ELSEVIER

Journal of Pure and Applied Algebra 112 (1996) 1-12

JOURNAL OF PURE AND APPLIED ALGEBRA

2-Dimensional vector invariants of parabolic subgroups of $Gl_2(\mathbf{F}_p)$ over the field $\mathbf{F}_p$ [1]

H.E.A. Campbell *, I.P. Hughes

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

Communicated by J.D. stasheff; received 26 september 1990; revised 3 May 1994

Abstract

Given a group G acting on a finite dimensional vector space V over any field $\mathbf{k}$, we ask for the structure of the ring of invariants of the diagonal action of the group on the symmetric algebra of m copies of V, the so-called m-dimensional vector invariants of G. In this paper we use elementary techniques to determine the structure of the 2-dimensional vector invariants of $Gl_2(\mathbf{F}_p), Sl_2(\mathbf{F}_p), U_2(\mathbf{F}_p)$ acting as usual on a vector space of dimension 2 over $\mathbf{F}_p$. We know that these rings of invariants are Cohen–Macaulay and we compute for each a free module basis over a suitably chosen homogeneous system of parameters.

1. Introduction

In this paper, we denote by R_m the polynomial algebra $\mathbf{F}_p[x_i, y_i;\ 1 \leq i \leq m]$ where the x_i and y_i are commuting indeterminates. For $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $Gl_2(\mathbf{F}_p)$ we define an action on R_m by the rule $g(x_i) = \alpha x_i + \gamma y_i$, $g(y_i) = \beta x_i + \delta y_i$, which defines an embedding of $Gl_2(\mathbf{F}_p)$ in $Gl_{2m}(\mathbf{F}_p)$. Then we extend this action to the whole of R_m in the natural multiplicative way.

We will denote by R_m^G the invariant subalgebra $\{a \in R_m \mid g(a) = a,\ \forall g \in G\}$ for G a subgroup of $Gl_{2m}(\mathbf{F}_p)$. In several invariant theory sources, including [14, pp. 23–24], the elements of this graded algebra are referred to as the m-dimensional vector invariants of G. This paper and others, for example [1, 2, 4, 10], illustrate the difficulties encountered in discussing the rings of invariants of groups whose orders are divisible

* Corresponding author. E-mail: hughesi@queensu.ca.

[1] This research is supported in part by the Natural Sciences and Engineering Research Council of Canada.

SSDI 0022-4049(95)00128-X

by the characteristic of the underlying ground field. If the characteristic of the field is prime to the order of the group, then invariant theory in general closely resembles the characteristic zero case (for example, see [12, Section 7, p. 504]) and seems to be much simpler, if not yet entirely understood, see [13].

We denote by G the general linear group $Gl_2(\mathbf{F}_p)$, by S the special linear group $Sl_2(\mathbf{F}_p)$, by $U = U_2(\mathbf{F}_p)$ the upper triangular group and by P the upper triangular p-Sylow subgroup (all elements of P have 1's on the main diagonal). The order of G is $(p^2-1)(p^2-p)$, the order of S is $p(p^2-1)$, the order of U is $p(p-1)$ and the order of P is p.

In [1] we prove a conjecture of Richman [10] yielding a set of algebra generators for R_m^P in the case $m > 2$ and we also prove that these rings of invariants are not Cohen–Macaulay. The paper [10] has a proof of the case $m = 2$ and it also refers to a (different) proof of ours for this case. We give our proof here in Section 2: it relies on a key technical result from [2, Proposition 3.1] which we quote here as Proposition 2.1. In particular, R_2^P is Cohen–Macaulay, and so all the bigger groups under discussion in this paper have a Cohen–Macaulay ring of invariants by [5, Theorem 1]. We use this result to compute the 2-dimensional vector invariants of the group $U = U_2(\mathbf{F}_p)$ and of the group $S = Sl_2(\mathbf{F}_p)$. It is this latter group that occupies most of our attention. We have discovered that our result for the group S is due to Krathwohl [8]. Finally we compute the 2-dimensional vector invariants of the group $G = Gl_2(\mathbf{F}_p)$.

