( \nu \in \mathbb{Z} \) and a \( T \)-weight vector \( v \in V_{\nu} \) for which
\[
\rho(\mathcal{X}(1))v \neq v.
\]
There are uniquely determined vectors \( \nu = v_0, v_1, \ldots, v_N \in V \) with \( \rho(\mathcal{X}(s))v = \sum_{i=0}^{N} s^i v_i \) and \( v_N \neq 0 \). Since \( \rho(\mathcal{X}(1))v \neq v \), we must have \( N > 1 \). Since \( \rho(\mathcal{X}(1))v_N = v_N \), the vectors \( v \) and \( v_N \) are linearly independent. By \( \Box \) we have \( v_N \in V_{\nu} \), whence the lemma.

Theorem 13. Suppose that \( (\rho, V) \) is a \( G \)-representation with \( \dim V \leq p + 2 \). Then \( \rho(\mathcal{X}(1)) = 1_V \). In particular, any faithful \( G \)-representation has dimension at least \( p + 3 \).

Proof. Let \( (\rho, V) \) be a \( G \)-representation for which \( \rho(\mathcal{X}(1)) \neq 1_V \). By Lemma 12, we have \( \rho(\mathcal{X}(0,1)) \neq 1_V \). According to Proposition 10, we may find \( \lambda \in \mathbb{Z} \) and \( s > 0 \) such that \( V_{\lambda + 2sj} \neq 0 \) for \( 0 \leq j \leq p \). Since by Lemma 12, there must be some \( \mu \in \mathbb{Z} \) with \( \dim V_{\mu} \geq 2 \), we deduce that \( \dim V \geq p + 2 \).

To finish the proof, we suppose that \( \dim V = p + 2 \) and deduce a contradiction. Since we may suppose that \( V \) has a 2 dimensional weight space \( V_{\mu} \), we see that the \( T \)-weights of \( V \) are precisely the \( \lambda + 2sj \) for \( 0 \leq j \leq p \). Since the character of \( V \) must be the character of an \( \text{SL}_2(k) \) module, we have \( \dim V_{\gamma} = \dim V_{-\gamma} \) for all weights \( \gamma \in \mathbb{Z} \). Since \( V_{\mu} \) is the unique 2 dimensional weight space, we deduce that \( \mu = 0 \).

It follows that \( \lambda, \lambda + 2s, \ldots, \lambda + 2sp \) must be the weights of some \( \text{SL}_2(k) \) module. Steinberg’s tensor product theorem now implies that \( s = p^r \) for some \( r \geq 0 \). We then have \( \lambda = -(\lambda + 2p^{r+1}) \), so that \( \lambda = -p^{r+1} \). If \( p > 2 \), then we see that \( \lambda + 2p^r j \neq 0 \) for any \( j \), so is not a weight of \( V \); this gives our contradiction when \( p > 2 \).

So we may suppose that \( p = 2 \), that \( \dim V_{\lambda + 2s} = 1 \), and that \( \dim V_{\lambda} = 2 \). Thus the composition factors of \( V \) are \( L(2^r) = L(1)^{|r|}, L(0), \) and \( L(0) \). We claim first that \( \dim V^R = 1 \). Indeed, since \( \rho(\mathcal{X}(0,1)) \neq 1 \), a look at the proof of Theorem 11...
shows that $V_{2r} \cap V^R = 0$. Moreover, since $\rho(\mathcal{X}(1)) \neq 1$, Lemma 13 shows that $V_0 \not\subset V^R$.

Next, we claim that $soc(V/V^R)$ can not have $L(0)$ as a summand. Indeed, otherwise one finds a 2 dimensional indecomposable $G$-module with composition factors $L(0), L(0)$ on which $\mathcal{X}(1)$ acts non-trivially. But $\mathcal{X}'(1,0)$ must act trivially on such a module, contrary to Lemma 4.

