PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 2, October 1992

VARIETIES ATTACHED TO AN $SL_2(2^k)$-MODULE

GEOFFREY MASON

(Communicated by Warren J. Wong)

ABSTRACT. Let $G_k = SL_2(2^k)$ and V be an FG_k-module with F a field containing $GF(2^k)$. We show that V is irreducible if and only if there is a subgroup U_0 contained in a 2-Sylow of G_k such that V affords the regular representation of U_0. We further show how to construct a variety, defined over an algebraic closure of $GF(2)$, whose $GF(2^k)$-rational points parameterize those conjugacy classes of subgroups of G_k, isomorphic to U_0, that are not represented regularly on V.

1. INTRODUCTION

We start with an outrageous result. Consider the recurrence relation

$$N_k = 2^k + 2 + N_{k-1} - 2N_{k-2} \tag{1.1}$$

for $k \geq 1$, with initial values

$$N_1 = 0, \qquad N_2 = 14. \tag{1.2}$$

Explicitly, we have

$$N_k = 1 + 2^k + 3k \sum_{n=[k+1/2]}^{k} (-1)^{n+k+1} n^{-1} \binom{n}{k-n} 2^{k-n}. \tag{1.3}$$

The first few values of N_k are as follows: 0, 14, 24, 14, 0, 38, 168, 350, 528, ..., which illustrates the fact that N_k is periodic (mod 168) with period of length 6. Therefore, the number F_k defined in (1.4) is an integer; namely, let $k \equiv r \pmod 6$ with $1 \leq r \leq 6$ and set

$$F_k = \begin{cases} (N_k - N_r)/168, & r \not\equiv 0 \pmod 3, \\ 1 + (N_k - N_r)/168, & r \equiv 0 \pmod 3. \end{cases} \tag{1.4}$$

The first few values of F_k are 0, 0, 1, 0, 0, 1, 1, 2, 4, ... The outrageous theorem gives a geometric interpretation of these numbers.

Received by the editors November 20, 1990 and, in revised form, March 28, 1991; presented during Fall, 1990, at the M.S.R.I., Berkeley Conference on Representation Theory.

1991 *Mathematics Subject Classification.* Primary 20G05, 14M99.

Research supported by grants from the NSF, including DMS-8505550 at MSRI, Berkeley.

0002-9939/92 $1.00 + $.25 per page

Theorem 1. *Let* $G = \mathrm{SL}_2(2^k)$, M *the natural* $\mathrm{GF}(2^k)G$*-module, and* φ *the Frobenius automorphism of* $\mathrm{GF}(2^k)$, *and set*

$$V = M \otimes M^{\varphi} \otimes M^{\varphi^3}. \tag{1.5}$$

Then F_k *is the number of conjugacy classes of subgroups* $E \leq G$ *such that*

(i) $|E| = 8$;
(ii) *the restriction of* V *to* E *is not the regular representation.*

Behind the proof of Theorem 1 lies a simple principle. To describe it, let k be an algebraic closure of $\mathrm{GF}(2)$, $\Gamma = \mathrm{SL}_2(k)$, and M the natural 2-dimensional $k\Gamma$-module. For an integer $n \geq 1$ with 2-adic expansion $n = 2^{i_1} + 2^{i_2} + \cdots$, $0 \leq i_1 < i_2 < \cdots$, we let

$$V_n = M^{\varphi^{i_1}} \otimes M^{\varphi^{i_2}} \otimes \cdots \tag{1.6}$$

be the corresponding tensor product module (φ again being Frobenius). For a finite field $K \subseteq k$ we get an $\mathrm{SL}_2(K)$-module by restriction.

Theorem 2. *Let* $n \geq 1$ *and assume that* $\dim_k V_n = 2^r$. *Then there is a* k*-variety* $\tilde{X}_n$ *whose* K*-rational points parameterize the conjugacy classes of subgroups* $E \leq \mathrm{SL}_2(K)$ *such that*

(i) $|E| = 2^r$;
(ii) *the restriction of* V_n *to* E *is not the regular representation.*

Thus Theorem 1 is concerned with the case $n = 11$ and amounts to a determination of the zeta-function of $\tilde{X}_{11}$.