As we work our way through the sequence of groups $P \subset U \subset S \subset G$ we use the trace of the subgroup in the larger group, that is, we average over a set of right coset representatives, see Remark 3.1: this is successful because P is a p-Sylow subgroup of each of U, S and G. This is how [5, Theorem 1] is proved, for example.

It is interesting to contrast our methods for the group S with those of Krathwohl. He guesses at a suitable set of generators and proceeds to prove that any invariant admits an expression in the given set of generators. In our case, we use the fact that this ring of invariants is Cohen–Macaulay. Guided by calculations with the traces we can guess at a free basis over a suitable homogeneous system of parameters. However, the proof that our alleged basis really is a basis is quite lengthy and involves some messy computations. Our techniques are elementary.

2. 2-Dimensional vector invariants of P recalled

We have described embeddings of P, U, S and G into $Gl_4(\mathbf{F}_p)$. We may also embed the groups $P \times P = P^2$, U^2, and G^2 into $Gl_4(\mathbf{F}_p)$ by forming the 4×4 matrix

$$\begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix},$$

for g and h in P, U, or G.

It is not hard, see [9, Theorem 6.4, p. 328] for example, to see that $R_2^{P^2} = \mathbf{F}_p[x_1, x_2, z_1, z_2]$, where

$$z_1 = y_1^p - x_1^{p-1}y_1 \quad \text{and} \quad z_2 = y_2^p - x_2^{p-1}y_2,$$

and so P^2 has a polynomial ring of invariants.

The present example led us to the following result, see [2, Proposition 3.1].

Proposition 2.1. *We let A denote an integral domain of characteristic p and we let K be a finite group of automorphisms of A. We take H to be a maximal proper subgroup of K and assume that $[K : H] \leq p$. We take k to be an element of K such that the group generated by H and k equals K. Assume that there is an element a of A such that $(k-1)(a) = b$ is an element of A^K, and that for every $c \in A^H$ there is an element $d \in A$, depending on c such that $(k-1)(c) = bd$. Then $A^H = A^K[a]$.*

Theorem 2.2. *If we denote $x_1y_2 - x_2y_1$ by u then*

$$R_2^P = \mathbf{F}_p[x_1, x_2, z_1, z_2][u] = \bigoplus_{i=0}^{p-1} R_2^{P^2} u^i,$$

and

$$u^p = (x_1^p z_2 - x_2^p z_1) + (x_1^{p-1}x_2^{p-1})u.$$

In particular, R_2^P is a hyper-surface.

Proof. We denote by g_i, $i = 1, 2$, the elements of P^2 defined by

$$g_i(x_j) = x_j, \quad j = 1, 2,$$
$$g_i(y_j) = y_j, \quad i \neq j,$$
$$g_i(y_i) = y_i + \varepsilon_i x_i, \quad \varepsilon_1 = 1, \ \varepsilon_2 = -1.$$

Then $(g_1 - 1)u = (g_2^{-1} - 1)u = x_1x_2$. As well, P^2 is the group generated by g_1 and P and P^2 is also generated by g_2 and P. Suppose $c \in R_2^P$. We recall that R_2^P is a unique factorization domain by [7, p. 166]. Now $(g_1 - 1)c = (g_2^{-1} - 1)c$ is divisible in R_2^P by both x_1 and x_2 and so by x_1x_2. So, by Proposition 2.1, $R_2^P = R_2^{P^2}[u]$ as required. The formula of the theorem is a straightforward computation. □