It now follows that $soc(V/V^R) = L(1)^{[\rho]}$. But then the inverse image $W$ in $V$ of $soc(V/V^R)$ is a $G$-submodule of $V$ containing $V_{2r}$. Moreover, dim $W = 3$, $\mathcal{X}'(0,1)$ acts non-trivially on $W$, while $\mathcal{X}'(1)$ must act trivially on $W$. Thus $\ker \rho \cap R$ is precisely $Z = \{ \mathcal{X}(t) \mid t \in k \}$; see Remark 3. Let $\mathcal{Y}: W_2 \to \Gamma_2$ be the map

$$\mathcal{Y}(w) = \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}.$$ 

Since $\mathcal{Y}(0,1) \not\in R$, we have $\rho(\mathcal{Y}(0,1)) \neq 1$. Moreover, we know that $\rho(\mathcal{Y}(0,1))$ commutes with $\rho(\mathcal{X}(0,1))$. But the fixed point space of $\rho(\mathcal{Y}(0,1))$ on $W$ is precisely $W_0 \oplus W_2$, which is not stable under $\rho(\mathcal{Y}(0,1))$ by (the proof of) Proposition 14. This gives the desired contradiction when $p = 2$.

Corollary 14. Suppose that $(\rho, V)$ is a $G$-representation with dim $V \leq p + 2$. Then the $p$-th power of each unipotent element of $G$ acts trivially on $V$.

Proof. Theorem 13 shows that $R \cap \ker(\rho)$ is a normal subgroup of $G$ containing $\mathcal{X}'(1)$, hence is $R$ by Lemma 4. If $u \in G$ is unipotent, then $u^p \in R$ whence the corollary.

8. The Lie algebra of $\Gamma_2$

Let $\mathfrak{g} = \operatorname{Lie}(\Gamma_2)$. There is an exact sequence of $p$-Lie algebras and of $\Gamma_2$-modules

$$0 \to \operatorname{Lie}(R) \to \mathfrak{g} \to \mathfrak{sl}_2(k) \to 0.$$ 

Lemma 15. Suppose that $p > 2$. Then $R$ acts trivially on $\mathfrak{g}$. In particular, (4) is an exact sequence of $\mathfrak{sl}_2(k)$-modules.

Proof. Since the adjoint module for $\mathfrak{sl}_2(k)$ is simple when $p > 2$, it suffices by Lemma 8 to show that $\operatorname{Ad}(\mathcal{X}(0,1)) = 1$. Note that the weights of $T$ on $\mathfrak{g}$ are $\pm 2, \pm 2p$, and $0$. Since $p > 2$, Proposition 14 implies that $\mathcal{X}'(0,1)$ acts trivially on $\mathfrak{g}$ as desired.

The Abelian Lie algebra $\operatorname{Lie}(W_2)$ contains an element $Y$ for which $Y$ and $Y^{[p]}$ form a $k$-basis. The element $Y^{[p]}$ spans the image of the differential of $(t \mapsto (0,t)) : k \to W_2$. Write $X = dX(Y)$. Then $X \not\in \operatorname{Lie}(R)$ and $X^{[p]} \in \operatorname{Lie}(R)$.

Proposition 16. (1) If $(d\lambda, V)$ is a restricted representation of the $p$-Lie algebra $\mathfrak{g}$, then $\ker d\lambda \cap \operatorname{Lie}(R) = 0$ if and only if $(d\lambda)(Z) \neq 0$ where $Z = d\mathcal{X}(1)$.

(2) Let $p > 2$. Then (4) is split as a sequence of $\Gamma_2$-modules.

(3) Let $p > 2$, and let $(d\lambda, V)$ be a representation of $\mathfrak{g}$ as a $p$-Lie algebra. Then $\ker d\lambda = 0$ if and only if $d\lambda(X^{[p]}) \neq 0$.

Proof. (1) is a consequence of Lemma 4.

(2) By Lemma 15, $R$ acts trivially on $\mathfrak{g}$, so $\mathfrak{g}$ may be viewed as a module for $\mathfrak{sl}_2(k)$. Note that (4) has the form $0 \to L(2p) \to \mathfrak{g} \to L(2) \to 0$. Since $p > 2$, 2 and
2p are not linked under the action of the affine Weyl group. Hence, the sequence splits thanks to the linkage principle \[\text{[Jan87] II.6.17}].