$\tilde{X}_n$ itself is only interesting if $r \geq 3$, and we shall see that if n is of the form $n = (2^r - 1)2^t$ then $\tilde{X}_n = \varnothing$. This says that if we take *consecutive* powers of Frobenius in (1.6) then *every* subgroup of $\mathrm{SL}_2(K)$ of order $\dim V_n$ is free on V_n. On the other hand if n is *not* of the form $(2^m - 1)2^t$ then $\tilde{X}_n \neq \varnothing$, so for some K there *is* a subgroup of order $\dim V_n$ that is not free on V_n.

I believe that the study of these varieties may lead to some interesting qualitative results concerning the modules V_n and the existence of certain subgroups of $\mathrm{SL}_2(K)$ acting freely on V_n—the remarks in the previous paragraphs are particularly simple illustrations of this—but for now at least the algebraic geometry has the better of me.

I also include below a result that is naturally related to these issues, but quite unrelated in its method of proof.

Theorem 3. *With the previous notation, let* W *be an arbitrary* $k\,\mathrm{SL}_2(K)$*-module. The following are equivalent for* $|K| \geq 4$:

(i) W *is irreducible*;
(ii) *there is a 2-group* $E \leq \mathrm{SL}_2(K)$ *such that the restriction of* W *to* E *is the regular representation*

The implication (i) $\Rightarrow$ (ii) is well known and easy to prove, but the converse seems not to have been noticed hitherto.

The idea of attaching varieties to nonfree actions of elementary abelian subgroups as in Theorems 1 and 2 is very reminiscent of ideas of Carlson (cf. [2]), but I make no use of his ideas here. The present methods will be seen

to be completely elementary, bordering on the trivial in fact, and it remains of interest to try and forge more significant ties with Carlson's point of view.

2. Proof of Theorem 3

We let $K = \mathrm{GF}(2^k)$ with $k \geq 2$, $G = \mathrm{SL}_2(K)$, and W be an (absolutely) irreducible KG-module. We remind the reader of the implication (i) $\Rightarrow$ (ii). So if W is irreducible it has a tensor decomposition

$$W = M^{\sigma_1} \otimes M^{\sigma_2} \otimes \cdots \otimes M^{\sigma_r} \tag{2.1}$$

with M the natural KG-module of dimension 2. We use induction on r, the result being clear if $r = 0$ or 1. Thus set $W_1 = M^{\sigma_1} \otimes \cdots \otimes M^{\sigma_{r-1}}$ and let $E_1 \leq U \leq G$ satisfy $W_1|E_1 \cong KE_1$, where U is a 2-Sylow subgroup of G.

As $\dim W = 2 \dim W_1 = 2|E_1|$ we get $\dim W^{E_1} = 2$ (W^{E_1} being the fixed-point subspace of E_1 on W). But as W is irreducible it is well known that W^U has dimension one, so there is $u \in U - E_1$ with $W^{\langle E_1, u\rangle}$ having dimension one. Then $E = \langle E_1, u\rangle$ satisfies (ii) of Theorem 3, as required.

Now assume that W is a KG-module with $W|E \cong KE$ for some $E \leq U$. We set $|U : E| = 2^n$ and use induction on n.

Suppose first that $n = 0$, that is, $U = E$. Then W is a projective, indecomposable KG-module of dimension $|U|$, and by work of Alperin [1], we know that W is the Steinberg module and in particular is irreducible. Incidentally, this is where we use the condition $|K| \geq 4$.

For each Galois twist M^σ of M let us define

$$V_\sigma = M^\sigma \otimes W. \tag{2.2}$$

If there is $F \leq U$ with $V_\sigma|F \cong KF$ then V_σ is irreducible by induction, whence so also is W. So without loss there is no such F.

As $V_\sigma|E \cong KE \oplus KE$ we have $\dim V_\sigma^E = 2$, and by the last paragraph we also get $V_\sigma^E = V_\sigma^{E_1}$ for each $E \leq E_1 \leq U$, $|E_1 : E| = 2$. Thus $V_\sigma^E = V_\sigma^U$ is of dimension 2 for each $\sigma \in \mathrm{Gal}(K/GF(2))$. As each M^σ is self-dual as a KG-module, we get from (2.2) that $\dim \mathrm{Hom}_{KU}(M^\sigma, W) = 2$, and hence for each σ there is a U-submodule of W isomorphic to $M^\sigma|U$. Call such a U-submodule N_σ.