3. Getting ready

We observe that S^2 and G^2 have polynomial rings of invariants. That is, if we define

$$v_i = x_i z_i \quad \text{and} \quad w_i = x_i^{p(p-1)} + z_i^{p-1}$$

for $i = 1, 2$, then because $R_2^{S^2} = R_1^S \otimes R_1^S$ and $R_2^{G^2} = R_1^G \otimes R_1^G$ we have

$$R_2^{S^2} = \mathbf{F}_p[v_i, w_i \mid i = 1, 2] \quad \text{and} \quad R_2^{G^2} = \mathbf{F}_p[v_i^{p-1}, w_i \mid i = 1, 2],$$

according to the well-known result of Dickson [6]. Of course P, U and S are subgroups of $S^2 \subset G^2$ so R_2^P, R_2^U, and R_2^S are finitely generated modules over the polynomial algebras $R_2^{S^2}$ and $R_2^{G^2}$. In the language of commutative algebra, $\{v_i, w_i \mid i = 1,2\}$ is a homogeneous system of parameters for each of R_2^P, R_2^U, and R_2^S and $\{v_i^{p-1}, w_i \mid i = 1,2\}$ is also a homogeneous system of parameters for each of R_2^P, R_2^U, R_2^S, and R_2^G.

Proposition 3.1. (1) R_2^P *has rank* $p(p^2-1)$ *as a free module over* $R_2^{S^2}$.
(2) R_2^U *has rank* $p(p^2-1)(p+1)$ *as a free module over* $R_2^{S^2}$.
(3) R_2^S *has rank* $p(p^2-1)$ *as a free module over* $R_2^{S^2}$.
(4) R_2^S *has rank* $p(p^2-1)(p-1)^2$ *as a free module over* $R_2^{G^2}$.
(5) $R_2^{S^2}$ *has rank* $(p-1)^2$ *as a free module over* $R_2^{G^2}$.
(6) R_2^G *has rank* $(p^2-1)(p^2-p)$ *as a free module over* $R_2^{G^2}$.

Proof. By Theorem 2.2 R_2^P is a hyper-surface and hence Cohen–Macaulay. P is a p-Sylow subgroup for each of U, S and G so their respective rings of invariants R_2^U, R_2^S and R_2^G are also Cohen–Macaulay by [5, Theorem 1]. In other words, each ring of invariants is a free module of finite rank over the algebra generated by any homogeneous system of parameters [11, Theorem 2, p. IV-20]. Since $\{v_1, w_1, v_2, w_2\}$ is a homogeneous system of parameters for R_2^P, R_2^U, and R_2^S, we have that R_2^P, R_2^U and R_2^S are free $R_2^{S^2} = \mathbf{F}_p[v_i, w_i \mid i = 1,2]$-modules. Similarly, R_2^U, R_2^S, and R_2^G are free $R_2^{G^2} = \mathbf{F}_p[v_i^{p-1}, w_i \mid i = 1,2]$-modules.

Each of the ranks is as claimed because of a more general result. If R^H is known to be Cohen–Macaulay and H is a subgroup of K with R^K a polynomial ring, then R^H is a free module over R^K of rank $[K : H]$. This is not hard to see. We denote by $Q(R)$, $Q(R^H)$ and $Q(R^K)$ the quotient fields of the domains R, R^H and R^K respectively. We have that $Q(R)$ is a Galois extension of both $Q(R^H)$ and $Q(R^K)$ with Galois groups H and K respectively. Hence $Q(R^H)$ is an extension of $Q(R^K)$ of degree $[K : H]$. It is not difficult to see that any element of $Q(R^H)$ may be written as a/b for $a \in Q(R^H)$ and $b \in Q(R^K)$. So a basis for $Q(R^H)$ as a vector space of dimension $[K : H]$ over $Q(R^K)$ may be chosen in R^H. Such a basis is also a basis for R^H as a free module over R^K. □

Remark 3.1. An important tool in our analysis of these rings of invariants is the trace of a subgroup in a supergroup. We suppose that we have $H \subset K$ with $[K : H]$ prime to p and we let $\{g_\alpha\}$ denote a set of right coset representatives for H in K. Then we may define the trace map $Tr : R^H \to R^K$ by the rule

$$Tr(f) = \frac{1}{[K : H]} \sum g_\alpha(f).$$

It is easy to see that Tr is a homomorphism of R^K-modules and, further, that Tr is an epimorphism.

