FAITHFUL REPRESENTATIONS OF SL_2 OVER TRUNCATED WITT VECTORS

GEORGE J. MCNINCH

ABSTRACT. Let Γ_2 be the six dimensional linear algebraic k-group $\mathrm{SL}_2(W_2)$, 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 Γ_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 $W_n = W/p^n W$ 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 $\mathbf{A}^n_{/k}$. If $n \geq 2$, the ring W_n is not a k-algebra.

Let $\Gamma_n = \mathrm{SL}_2(W_n)$ be the group of 2×2 matrices with entries in W_n and with determinant 1. Then Γ_n is a closed subvariety of the $4n$ dimensional affine space of 2×2 matrices over W_n; thus, it is an affine algebraic group over k. As such, it is a closed subgroup of $\mathrm{GL}(V)$ 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 Γ_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 (ρ, V) is said to be faithful if ρ defines a closed embedding $H \to \mathrm{GL}(V)$; this is equivalent to the condition: both ρ and $d\rho$ are injective.

Theorem 1. *If (ρ, V) is a representation of Γ_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 Γ_2 is $p + 3$.*

With the same notation, if $p = 2$ then Γ_2 has a rational representation (ρ, V) with $\dim V = p + 3 = 5$, and ρ 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 Γ_2.

After some preliminaries in §2 through §4, we construct in §5 a representation (ρ, V) of Γ_2 of dimension $p+3$ and show that ρ is abstractly faithful; in §8 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 Γ_2 acts trivially on any rational module with dimension $\leq p + 2$; this completes the verification of Theorem 1. An

Date: February 11, 2002.
This work was supported in part by a grant from the National Science Foundation.

important tool in the proof is a result obtained in §6 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 §9, we prove the analogue of Theorem 2 for the finite groups $\Gamma_2(\mathbf{F}_q)$ 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 §6 with some more elementary arguments (see Proposition 19). In fact, we could use these more elementary arguments in the "algebraic" case, but the techniques in §6 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 $\Gamma_2(\mathbf{F}_p) = \mathrm{SL}_2(\mathbf{Z}/p^2\mathbf{Z})$ 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 $\mathrm{SL}_2(k) \to H$ with u in its image. This was proved by Testerman [Tes95]; 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 $W_n = \mathbf{G}_a(W_n) \to H$ 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 $\gamma : \mathrm{SL}_2(W_n) \to H$. Theorem 1 shows that, in general, the answer is "no".

Indeed, let H be the reductive group $\mathrm{GL}_{p+1/k}$. Then a regular unipotent element u of H has order p^2. On the other hand, if $f : \mathrm{SL}_2(W_2) \to H$ 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:

$$w + w' = (a_0 + b_0, a_1 + b_1 + F(a_0, b_0)) \quad \text{and} \quad w \cdot w' = (a_0 b_0, a_0^p b_1 + b_0^p a_1), \tag{1}$$

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

We have also the identity in W_n

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

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

Let $\mathscr{X}_n : W_n = \mathbf{G}_a(W_n) \to \Gamma_n$ and $\phi : k^\times \to \Gamma_n$ be the maps

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

Using (2), one observes the relation

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

The element $\mathscr{X}_n(a_0, a_1, \ldots, a_{n-1})$ 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 $\eta : \Gamma_n \to \mathrm{SL}_2(k)$.

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 Γ_n-equivariant isomorphism of algebraic groups*

$$\gamma : R_n \to \mathfrak{sl}_2(k); \tag{4}$$

the action of Γ_n on $\mathfrak{sl}_2(k)$ is by $\mathrm{Ad}^{[n-1]} \circ \eta$, where $\mathrm{Ad}^{[n-1]}$ is the $(n-1)$-st Frobenius twist of the adjoint representation of $\mathrm{SL}_2(k)$, and the action of Γ_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 η is a $3(n-1)$ dimensional unipotent group. In particular, Γ_n has dimension $3n$. Since $\Gamma_n / \ker \eta \simeq \mathrm{SL}_2(k)$ is reductive, $\ker \eta$ is the unipotent radical of Γ_n. In particular, we see that the image of ϕ is a maximal torus T of Γ_n.