Next, as $W|E \cong KE$, $W^E = \mathrm{Soc}(W|E)$ is 1-dimensional and the second socle $S \leq W|E$, defined by $W^E \leq S$, $S/W^E = \mathrm{Soc}(W|E/W^E)$ satisfies $\dim_K S = r + 1$ where $|E| = 2^r$. Note that for each σ we have $N_\sigma \subseteq S$.

Let $\{x_1, \ldots, x_r\}$ be a set of generators of E contained in the generating set $\{x_1, \ldots, x_r, x_{r+1}, \ldots, x_k\}$ of U. As matrices operating on M we may suppose that

$$x_i = \begin{pmatrix} 1 & a_i \\ 0 & 1 \end{pmatrix}, \qquad a_i \in K,\ 1 \leq i \leq k, \tag{2.3}$$

with $\{a_1, \ldots, a_k\}$ linearly independent over $GF(2)$. Let $E_i = \langle x_1, \ldots, \hat{x}_i, \ldots, x_r\rangle$ be the hyperplane of E spanned by the generators x_i of E with the ith element omitted. If we set $W_i = W^{E_i}$, $Z = W^E$ then we have $S = \sum_i W_i$, and indeed

$$S/Z = \bigoplus_{i=1}^{r} W_i/Z. \tag{2.4}$$

Let $Z = Kz$ and $W_i = K\{z, w_i\}$. Each W_i admits U, and with respect to the indicated base x_i has a matrix representation as

$$x_i = \begin{pmatrix} 1 & t_{ij} \\ 0 & 1 \end{pmatrix} \quad \text{on } W_j, \quad 1 \le i \le k, \quad 1 \le j \le r. \tag{2.5}$$

As $N_\sigma \le S$ we may choose a K-base of N_σ of the form $\{z, \sum_{j=1}^r b_{j,\sigma} w_j\}$ as follows from (2.5). Then x_i is represented via

$$x_i = \begin{pmatrix} 1 & \sum_{j=1}^r b_{j,\sigma} t_{ij} \\ 0 & 1 \end{pmatrix} \quad \text{on } N_\sigma; \tag{2.6}$$

as this representation is equivalent to that on M^σ, we have equations of the following form: for some constant $q_\sigma \in K$,

$$\sum_{j=1}^r b_{j,\sigma} t_{ij} = q_\sigma \sigma(a_i), \qquad 1 \le i \le k. \tag{2.7}$$

By relabelling the $b_{j,\sigma}$ we may evidently take $q_\sigma = 1$, whence we get a matrix equation for each σ

$$T \begin{pmatrix} b_{1,\sigma} \\ \vdots \\ b_{r,\sigma} \end{pmatrix} = \begin{pmatrix} \sigma(a_1) \\ \vdots \\ \sigma(a_k) \end{pmatrix} \tag{2.8}$$

where $T = (t_{ij})$ is a $k \times r$ matrix.

Now as σ ranges over the elements of $\mathrm{Gal}(K/\mathrm{GF}(2))$, the columns on the right-hand side of (2.8) span the full column space K^k. This is because $a_1, \dots, a_k$ are GF(2)-independence and because of the linear independence of Galois automorphisms. As T is a $k \times r$ matrix, we must have $k = r$. Thus $E = U$, a case already dealt with.

Remark. Jon Alperin showed me a somewhat less computational approach to the above proof.

3. Proof of Theorem 2

We retain the notation of §2. The key to the kingdom is the following simple result.