(3) By hypothesis both \(d\lambda(X)\) and \(d\lambda(X[p])\) are non-0. The image of \(X\) is a generator for \(g/\text{Lie}(R)\) as a \(\Gamma_2\)-module, and \(X[p]\) is a generator for \(\text{Lie}(R)\) as a \(\Gamma_2\)-module, so the claim follows from (2).

**Corollary 17.** Consider the \(\Gamma_2\) representation \((\rho_p, \mathcal{A}_p)\) of \(\mathfrak{g}\).

1. If \(p > 2\), then \((d\rho_p, \mathcal{A}_p)\) is a faithful representation of \(g\).
2. If \(p = 2\), then \(\ker d\rho_p = \text{Lie}(T)\) is 1-dimensional.

**Proof.** With notations as before, using (1) one sees that \(\rho_p(\mathcal{F}(0, s))A_1 = A_1 + sB_0^p\) for \(s \in k\). It follows that \(d\rho_p(X[p])A_1 = cB_0^p\) for some \(c \in k^\times\). When \(p > 2\), part (3) of the proposition shows that \(d\rho_p\) is faithful.

Let \(Z = d\mathcal{F}(1)\) as before. The calculation in the proof of Theorem 8 implies that \(d\rho_p(Z)A_1 = A_0^p\). In particular, part (1) of the proposition shows that \(\ker d\rho_p \cap \text{Lie}(R) = 0\) for all \(p\). When \(p = 2\), note that \(\text{Lie}(T)\) indeed acts trivially; see Remark \[\text{[Jan87] II.6.17}\]. The corollary now follows. \[\square\]

### 9. Representations of the Associated Finite Groups

In this section, a representation of a group is always assumed to be on a finite dimensional \(k\)-vector space.

#### 9.1. Representations of \(\mathbb{F}_p\)-Simple Groups

Let \(C\) be a finite cyclic group of order relatively prime to \(p\), and suppose that \(\rho : C \to \text{Aut}_{k\text{-alg}}(A)\) is a representation of \(C\) by algebra automorphisms on the algebra of truncated polynomials 

\[A = k[z]/(z^N)\]

for some \(N \geq 2\). Let \(X = \text{Hom}(C, k^\times)\) be the group of characters of \(C\). Since \(|C|\) is prime to \(p\), \(X\) is (non-canonically) isomorphic to \(C\); in particular, it is cyclic. Note that an element \(\mu \in X\) is a generator if and only if \(\mu\) is injective as a homomorphism. If \((\rho, V)\) is a \(C\)-representation, and \(\mu \in X\), let 

\[V_\mu = \{v \in V \mid \rho(c)v = \mu(c)v \text{ for each } c \in C\}.
\]

Of course, \(V \simeq \bigoplus_{\mu \in X} V_\mu\).

Write \(m = (z)\) for the maximal ideal of \(A\).

**Lemma 18.** With notations as above, if \((\rho, A)\) is a faithful \(C\)-representation, then there is \(\mu \in X\) and an element \(f \in m \cap A_\mu\) such that \(f\) has non-zero image in \(m/m^2\).

**Proof.** Since \(C\) acts by algebra automorphisms, the ideal \(m^i\) is \(C\)-invariant for each \(i \geq 1\). Since the \(C\) representation \((\rho, m)\) is semisimple, the subrepresentation \(m^2\) has a complement \(k.f\) for some \(0 \neq f \in m\). Thus there is \(\mu \in X\) such that \(\rho(c)f = \mu(c)f\) for each \(c \in C\), and since \(f \notin m^2\), the image of \(f\) in \(m/m^2\) is non-zero. It remains to argue that \(\mu\) is a generator for \(X\). Note that \(1, f, f^2, \ldots, f^{N-1}\) form a \(k\)-basis for \(A\), so that 