We now consider the case $n = 2$; we write R for R_2. Let $\mathscr{X} : \mathbf{G}_a(k) \to R < G$ be the homomorphism

$$\mathscr{X}(s) = \begin{pmatrix} (1,s) & 0 \\ 0 & (1,-s) \end{pmatrix}. \tag{5}$$

An easy matrix calculation yields:

$$\mathrm{Int}(\phi(t))\mathscr{X}(s) = \mathscr{X}(s) \quad \text{for each } t \in k^\times \text{ and } s \in k. \tag{6}$$

Recall that any non-0 nilpotent element of $\mathfrak{sl}_2(k)$ is a cyclic generator as a Γ_2-module, and any non-0 semisimple element of $\mathfrak{sl}_2(k)$ generates the socle of this module. (These remarks are trivial for $p > 2$ since in that case $\mathfrak{sl}_2(k)$ is a simple $\mathrm{SL}_2(k)$-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 Γ_2-invariant subgroups of R containing $\mathscr{X}_2(0,1)$. Any non-trivial Γ_2-invariant subgroup of R contains $\mathscr{X}(1)$.*

Remark 5. J. Humphreys pointed out that Γ_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 Γ_2 is a quotient of Γ_n, the above observation follows from:

- The group Γ_2 has no Levi decomposition.

Let $H = (\mathrm{Ad}^{[1]}, \mathfrak{sl}_2(k)) \rtimes \mathrm{SL}_2(k)$. If we know that H has a representation (μ, V) such that $\dim V < p + 3$ and $\ker \mu$ is finite, then Theorem 1 implies that Γ_2 is not isomorphic to H, hence that Γ_2 has no Levi decomposition.

If (λ, 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 $(\hat{\lambda}, V \oplus k)$

of $\hat{A}$ 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 $A = \mathrm{SL}_2(k)$, $(\lambda, V) = (\mathrm{Ad}^{[1]}, \mathfrak{sl}_2(k))$, $\hat{A} = H$, we find a representation

$$(\widehat{\mathrm{Ad}^{[1]}}, \mathfrak{sl}_2(k) \oplus k)$$

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 [Ser68, §IV.23].

Remark 6. One can list all normal subgroups N of Γ_2. If $p > 2$, $N \cap R$ must be either 1 or R. Since the only proper, non-trivial normal subgroup of $\mathrm{SL}_2(k) = \Gamma_2/R$ 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 Γ_2.

If $p = 2$, $N \cap R$ is either 1, R, or Z, the inverse image under γ of the 1 dimensional center of $\mathfrak{sl}_2(k)$. The group $\mathrm{SL}_2(k) = \Gamma_2/R$ is (abstractly) a simple group. Let $N \lhd \Gamma_2$ satisfy $N \cap R = Z$. Then $\eta(N)$ is either trivial or equal to $\mathrm{SL}_2(k)$. If $\eta(N) \neq 1$, there is an extension

$$1 \to Z \to N \to \mathrm{SL}_2(k) \to 1.$$

We have $H^2(\mathrm{SL}_2(k), Z) = H^2(\mathrm{SL}_2(k), k) = 0$ by [Jan87, Proposition II.4.13], so such an extension must be split. But a splitting would yield a Levi decomposition for Γ_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 1; 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 $\mathscr{Z}(k)$.

4. UNIPOTENT RADICALS AND REPRESENTATIONS

Let A be a linear algebraic group over k, and let R denote its unipotent radical. If (ρ, 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 [Spr98, Theorem 6.3.1]). This implies that there is a filtration of V by A-subrepresentations

$$V = \mathcal{R}^0 V \supset \mathcal{R}^1 V \supset \mathcal{R}^2 V \supset \cdots \supset \mathcal{R}^n V = 0 \tag{7}$$

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 $\mathrm{SL}_2(k)$ modules and the simple Γ_n-modules; for $a \geq 0$, there is thus a simple Γ_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 [Jan87, 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 Γ_n module V.