Proposition 3.1. *Let W be the KG-module of dimension 2^r given by* (2.1) *(though W need not be assumed irreducible). Let $E \le U$ be a subgroup of order 2^r with generators $x_1, x_2, \dots, x_r$ that are represented on the natural module M as in* (2.3). *Then the following are equivalent*:

(a) *the restriction of W to E is the regular representation*;

(b) $$\det \begin{pmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \cdots & \sigma_1(a_r) \\ \vdots & \vdots & & \vdots \\ \sigma_r(a_1) & \sigma_r(a_2) & \cdots & \sigma_r(a_r) \end{pmatrix} \neq 0.$$

Proof. It is well known that (a) holds if and only if we have the inequality

$$[W, \underbrace{E, E, \dots, E}_{r}] \neq 0, \tag{3.1}$$

so we have to sort out the left-hand side of (3.1). It is spanned by elements of the form $[w, e_1, e_2, \dots, e_r]$ with $w \in W$ and $e_i \in E$. As such an expression is

GF(2)-linear in the e_i's, since $[w, e, e] = 0$ for $e \in E$, and since $[w, e, f] = [w, f, e]$ for $e, f \in E$, we see that the left-hand side of (3.1) is spanned by elements of the form

$$[w, x_1, x_2, \dots, x_r], \qquad w \in W. \tag{3.2}$$

If we start with the standard base $\{\binom{1}{0}, \binom{0}{1}\}$ for M, we can represent the 'tensor product' base for W as the ordered set

$$\left\{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \end{pmatrix}\right\}$$

with the appropriate G-action. Let us set $R = \{1, 2, \dots, r\}$ and denote by w_J for $J \subseteq R$ the element of the indicated base for W with a 1 in the lower row in exactly the positions determined by J. Then one calculates quite readily that

$$[w_J, x_i] = \sum_{\substack{J' \subseteq R \\ |J'|<|J|}} a_{J'} w_{J'}, \qquad a_{J'} \in K. \tag{3.3}$$

From this we see that $[w_J, x_1, \dots, x_r] = 0$ whenever $|J| < r$, whence from (3.2) we conclude that

$$[W, \underbrace{E, E, \dots, E}_{r}] = K[w_R, x_1, \dots, x_r]. \tag{3.4}$$

Finally, since $w_R = \left(\begin{smallmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \end{smallmatrix}\right)$, one can prove easily by induction and (3.3) that for $1 \le m \le r$,

$$\begin{aligned}[w_R, x_1, \dots, x_m] = &\sum_{\{j_1, \dots, j_m\}} \sigma_{j_1}(a_1) \cdots \sigma_{j_m}(a_m) w_{R-\{j_1, \dots, j_m\}} \\ &+ \sum_{\substack{J \subseteq R \\ |J|<r-m}} b_J w_J\end{aligned} \tag{3.5}$$

where the first sum on the right-hand side runs over all m-element subsets $\{j_1, \dots, j_m\}$ of R. Setting $m = r$ yields

$$[w_R, x_1, \dots, x_r] = d w_\varnothing \tag{3.6}$$

where d is the determinant of (b) in the statement of the proposition. The desired result is then a consequence of (3.6) and (3.4).

Let us now assume that the automorphism $\sigma_i \in \mathrm{Gal}(K/\mathrm{GF}(2))$ satisfies $\sigma_i = \varphi^{n_i}$. Then of course $\sigma_i(a_j) = a_j^{2^{n_i}}$. So if we consider the determinantal equation

$$D \equiv \det \begin{pmatrix} X_1^{2^{n_1}} & X_2^{2^{n_1}} & \cdots & X_r^{2^{n_1}} \\ \vdots & & & \\ X_1^{2^{n_r}} & X_2^{2^{n_r}} & \cdots & X_r^{2^{n_r}} \end{pmatrix} = 0 \tag{3.7}$$

as defining an affine variety over K, say, then Proposition 3.1 says that $W|E \cong KE$ precisely when $(a_1, \dots, a_r)$ is *not* a point on the variety.

Turned around, then, the affine K-variety $D = 0$ classifies r-ruples $(a_1, \dots, a_r)$ such that the subgroup $\langle \left(\begin{smallmatrix} 1 & a_1 \\ 0 & 1 \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} 1 & a_r \\ 0 & 1 \end{smallmatrix}\right) \rangle$ of G is *not* represented regularly on W.

Since D is homogeneous, we may also think of $D = 0$ as defining a projective variety. Since

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & \lambda^2 a \\ 0 & 1 \end{pmatrix},$$

it follows that the projective variety $D = 0$ classifies r-tuples $(a_1, \ldots, a_r)$ such that the conjugacy class of subgroups of G determined by $\langle \left(\begin{smallmatrix} 1 & a_1 \\ 0 & 1 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 1 & a_r \\ 0 & 1 \end{smallmatrix}\right) \rangle$ are not represented regularly on W. (Technically, this uses Sylow's theorem, too.)