Our next task is to find a free module basis for R_2^P over $R_2^{S^2}$. We recall that the Poincaré series of a graded algebra $A = \bigoplus A(i)$ is defined to be $\sum dim_{\mathbf{F}_p}(A(i))$. The Poincaré series of a polynomial algebra $T = \mathbf{F}_p[w_1, \ldots, w_r]$ with $|w_i| = d_i$ is easily

seen to be

$$P(T,t) = \prod_{i=1}^{r} (1 - t^{d_i})^{-1}.$$

It follows that a free T-module M on m basis elements of degrees $\{e_i\}$ has Poincaré series

$$P(M,t) = \left(\sum_{j=1}^{m} t^{e_j} \right) P(T,t).$$

We refer to the numerator $\sum_{j=1}^{m} t^{e_j}$ of $P(M,t)$ for such a free module M as the Poincaré polynomial for M with respect to T.

At the center of the present calculation is our construction of a basis for $R_1^P = \mathbf{F}_p[x_1, z_1]$ as a free module over $R_1^S = \mathbf{F}_p[v_1, w_1]$. We observe that

$$\begin{aligned} \frac{P(R_1^P,t)}{P(R_1^S,t)} &= \left(\frac{1 - t^{p-1}}{1 - t} \right) \left(\frac{1 - t^{p(p-1)}}{1 - t^p} \right) \\ &= (1 + t + t^2 + \cdots + t^p)(1 + t^p + t^{2p} + \cdots + t^{p(p-2)}). \end{aligned}$$

The form of this Poincaré polynomial suggests that a free basis for R_1^P as a module over R_1^S might be $\{x_1^i z_1^j \mid 0 \le i \le p,\ 0 \le j \le p-2\}$. This is clearly not so, since $x_i z_i = v_i \in R_1^S$. However, with this in mind, another look at the Poincaré polynomial suggests that $\{x_1^i, z_1^j \mid 0 \le i \le p(p-1),\ 1 \le j \le p-2\}$ might be a free basis. This is indeed the case. Guided by this 'numerology' we have

Proposition 3.2. *R_2^P is free as a module over R_2^S on the set*

$$\mathcal{M} = \begin{cases} x_1^i x_2^j u^k, & 0 \le i,j \le p(p-1),\quad 0 \le k \le p-1; \\ x_1^i z_2^j u^k, & 0 \le i \le p(p-1),\quad 1 \le j \le p-2,\quad 0 \le k \le p-1; \\ x_2^i z_1^j u^k, & 0 \le i \le p(p-1),\quad 1 \le j \le p-2,\quad 0 \le k \le p-1; \\ z_1^i z_2^j u^k, & 1 \le 1 \le i,j \le p-2,\quad 0 \le k \le p-1. \end{cases}$$

Remark 3.2. There are other cases where the 'numerology' of the Poincaré polynomial is useful, see [3].

Proof. We denote by I the homogeneous ideal of R_2^P generated by $\{v_i, w_i \mid i = 1,2\}$. Since I is homogeneous, we may assume that R_2^P/I has a basis consisting of the images of monomials $x_1^i x_2^j z_1^k z_2^l u^m$, since these monomials span R_2^P by Theorem 2.2. Equivalently, we may assume that the free R_2^S-module basis for R_2^P consists of such monomials. From the definitions, for $i = 1,2$

$$\begin{aligned} &x_i z_i = v_i, \\ &z_i^{p-1} = w_i - x_i^{p(p-1)}, \\ &x_i^{p(p-1)+1} = w_i x_i - v_i z_i^{p-2}. \end{aligned} \tag{3.1}$$

We observe that the first and last equation tell us that each monomial on its left-hand side is in I, and consequently none of these monomials may appear in a free basis. And, of course, all higher powers of these monomials are in I as well. The second equation tells us that one of z_i^{p-1} or $x_i^{p(p-1)}$ may appear in a free basis but not both. We choose $x_i^{p(p-1)}$. In addition, we have $u^p = (x_1x_2)^{p-1}u + x_1^p z_2 - x_2^p z_1$ by Theorem 2.2 so powers of u larger than $p-1$ need not appear in a free basis either. The collection of monomials not yet eliminated from a free basis is $\mathscr{A}$. We observe that $\mathscr{A}$ has exactly $p(p^2-1)^2$ elements and so $\mathscr{A}$ must be a free basis by Proposition 3.1(1). □

No such argument is available for U, S, or G since we have no a priori computation of their rings of invariants.