5. A FAITHFUL G-REPRESENTATION

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

Lemma 7. *Let (ρ, V) be a rational finite dimensional G-representation. Then ρ 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) $u = \rho(\mathscr{Z}(1)) \neq 1_V$.*

Proof. The necessity of conditions (i) and (ii) is clear, so suppose these conditions hold and let K be the kernel of ρ. Let $\mathrm{gr}(V)$ denote the associated graded space for any filtration as in (7). Then $\mathrm{gr}(V)$ is a module for $\Gamma_2/R = \mathrm{SL}_2(k)$. Condition (i) implies that $\mathrm{gr}(V)$ is an abstractly faithful representation of $\mathrm{SL}_2(k)$. Thus $\ker\rho$ is contained in R. Now (ii) together with Lemma 4 imply that $\ker\rho = 1$ as desired. □

Theorem 8. *G has an abstractly faithful representation (ρ, V) with $\dim V = p + 3$.*

Proof. Since G acts as a group of automorphisms on the 4 dimensional affine k-variety $W_2 \oplus W_2$, there is a representation ρ of G on the coordinate ring $\mathscr{A} = k[W_2 \oplus W_2]$ given by $(\rho(g)f)(w) = f(g^{-1}w)$ for $g \in G, f \in \mathscr{A}, w \in W_2 \oplus W_2$. If we denote by A_0 and A_1 the coordinate functions on $W_2 \oplus 0$, and by B_0 and B_1 those on $0 \oplus W_2$, then $\mathscr{A}$ identifies with the polynomial ring $k[A_0, A_1, B_0, B_1]$.

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

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

Since G acts "W_2-linearly" on $W_2 \oplus W_2$, $\lambda(k^\times)$ centralizes $\rho(G)$; thus each $\mathscr{A}_\nu$ is a G-subrepresentation of $\mathscr{A}$. We consider the G-representation $(\rho_p, \mathscr{A}_p)$. One sees that $\mathscr{A}_p$ is spanned by all $A_0^i B_0^j$ with $i + j = p$ and $i, j \geq 0$, together with A_1 and B_1. Thus $\dim \mathscr{A}_p = p + 3$.

Using (1), one checks for each $s \in k$ that

$$\rho_p(\mathscr{Z}(s))A_1 = A_1 + sA_0^p,$$

so that $\rho_p(\mathscr{Z}(1)) \neq 1$. Since A_1 has T-weight p, $\mathscr{A}_p$ is an abstractly faithful representation of T; thus the lemma shows that $(\rho_p, \mathscr{A}_p)$ is an abstractly faithful G-representation. □

Remarks 9.
(a) It is straightforward to see that $(\rho_p, \mathscr{A}_p)$ 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 ρ_p is defined over the prime field $\mathbf{F}_p$. In particular, the finite group $\mathrm{SL}_2(\mathbf{Z}/p^2\mathbf{Z})$ has a faithful representation on a $p + 3$ dimensional $\mathbf{F}_p$-vector space. More generally, the finite group $\mathrm{SL}_2(W_2(\mathbf{F}_q))$ has

a faithful representation on a $p+3$ dimensional $\mathbf{F}_q$-vector space for each $q = p^r$).

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

6. ALGEBRAS OF DISTRIBUTIONS

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

The algebra structure of $\mathrm{Dist}(H)$ is determined by the comultiplication Δ of $k[H]$; the product of $\mu, \nu \in \mathrm{Dist}(H)$ 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:

(8) If H is Abelian, then $\mathrm{Dist}(H)$ is a commutative k-algebra.

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

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

$$\Delta_V : V \to V \otimes_k k[W];$$

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 $\psi_{i,j} \in \mathrm{End}_k(V)$.

The W_2-module (ρ, V) becomes a $\mathrm{Dist}(W_2)$-module by the recipe give in [Jan87, I.7.11]. A look at that recipe shows that the basis elements $\gamma_{i,j} \in \mathrm{Dist}(W_2)$ 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

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

identically in a, b; thus $\psi_{0,0} = 1_V$ and $\psi_{i,j}^{p^2} = 0$ if $i > 0$ or $j > 0$.

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

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

Fix a weight vector $v \in V_\lambda$. Then

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

where the $\psi_{i,j}$ are determined as before by the comodule map for the W_2-module V. A look at (3) shows that $\psi_{i,j}(v) \in V_{\lambda+2i+2pj}$. It follows that $\psi_{i,j} \in \mathrm{End}_k(V)_{2i+2pj}$.