\[(\rho, A) \simeq 1 \oplus \mu \oplus \mu^2 \oplus \cdots \oplus \mu^{N-1}\]
as \(C\)-representations. Since \((\rho, A)\) is a faithful representation, we see that \(\mu\) must itself be a faithful representation of \(C\), so that \(\mu\) indeed generates \(X\). \[\square\]
9.2. Let $V$ be a $k$-vector space of dimension $n \geq 2$. Let $u$ be a regular unipotent element in $GL(V)$; thus $u$ acts on $V$ as a single unipotent Jordan block. It is well known (and easy to see) that the centralizer of $u$ in $gl(V) = End_k(V)$ is the (associative) algebra $k[u]$ generated by $u$. Let $A = u - 1$. Then $A$ is a regular nilpotent element (it acts as a single nilpotent Jordan block), and $k[u] = k[A]$. Now, $k[A]$ is isomorphic to the algebra of truncated polynomials $k[z]/(z^{n-1})$. Moreover, if $f \in k[A]$ is a regular nilpotent element of $gl(V)$ if and only if $f \in m \setminus m^2$.

9.3. Suppose that $H$ is a finite group, that $C < H$ is a cyclic subgroup of order prime to $p$, and that $W < H$ is an Abelian $p$-group which is normalized by $C$. As before, let $X = \text{Hom}(C, k^\times)$. Write $C'$ for the centralizer in $C$ of $W$, and let $X' = \{\mu \in X \mid \mu_{C'} = 1\}$.

**Proposition 19.** Let $(\rho, V)$ be a faithful, finite dimensional $H$-representation, and suppose that $\rho(W)$ contains a regular unipotent element of $GL(V)$. If $|C/C'| \geq \dim V$, then $V_\mu$ is 1 dimensional for each $\mu \in X$. Moreover, there is $\lambda \in X$ and a generator $\mu \in X'$ such that $V \cong V_\lambda \oplus V_{\lambda+\mu} \oplus \cdots \oplus V_{\lambda+d\mu}$ where $\dim V = d + 1$.

**Proof.** Let $u \in \rho(W)$ be a regular unipotent element. As in 9.2, the centralizer of $u$ in $End_k(V)$ is $k[u]$. For each $c \in C$ we have, $\rho(c) u \rho(c)^{-1} \in k[u]$ since $W$ is Abelian. It follows that $C$ acts by conjugation on $A = k[u]$. Moreover, $C/C'$ acts faithfully on $A$. According to Lemma 13, there is a generator $\mu \in X'$ with $X' = X(C/C')$ and (in view of 9.2) a regular nilpotent element $A \in (gl(V))_\mu$.

Let $d = \dim V - 1$. We may thus find $\lambda \in X$ such that $A^d(V_\lambda) \neq 0$. It follows that $V_\lambda, V_{\lambda+\mu}, \ldots, V_{\lambda+d\mu}$ are all non-0. Since $\mu$ has order $|C/C'| > d$, each of these subspaces has dimension 1. The proposition follows. \hfill \square

9.4. Fix a $p$-power $q = p^m$, and let $F_q$ be the field with $q$ elements. The group $\Gamma_n$, and the homomorphisms $\phi: G_m \rightarrow \Gamma_n$ and $\mathcal{X}_n: W_n \rightarrow \Gamma_n$, are defined over $F_q$.

Let $n = 2$, and let $C, W \leq \Gamma_2(F_q) = SL_2(W_2(F_q))$ be respectively the image under $\phi$ of $G_m(F_q) \cong F_q^\times$ and the image under $\mathcal{X}_2$ of $W_2(F_q)$. Then $C$ is cyclic of order prime to $p$, and $W$ is a $p$-group normalized by $C$. Moreover, the centralizer $C'$ of $W$ in $C$ has order 2.

**Theorem 20.** Suppose that $p \geq 3$ and $q \geq p^2$. Then the minimal dimension of a faithful $k$-representation of $\Gamma_2(F_q)$ is $p + 3$.

**Proof.** That $\Gamma = \Gamma_2(F_q)$ has a faithful representation of dimension $p + 3$ follows from Remark 3(b).

We now suppose that $(\rho, V)$ is a faithful representation of $\Gamma$ with $\dim V \leq p + 2$ and deduce a contradiction. Since the element $\mathcal{X}_2(1, 0)$ of $\Gamma_2(F_q)$ has order $p^2$, we see that $\dim V \geq p + 1$. Suppose first that $\dim V = p + 1$. Then the image $\rho(W)$ must contain a regular unipotent element.