Next we consider some obvious factors of the determinant $D = D(X_1, \ldots, X_r)$ of (3.7). We may assume that $0 \leq n_1 \leq n_2 \leq \cdots \leq n_r$, whence because we are in characteristic 2, D is clearly the 2^{n_1}th power of another matrix. So there is little loss in assuming that $n_1 = 0$, and since it is really the only interesting case we shall further take

$$0 = n_1 < n_2 < \cdots < n_r. \tag{3.8}$$

In this case we factor D as $D = LP$ with

$$L = \prod_{t=1}^{r} \prod (X_{i_1} + \cdots + X_{i_t}) \tag{3.9}$$

where the inner product runs over all t-tuples of distinct indices $1 \leq i_1 < i_2 < \cdots < i_t \leq r$. Both L and P are homogeneous, and the projective variety defined by

$$Y : P = 0 \tag{3.10}$$

will be of interest. Now a point $(a_1, \ldots, a_r)$ in $D = 0$ lies in the variety $L = 0$ precisely when $\langle \left(\begin{smallmatrix} 1 & a_r \\ 0 & 1 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 1 & a_r \\ 0 & 1 \end{smallmatrix}\right) \rangle$ has order less than 2^r, for both conditions are equivalent to the existence of a nontrivial GF(2)-linear relation amongst the a_i's. Thus if we set

$$X = Y - \{L = 0\} \tag{3.11}$$

then X is a quasi-projective variety and $(a_1, \ldots, a_r) \in X$ corresponds to conjugacy classes of subgroups in G determined by $\langle \left(\begin{smallmatrix} 1 & a_1 \\ 0 & 1 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 1 & a_r \\ 0 & 1 \end{smallmatrix}\right) \rangle$ that (i) have order 2^r and (ii) are not represented regularly on W.

Finally, let $S = \mathrm{SL}_r(2)$. It acts in the natural manner on $\mathbb{P}^{r-1}(K)$, and this action preserves both Y and $\{L = 0\}$. So S also acts on X. Now it is clear that if $(a_1, \ldots, a_r)$ and $(a_1', \ldots, a_r')$ are two points of X then the corresponding subgroups

$$\left\langle \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & a_r \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & a_1' \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & a_r' \\ 0 & 1 \end{pmatrix} \right\rangle$$

coincide if and only if some element of S maps $(a_1, \ldots, a_r)$ to $(a_1', \ldots, a_r')$. Thus if we set

$$\tilde{X} = X/S \tag{3.12}$$

then $\tilde{X}$ is a variety over K that classifies subgroups $E \subseteq G$ satisfying (i) and (ii) of Theorem 2.

From the foregoing it should be evident that if we start with $\Gamma = \mathrm{SL}_2(k)$ instead of $G = \mathrm{SL}_2(K)$ then the k-variety defined by (3.12) is such that its

K-rational points are just those that we have been considering. So the variety $\tilde{X}_n$ of Theorem 2 is just $\tilde{X} = X/S$ regarded as a variety over k.

4. Proof of Theorem 1 and other comments

Suppose first that we take the integer n in Theorem 2 to be of the form $n = 2^t(2^r - 1)$. Then the module V_n of (1.6) becomes

$$V_n = M^{\varphi^t} \otimes M^{\varphi^{t+1}} \otimes \cdots \otimes M^{\varphi^{t+r-1}}. \tag{4.1}$$

Then

$$D = \det \begin{pmatrix} X_1 & X_2 & \cdots & X_r \\ X_1^2 & X_2^2 & \cdots & X_r^2 \\ \vdots & & & \\ X_1^{2^{r-1}} & X_2^{2^{r-1}} & \cdots & X_r^{2^{r-1}} \end{pmatrix}^{2^t},$$

i.e., $D = L^{2^t}$ where L is given by (3.9). Thus both X and $\tilde{X}_n$ are empty. This proves the assertion following the statement of Theorem 2, namely,

Lemma 4.1. *If $n = 2^t(2^r - 1)$ then $\tilde{X}_n = \varnothing$. In other words, if V_n is of the 'consecutive Frobenius type' exemplified by* (4.1) *then every subgroup of $SL_2(K)$ of order 2^r is represented regularly on V_n.*

Note that if n is *not* of this form then certainly P is not constant, so $\tilde{X}_n \neq \varnothing$.