Proposition 10. *Let (ρ, V) be a representation of $H = \mathscr{X}_2(W_2) \rtimes T$. Suppose that $\rho(\mathscr{X}_2(0,1)) \neq 1_V$. Then T has at least $p+1$ distinct weights on V. More precisely, there are weights $s \in \mathbf{Z}_{>0}$ and $\lambda \in \mathbf{Z}$ such that $V_{\lambda+2sj} \neq 0$ for $0 \leq j \leq p$.*

Proof. We have $\mathscr{X}_2(0,1) = \mathscr{X}_2(1,0)^p$. With notation as above, our hypothesis means that

$$1_V \neq \rho(\mathscr{X}_2(1,0))^p = \left(\sum_{i \geq 0} \psi_{i,0}\right)^p = \sum_{i \geq 0} \psi_{i,0}^p.$$

Thus there is some $s > 0$ for which $\psi_{s,0}^p \neq 0$. Write $\psi = \psi_{s,0}$. Recall that ψ has T-weight $2s$. We may find a weight $\lambda \in \mathbf{Z}$ 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 $H_n = \mathscr{X}_n(W_n) \cdot T \leq \Gamma_n$ may be proved by the same method: if (ρ, V) is an H_n module such that $\rho(\mathscr{X}_n(0, \ldots, 0, 1)) \neq 1$, then there are weights $s \in \mathbf{Z}_{>0}$ and $\lambda \in \mathbf{Z}$ 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 $\Gamma_2 = \mathrm{SL}_2(W_2)$, and $\mathscr{X} = \mathscr{X}_2$.

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

Proof. We may find $\nu \in \mathbf{Z}$ and a T-weight vector $v \in V_\nu$ for which

$$\rho(\mathscr{Z}(1))v \neq v.$$

There are uniquely determined vectors $v = v_0, v_1, \ldots, v_N \in V$ with $\rho(\mathscr{Z}(s))v = \sum_{i=0}^N s^i v_i$ and $v_N \neq 0$. Since $\rho(\mathscr{Z}(1))v \neq v$, we must have $N > 1$. Since $\rho(\mathscr{Z}(1))v_N = v_N$, the vectors v and v_N are linearly independent. By (6) we have $v_N \in V_\nu$, whence the lemma. □

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

Proof. Let (ρ, V) be a G-representation for which $\rho(\mathscr{Z}(1)) \neq 1_V$. By Lemma 4, we have $\rho(\mathscr{X}(0,1)) \neq 1_V$. According to Proposition 10 we may find $\lambda \in \mathbf{Z}$ and $s > 0$ such that $V_{\lambda+2sj} \neq 0$ for $0 \leq j \leq p$. Since by Lemma 12 there must be some $\mu \in \mathbf{Z}$ 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_μ, 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 $\mathrm{SL}_2(k)$ module, we have $\dim V_\gamma = \dim V_{-\gamma}$ for all weights $\gamma \in \mathbf{Z}$. Since V_μ 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 $\mathrm{SL}_2(k)$ 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 0 is not a weight of V; this gives our contradiction when $p > 2$.

So we may suppose that $p = 2$, that $\dim V_{\pm 2^r} = 1$, and that $\dim V_0 = 2$. 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 $\rho(\mathscr{X}(0,1)) \neq 1$, a look at the proof of Theorem 10 shows that $V_{\pm 2^r} \cap V^R = 0$. Moreover, since $\rho(\mathscr{Z}(1)) \neq 1$, Lemma 12 shows that $V_0 \not\subset V^R$.

Next, we claim that $\mathrm{soc}(V/V^R)$ 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 $\mathscr{Z}(1)$ acts non-trivially. But $\mathscr{X}(1,0)$ must act trivially on such a module, contrary to Lemma 4.

It now follows that $\mathrm{soc}(V/V^R) = L(1)^{[r]}$. But then the inverse image W in V of $\mathrm{soc}(V/V^R)$ is a G-submodule of V containing $V_{\pm 2^r}$. Moreover, $\dim W = 3$, $\mathscr{X}(0,1)$ acts non-trivially on W, while $\mathscr{Z}(1)$ must act trivially on W. Thus $\ker \rho \cap R$ is precisely $Z = \{\mathscr{Z}(t) \mid t \in k\}$; see Remark 6. Let $\mathscr{Y} : \mathrm{W}_2 \to \Gamma_2$ be the map

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

Since $\mathscr{Y}(0,1) \notin R$, we have $\rho(\mathscr{Y}(0,1)) \neq 1$. Moreover, we know that $\rho(\mathscr{Y}(0,1))$ commutes with $\rho(\mathscr{X}(0,1))$. But the fixed point space of $\rho(\mathscr{X}(0,1))$ on W is precisely $W_0 \oplus W_2$, which is not stable under $\rho(\mathscr{Y}(0,1))$ by (the proof of) Proposition 10. This gives the desired contradiction when $p = 2$. □