4. 2-Dimensional vector invariants of $U = U_2(\mathbf{F}_p)$

We recall Proposition 3.1(2), R_2^U is a free $R_2^{S^2}$-module of rank $p(p^2-1)(p+1)$.

We observe that P is normal in U with quotient group D of order $p-1$ consisting of the diagonal matrices of determinant 1, that is, matrices of the form

$$g_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix},$$

as α varies over $\mathbf{F}_p^*$, the non-zero elements of $\mathbf{F}_p$. We recall Remark 3.1 and consider the epimorphism of R_2^U-modules $Tr : R_2^P \to R_2^U$ defined by the rule

$$Tr(f) = \frac{1}{[U : P]} \sum_{\alpha \in \mathbf{F}_p^*} g_\alpha(f) = -\sum_{\alpha \in \mathbf{F}_p^*} g_\alpha(f).$$

It is easy to see that

$$Tr(x_i) = \alpha x_i, \quad Tr(z_i) = \alpha^{-1} z_i, \quad \text{and} \quad Tr(u) = u.$$

We also note that $Tr(f) = f$ for $f \in R_2^U$, in particular $Tr(f) = f$ for $f \in R_2^{S^2}$. With this tool in hand, we are able to prove

Theorem 4.1. *R_2^U has as basis over $R_2^{S^2}$ the set*

$$\mathscr{B} = \begin{cases} x_1^i x_2^j u^k, & 0 \le i,j \le p(p-1), \quad 0 \le k \le p-1, \\ & \text{and} \quad i + j \equiv 0 \pmod{p-1}; \\ x_1^i z_2^j u^k, & 0 \le i \le p(p-1), \quad 1 \le j \le p-2, \quad 0 \le k \le p-1, \\ & \text{and} \quad i \equiv j \pmod{p-1}; \\ x_2^i z_1^j u^k, & 0 \le i \le p(p-1), \quad 1 \le j \le p-2, \quad 0 \le k \le p-1, \\ & \text{and} \quad i \equiv j \pmod{p-1}; \\ z_1^i z_2^j u^k, & 1 \le i,j \le p-2, \quad 0 \le k \le p-1 \\ & \text{and} \quad i + j \equiv 0 \pmod{p-1}. \end{cases}$$

Proof. Since Tr is onto and $\mathscr{B}$ has the correct number of elements by Proposition 3.1(2) we observe that it suffices to verify that the image of $\mathscr{A}$ under Tr is the set $\mathscr{B}$. But it is simple to see that $Tr(\mathscr{A}) = \mathscr{B}$. For example, consider

$$Tr(x_1^i x_2^j u^k) = -\sum_{\alpha \in \mathbf{F}_p^*} \alpha^{i+j} x_1^i x_2^j u^k = -x_1^i x_2^j u^k \left(\sum_{\alpha \in \mathbf{F}_p^*} \alpha^{i+j} \right)$$
$$= \begin{cases} 0, & i+j \not\equiv 0 \pmod{p-1}, \\ x_1^i x_2^j u^k, & i+j \equiv 0 \pmod{p-1}, \end{cases}$$

using the well-known identity

$$\sum_{\alpha \in \mathbf{F}_p^*} \alpha^\ell = \begin{cases} 0, & \ell \not\equiv 0 \pmod{p-1}, \\ -1, & \ell \equiv 0 \pmod{p-1}. \end{cases} \qquad \square$$

5. 2-Dimensional vector invariants of $S = Sl_2(\mathbf{F}_p)$

We will determine the structure of R_2^S as a free module over the polynomial algebra $R_2^{S^2}$. We recall from Proposition 3.1(3) that R_2^S is a free $R_2^{S^2}$-module of rank $p(p^2-1)$.