The smallest integer n *not* of the form $2^t(2^r - 1)$, and for which $r \geq 3$, is $n = 11$. This case is thus completely covered by Theorem 1, which we now discuss.

We have in this case

$$D = \det \begin{pmatrix} X_1 & X_2 & X_3 \\ X_1^2 & X_2^2 & X_3^2 \\ X_1^8 & X_2^8 & X_3^8 \end{pmatrix} = LP,$$

$$L = X_1X_2X_3(X_1 + X_2)(X_1 + X_3)(X_2 + X_3)(X_1 + X_2 + X_3),$$

$$P = X_1^4 + X_2^4 + X_3^4 + X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2 + X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2.$$

One verifies that P defines a smooth projective curve in $\mathbb{P}^2(k)$ (i.e., there is no nonzero simultaneous solution of $P = 0$, $\partial P/\partial X_i = 0$, $1 \leq i \leq 3$).

As P has degree 4 it has genus $\binom{4-1}{2} = 3$; so if we let $Z(t)$ denote the zeta-function of the curve $P = 0$ over $GF(2)$, defined by

$$Z(t) = \exp\left\{\sum_{k=1}^{\infty} N_k' \frac{t^k}{k}\right\} \tag{4.2}$$

with $N_k' = \#$ of points of $GF(2^k)$, then one knows by the Weil conjectures for curves that the following hold:

(i) $Z(t) = Q(t)/(1 - t)(1 - 2t)$ with $Q(t)$ a polynomial of degree 6;
(ii) $Q(t) = \prod_{i=1}^{3}(1 - \alpha_i t)(1 - \overline{\alpha}_i t)$ with $|\alpha_i| = \sqrt{2}$;
(iii) $Z(1/2t) = Z(t)/4t^4$.

One finds by computation that the first three values of N_k' are the same as the first three values of N_k in (1.1), namely $N_1 = 0$, $N_2 = 14$, $N_3 = 24$.

This is enough to find that

$$Z(t) = (2t^2 - t + 1)^3/(1 - t)(1 - 2t). \tag{4.3}$$

From (4.3) one verifies that $N_k = N_k'$ for all k, so that (1.1)–(1.3) give the coefficients of $Z(t)$ defined by (4.2).

Finally, to establish Theorem 1 we must consider the map $X \to \tilde{X} = X/S$ where the notation is that of §3. In the present situation, $S = \mathrm{SL}_3(2)$ and X is the quasi-projective variety $\{P = 0\}\backslash\{L = 0\}$.

Now $\{P = 0\} \cap \{L = 0\}$ consists of 14 points that are permuted transitively by S, one of them being $(0, 1, \omega)$ where ω generates $\mathrm{GF}(4)^{\#}$.

Apart from this orbit, S has one other exceptional orbit (i.e., one of length less than $|S| = 168$) in its action on X. Namely, an orbit of length 24 corresponding essentially to eigenvectors of elements of order 7 in their action on the natural 3-dimensional k-module. So such points are rational over $\mathrm{GF}(8)$.

Now we see that F_k defined by (1.4) is the number of $\mathrm{GF}(2^k)$-rational points of $\tilde{X}$, and we are done.

Recently, in joint work with Jon Alperin, we have established analogues of Theorems 2 and 3 for $\mathrm{SL}_2(p^k)$, p any prime.

Acknowledgment

We would like to thank Irving Kaplansky, the Director of the MSRI, for providing such a stimulating environment in which to work, and Jon Alperin for useful discussions.

References

1. J. Alperin, *Projective methods for* $\mathrm{SL}(2, 2^n)$, J. Pure Appl. Algebra **15** (1979), 219–234.
2. J. F. Carlson, *Varieties for modules*, Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, RI, 1987.

Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, California 94720

Department of Mathematics, University of California, Santa Cruz, California 95064