Corollary 14. *Suppose that (ρ, 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 $\mathscr{Z}(1)$, 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 Γ_2

Let $\mathfrak{g} = \mathrm{Lie}(\Gamma_2)$. There is an exact sequence of p-Lie algebras and of Γ_2-modules

$$0 \to \mathrm{Lie}(R) \to \mathfrak{g} \to \mathfrak{sl}_2(k) \to 0. \tag{9}$$

Lemma 15. *Suppose that $p > 2$. Then R acts trivially on $\mathfrak{g}$. In particular,* (9) *is an exact sequence of $\mathrm{SL}_2(k)$-modules.*

Proof. Since the adjoint module for $\mathrm{SL}_2(k)$ is simple when $p > 2$, it suffices by Lemma 4 to show that $\mathrm{Ad}(\mathscr{X}(0,1)) = 1$. Note that the weights of T on $\mathfrak{g}$ are ± 2, $\pm 2p$, and 0. Since $p > 2$, Proposition 10 implies that $\mathscr{X}(0,1)$ acts trivially on $\mathfrak{g}$ as desired. □

The Abelian Lie algebra $\mathrm{Lie}(\mathrm{W}_2)$ 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 $(t \mapsto (0,t)) : k \to \mathrm{W}_2$. Write $X = d\mathscr{X}(Y)$. Then $X \notin \mathrm{Lie}(R)$ and $X^{[p]} \in \mathrm{Lie}(R)$.

Proposition 16.
1. *If $(d\lambda, V)$ is a restricted representation of the p-Lie algebra $\mathfrak{g}$, then $\ker d\lambda \cap \mathrm{Lie}(R) = 0$ if and only if $(d\lambda)(Z) \neq 0$ where $Z = d\mathscr{Z}(1)$.*
2. *Let $p > 2$. Then* (9) *is split as a sequence of Γ_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 $\mathrm{SL}_2(k)$. Note that (9) 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 [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 $\mathfrak{g}/\operatorname{Lie}(R)$ as a Γ_2-module, and $X^{[p]}$ is a generator for $\operatorname{Lie}(R)$ as a Γ_2-module, so the claim follows from (2). □

Corollary 17. *Consider the Γ_2 representation $(\rho_p, \mathscr{A}_p)$ of §5.*

1. *If $p > 2$, then $(d\rho_p, \mathscr{A}_p)$ is a faithful representation of $\mathfrak{g}$.*
2. *If $p = 2$, then $\ker d\rho_2 = \operatorname{Lie}(T)$ is 1-dimensional.*

Proof. With notations as before, using (1) one sees that

$$\rho_p(\mathscr{X}(0, s))A_1 = A_1 + sB_0^p$$

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 $Z = d\mathscr{X}(1)$ 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 $\ker d\rho_p \cap \operatorname{Lie}(R) = 0$ for all p. When $p = 2$, note that $\operatorname{Lie}(T)$ indeed acts trivially; see Remark 9 (a). The corollary now follows. □

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. Let C be a finite cyclic group of order relatively prime to p, and suppose that $\rho : C \to \operatorname{Aut}_{k\text{-alg}}(A)$ 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 $X = \operatorname{Hom}(C, k^\times)$ 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 μ is injective as a homomorphism. If (ρ, 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 $\mathfrak{m} = (z)$ for the maximal ideal of A.

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

Proof. Since C acts by algebra automorphisms, the ideal $\mathfrak{m}^i$ is C-invariant for each $i \geq 1$. Since the C representation $(\rho, \mathfrak{m})$ is semisimple, the subrepresentation $\mathfrak{m}^2$ has a complement $k \cdot f$ for some $0 \neq f \in \mathfrak{m}$. Thus there is $\mu \in X$ such that $\rho(c)f = \mu(c)f$ for each $c \in C$, and since $f \notin \mathfrak{m}^2$, the image of f in $\mathfrak{m}/\mathfrak{m}^2$ is non-zero. It remains to argue that μ is a generator for X. Note that $1, f, f^2, \dots, f^{N-1}$ 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 (ρ, A) is a faithful representation, we see that μ must itself be a faithful representation of C, so that μ indeed generates X. □

9.2. Let V be a k-vector space of dimension $n \geq 2$. Let u be a regular unipotent element in $\mathrm{GL}(V)$; 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 $\mathfrak{gl}(V) = \mathrm{End}_k(V)$ 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, $f \in k[A]$ is a regular nilpotent element of $\mathfrak{gl}(V)$ if and only if $f \in \mathfrak{m} \setminus \mathfrak{m}^2$.