Let us describe our procedure for computing this particular ring of invariants. We find a likely collection, say $\mathscr{C}$, of $p(p^2-1)$ invariants and we wish to show that this set is a free basis for R_2^S as a module over $R_2^{S^2}$. By [13, Proposition 3.1, p. 482] we need only show that the image of $\mathscr{C}$ modulo the ideal J of R_2^S generated by $\{z_i, w_i \mid \text{for } i = 1,2\}$ is a linearly independent set over $\mathbf{F}_p$. We show that our alleged basis $\mathscr{C}$ really is a basis by comparing it to $\mathscr{A}$: if there were a relation in $\mathscr{C}$ modulo J there would be a similar relation in $\mathscr{A}$ modulo I, where I is the ideal of R_2^P generated by $\{v_i, w_i \mid \text{for } i = 1,2\}$, as above.

We recall the P-invariants and S^2-invariants

$$P \quad \begin{cases} u = x_1 y_2 - x_2 y_1, \\ z_1 = y_1^p - x_1^{p-1} y_1, \\ z_2 = y_2^p - x_2^{p-1} y_2; \end{cases} \qquad S^2 \quad \begin{cases} v_1 = x_1 z_1, \\ v_2 = x_2 z_2, \\ w_1 = x_1^{p(p-1)} + z_1^{p-1}, \\ w_2 = x_2^{p(p-1)} + z_2^{p-1}. \end{cases}$$

Remark 5.1. We have, in fact, an alternate method of proof along the lines of Section 4 and 6. That is, using Remark 3.1, we may trace a P-invariant over a set of right coset representatives for P in S to get an S-invariant. As usual, we denote the resulting R_2^S-module epimorphism $Tr : R_2^P \to R_2^S$. We can show that the image of $\mathscr{A}$ under Tr is the $R_2^{S^2}$-module spanned by $\mathscr{C}$. The calculation serves to explain the existence of the S-invariants below, for we found that $Tr(x_1 z_2) = u_2$, $Tr(x_2 z_1) = u_1$ and $Tr(z_1^{p-k-1} z_2^k) = n_k$. It follows immediately that the $\mathbf{F}_p$-algebra generated by $\{v_i, w_i, u_i, n_k\}$ is a subalgebra of R_2^S. Both proofs are about the same length and degree of difficulty.

We define

$$u_1 = y_1^p x_2 - x_1^p y_2 \quad \text{and} \quad u_2 = y_2^p x_1 - x_2^p y_1.$$

It is easy to verify that these elements are S-invariant. We have

$$u^p = (x_1x_2)^{p-1}u + x_1^p z_2 - x_2^p z_1 \quad \text{from Theorem 2.2,} \tag{5.1}$$

$$u^{p+1} = v_1v_2 - u_1u_2, \tag{5.2}$$

$$u_1 = -x_1^{p-1}u + x_2z_1, \quad u_2 = x_2^{p-1}u + x_1z_2, \tag{5.3}$$

$$u_1^p = u_2v_1^{p-1} - u^pw_1, \quad u_2^p = u_1v_2^{p-1} + u^pw_2. \tag{5.4}$$

The first and last of these equations are the syzygies in [8, p. 57]. All of these identities flow directly from the definitions. For example, we prove

$$u_1^p = u_2v_1^{p-1} - u^pw_1.$$

Proof. By (5.3)

$$\begin{aligned} u_1^p &= (-x_1^{p-1}u + x_2z_1)^p \\ &= -x_1^{p(p-1)}u^p + x_2^pz_1^p \\ &= (z_1^{p-1} - w_1)u^p + x_2^pz_1^p \quad \text{by definition of } w_1 \\ &= z_1^{p-1}u^p - w_1u^p + z_1^{p-1}(x_1^{p-1}x_2^{p-1}u + x_1^pz_2 - u^p) \qquad \text{by (5.1)} \\ &= -w_1u^p + v_1^{p-1}u_2 \quad \text{by (5.3).} \qquad \square \end{aligned}$$

We define n_k by

$$u^pn_k = v_1^{p-k-1}u_2^{k+1} - v_2^ku_1^{p-k}, \quad 0 \le k \le p-1.$$

Lemma 5.1. $n_k \in R_2^S$.