With our assumption on $q$, we have $|C/C'| = \frac{q - 1}{2} \geq p + 1 = \dim V$. An application of Proposition 14 for the subgroups $C, W < \Gamma'$ therefore shows that the spaces $V_\mu$ with $\mu \in X(C)$ are all 1-dimensional. Lemma 12 now shows that the element $\mathcal{X}_2(1) \in \Gamma$ must act trivially; this contradicts our assumption that $(\rho, V)$ is faithful.

Finally, suppose that $\dim V = p + 2$. Let $H$ be the subgroup of $\Gamma$ generated by $C$ and $W$. Since $H$ is nilpotent and since $\rho(H)$ contains a unipotent element with Jordan block sizes $(p + 1, 1)$, we have $V = V' \oplus V''$ with $V'$ and $V''$ invariant
under \( H \), and with \( \dim V' = p + 1 \). Now an application of Proposition 19 to the \( H \)-representation \( V' \) shows that there is a weight \( \lambda \in X(C) \) and a generator \( \mu \in X' \) such that \( V' = \bigoplus_{i=0}^{p} V'_{\lambda + i\mu} \) with \( \dim V'_{\lambda + i\mu} = 1 \) for each \( i \). In view of Lemma 12, there is precisely one \( \gamma \in X \) with \( \dim V'_{\gamma} = 2 \).

As in §4, the composition factors of the \( \Gamma \)-representation \( (\rho, V) \) may be identified with simple representations of the group \( \text{SL}_2(F_q) = \Gamma / R(F_q) \). Thanks to a theorem of Curtis ([Ste68, Theorem 43]) the semisimplification of \( (\rho, V) \) is the restriction to \( \text{SL}_2(F_q) \) of a semisimple rational \( \text{SL}_2(k) \) module \( (\psi, W) \) with \( \dim W = p + 2 \) and with precisely one two-dimensional weight space. As in the proof of Theorem 13, one knows that this is impossible (since \( p > 2 \)).

Example 21. As a “concrete” example, let \( A = \mathbb{Z}[i] \) be the ring of Gaussian integers. Suppose that the prime \( p \) satisfies \( p \equiv 1 \pmod{4} \); such a prime may be written \( p = a^2 + b^2 \) for \( a, b \in \mathbb{Z} \). Denoting by \( \mathfrak{P} \) the ideal \((a + bi)A\), one has \( A/\mathfrak{P} \simeq F_p^2 \). Then \( A/\mathfrak{P}^2 \simeq W_2(F_p^2) \), so the minimal dimension of a faithful \( p \)-modular representation of \( \text{SL}_2(A/\mathfrak{P}^2) \) has dimension \( p + 3 \).

References

[DG70] Michel Demazure and Pierre Gabriel, Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs, Masson & Cie, Éditeur, Paris, 1970, Avec un appendice Corps de classes local par Michel Hazewinkel.

[Jan87] Jens C. Jantzen, Representations of algebraic groups, Pure and Applied Mathematics, vol. 131, Academic Press, Orlando, FL, 1987.

[McNa] George J. McNinch, Abelian unipotent subgroups of reductive groups, J. Pure Appl. Algebra 167 (2002), 269–300, arXiv:math.RT/0007056.

[McNb] George J. McNinch, Sub-principal homomorphisms in positive characteristic, arXiv: math.RT/0108140.

[Pro01] Richard Proud, Witt groups and unipotent elements in algebraic groups, Proc. London Math. Soc. (3) 82 (2001), no. 3, 647–675.

[Ser68] Jean-Pierre Serre, Abelian \( l \)-adic representations and elliptic curves, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser79] Jean-Pierre Serre, Local fields, Grad. Texts in Math., vol. 67, Springer Verlag, 1979.

[Spr98] Tonny A. Springer, Linear algebraic groups, 2nd ed., Progr. in Math., vol. 9, Birkhäuser, Boston, 1998.

[Ste68] Robert Steinberg, Lectures on Chevalley groups, Yale University, 1968.

[Tes95] Donna Testerman, \( A_1 \)-type overgroups of elements of order \( p \) in semisimple algebraic groups and the associated finite groups, J. Algebra 177 (1995), 54–76.