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 $X = \mathrm{Hom}(C, k^\times)$. Write C' for the centralizer in C of W, and let $X' = \{\mu \in X \mid \mu_{|C'} = 1\}$.

Proposition 19. *Let (ρ, V) be a faithful, finite dimensional H-representation, and suppose that $\rho(W)$ contains a regular unipotent element of $\mathrm{GL}(V)$. If $|C/C'| \geq \dim V$, then V_μ is 1 dimensional for each $\mu \in X$. Moreover, there is $\lambda \in X$ and a generator $\mu \in X'$ such that $V \simeq V_\lambda \oplus V_{\lambda+\mu} \oplus \cdots \oplus V_{\lambda+d\mu}$ 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 $\mathrm{End}_k(V)$ is $k[u]$. For each $c \in C$ we have, $\rho(c)u\rho(c)^{-1} \in \rho(W) \subset k[u]$ 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 18, there is a generator $\mu \in X' = X(C/C')$ and (in view of 9.2) a regular nilpotent element $A \in (\mathfrak{gl}(V))_\mu$.

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 μ has order $|C/C'| > d$, each of these subspaces has dimension 1. The proposition follows. $\square$

9.4. Fix a p-power $q = p^a$, and let $\mathbf{F}_q$ be the field with q elements. The group Γ_n, and the homomorphisms $\phi : \mathbf{G}_m \to \Gamma_n$ and $\mathscr{X}_n : W_n \to \Gamma_n$ are defined over $\mathbf{F}_q$.

Let $n = 2$, and let $C, W \leq \Gamma_2(\mathbf{F}_q) = \mathrm{SL}_2(W_2(\mathbf{F}_q))$ be respectively the image under ϕ of $\mathbf{G}_m(\mathbf{F}_q) \simeq \mathbf{F}_q^\times$, and the image under $\mathscr{X}_2$ of $W_2(\mathbf{F}_q)$. 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 $\Gamma_2(\mathbf{F}_q)$ is $p + 3$.*

Proof. That $\Gamma = \Gamma_2(\mathbf{F}_q)$ has a faithful representation of dimension $p + 3$ follows from Remark 9(b).

We now suppose that (ρ, V) is a faithful representation of Γ with $\dim V \leq p + 2$ and deduce a contradiction. Since the element $\mathscr{X}_2(1, 0)$ of $\Gamma_2(\mathbf{F}_q)$ 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 $|C/C'| = \dfrac{q-1}{2} \geq p + 1 = \dim V$. An application of Proposition 19 for the subgroups $C, W < \Gamma$ therefore shows that the spaces V_μ with $\mu \in X(C)$ are all 1-dimensional. Lemma 12 now shows that the element $\mathscr{Z}(1) \in \Gamma$ must act trivially; this contradicts our assumption that (ρ, V) is faithful.

Finally, suppose that $\dim V = p + 2$. Let H be the subgroup of Γ 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 Γ-representation (ρ, V) may be identified with simple representations of the group $\mathrm{SL}_2(\mathbf{F}_q) = \Gamma/R(\mathbf{F}_q)$. Thanks to a theorem of Curtis ([Ste68, Theorem 43]) the semisimplification of (ρ, V) is the restriction to $\mathrm{SL}_2(\mathbf{F}_q)$ of a semisimple rational $\mathrm{SL}_2(k)$ module (ψ, 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 $A = \mathbf{Z}[i]$ 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 $a, b \in \mathbf{Z}$. Denoting by $\mathfrak{P}$ the ideal $(a+bi)A$, one has $A/\mathfrak{P} \simeq \mathbf{F}_{p^2}$. Then $A/\mathfrak{P}^2 \simeq W_2(\mathbf{F}_{p^2})$, so the minimal dimension of a faithful p-modular representation of $\mathrm{SL}_2(A/\mathfrak{P}^2)$ 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 Michiel 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), 34–76.

E-mail address: mcninchg@member.ams.org