Proof. Our proof is by induction on k. For $k = 0$, we observe first from the definitions that

$$\begin{aligned} u^pn_0 &= u_2v_1^{p-1} - u_1^p = u_2v_1^{p-1} - (u_2v_1^{p-1} - u^pw_1) \\ &= u^pw_1 \quad \text{by (5.4).} \end{aligned}$$

That is, $n_0 = w_1$. For $k > 0$ we observe further, again by a simple calculation from the definitions, that

$$u_1n_k = -uu_2^kv_1^{p-k-1} + v_2n_{k-1}. \tag{5.5}$$

This formula is also of use later on. So u_1n_k and $u^pn_k \in R_2$ and this implies n_k is in R_2 since R_2 is a unique factorization domain and u_1 and u^p have no common factors. An easy induction shows also that $n_k \in R_2^S$. We observe also that $n_{k-1} = w_2$, which is used in the proof of (5.7) below. $\square$

There is another useful formula similar to that of (5.5):

$$u_2 n_k = u u_1^{p-k-1} v_2^k + v_1 n_{k+1}. \tag{5.6}$$

The following two identities are easily verified using the identities above:

$$u_1^{p-1} u = w_1 u_2 - n_1 v_1 \quad \text{and} \quad u_2^{p-1} u = w_2 u_1 + n_{p-2} v_2. \tag{5.7}$$

We are now ready to prove

Theorem 5.2. *R_2^S has as basis over $R_2^{S^2}$ the set*

$$\mathscr{C} = \begin{cases} u_1^i u_2^j & (0 \le i,j \le p-1); \\ u_1^i u_2^j u^k & (0 \le i,j \le p-2,\ 1 \le k \le p); \\ n_k u^i & (1 \le k \le p-2,\ 0 \le i \le p-1). \end{cases}$$

Remark 5.2. We observe that the numbered equations above hint at the upper bounds as stated in the theorem.

The rest of this section is devoted to the proof of Theorem 5.2.

$\mathscr{C}$ has $p(p^2-1)$ elements. Consequently the result follows if we can show that the image of $\mathscr{C}$ modulo J is linearly independent over $\mathbf{F}_p$, where J is the ideal of R_2^S generated by v_1, w_1, v_2, w_2, i.e., J is the ideal of R_2^S generated by the elements of positive degree in $R_2^{S^2}$. The proof is a straightforward and somewhat tedious verification of this fact.

We also need to consider the ideal I of R_2^P generated by v_1, w_1, v_2, w_2. Of course, since $R_2^S \subset R_2^P$ we have $J \subset I$.

Lemma 5.3. *We have $(u_1u_2)^{p-1} \equiv -(x_1x_2)^{p(p-1)} u^{p-1}$ modulo I.*

Proof. We have, working modulo I,

$$\begin{aligned} u_1^{p-1} &= (x_1^{p-1} u + x_2 z_1)^{p-1} \quad \text{by (5.3)} \\ &\equiv (-x_1^{p-1} u)^{p-1} + (x_2 z_1)^{p-1} \quad \text{since } x_1 z_1 = v_1 \equiv 0. \end{aligned}$$

Similarly, we have $u_2^{p-1} \equiv (x_2^{p-1} u)^{p-1} + (x_1 z_2)^{p-1}$. Thus

$$\begin{aligned} u_1^{p-1} u_2^{p-1} &\equiv (x_1x_2)^{(p-1)^2} u^{2p-2} + u^{p-1}(x_1^{p(p-1)} z_2^{p-1} + x_2^{p(p-1)} z_1^{p-1}) \\ &\qquad \text{since } (x_1^{(p-1)} z_2^{p-1})(x_2^{(p-1)} z_1^{p-1}) \equiv 0, \\ &\equiv (x_1x_2)^{(p-1)^2} u^{2p-2} - 2(x_1x_2)^{p(p-1)} \quad \text{since } z_i^{p-1} \equiv -x_i^{p(p-1)} \text{ by (3.1)}. \end{aligned}$$

But

$$\begin{aligned} (x_1x_2)^{(p-1)^2} u^{2p-2} &\equiv (x_1x_2)^{(p-1)^2} u^{p-2}((x_1x_2)^{p-1} u + x_1^p z_2 + x_2^p z_1) \quad \text{by (5.1)}, \\ &\equiv (x_1x_2)^{p(p-1)} u^{p-1} \quad \text{since } x_i z_i \equiv 0. \end{aligned}$$

The result follows. □

Corollary 5.4. *No monomial $u_1^i u_2^j$, $0 \le i,j, \le p-1$, is in J, and, in addition, the set $\{u_1^i u_2^j \mid 0 \le i,j, \le p-1\}$ is linearly independent modulo J.*

Proof. We observe that $(x_1x_2)^{p(p-1)}u^{p-1}$ is in $\mathscr{A}$ so its image in R_2^p modulo I is not zero. It follows immediately that the image of $(u_1u_2)^{p-1}$ in R_2^S modulo I cannot be zero. It follows that $u_1^i u_2^j$ is not in J.

We order the monomials $u_1^i u_2^j$ lexicographically using their exponent sequences (i,j) and consider the equation $\sum a(i,j)u_1^i u_2^j \equiv 0$ modulo J for $a(i,j) \in \mathbf{F}_p$. Suppose (k,ℓ) is the smallest monomial in this sum for which $a(k,\ell) \neq 0$. If we multiply this sum by $u_1^{p-1-k}u_2^{p-1-\ell}$ we observe that each term $a(i,j)u_1^i u_2^j u_1^{p-1-k}u_2^{p-1-\ell}$ has an exponent in either u_1 or u_2 bigger than $p-1$ for $(i,j) > (k,\ell)$. But by (5.4) each such term is in J. Therefore $0 \equiv u_1^{p-1-k}u_2^{p-1-\ell}\sum a(i,j)u_1^i u_2^j \equiv a(k,\ell)u_1^{p-1}u_2^{p-1}$ modulo J. Therefore $a(k,\ell) = 0$. This contradiction proves the corollary. □

Corollary 5.5. *The set $\{u_1^i u_2^j u^k \mid 0 \le i,j \le p-2, 1 \le k \le p\}$ is linearly independent modulo J.*

Proof. We observe that $u_1^{p-2}u_2^{p-2}u^{p+1} \equiv -u_1^{p-1}u_2^{p-1}$ modulo J by (5.2). The latter term is not congruent to 0 modulo J by Lemma 5.3. Suppose there were a dependence relation $\sum a(i,j,k)u_1^i u_2^j u^k \equiv 0$ modulo J. Proceeding as above we find the exponent sequences (r,s,k) with (r,s) smallest in the lexicographical order, and then multiply the sum by $u_1^{p-2-r}u_2^{p-2-s}$. The resulting sum has terms of the form $a(r,s,k)u_1^{p-2}u_2^{p-2}u^k$ and other 'higher' terms with even larger powers of u_1 and u_2. Suppose ℓ is the least integer for which $a(r,s,\ell) \neq 0$. We multiply $u_1^{p-2-r}u_2^{p-2-s}(\sum a(i,j,k)u_1^i u_2^j u^k)$ by $u^{p+1-\ell}$ and then use (5.2) on the resulting sum again. The 'higher' terms are all in J by (5.4). Hence, modulo J we have $\sum a(r,s,k)u_1^{p-2}u_2^{p-2}u^{p-1+k-\ell} + a(r,s,\ell)u_1^{p-2}u_2^{p-2}u^{p-1}$. However, since $k > \ell$ we may use (5.2) to rewrite all of the former terms modulo J as $u_1^{p-1}u_2^{p-1}u^m$ where $m \ge 1$. Hence all of these terms are in J by (5.7). It follows that $a(r,s,\ell) = 0$ and this contradiction proves the corollary. □

Lemma 5.6. *We have $u^{p-1}n_k \equiv z_1^{p-k-1}z_2^k u^{p-1}$ modulo I for $1 \le k \le p-2$.*

Proof. Working modulo I we have, by definition of n_k,

$$\begin{aligned} u^{p-1}n_k &= (u_2^{k+1}v_1^{p-k-1} - u_1^{p-k}v_2^k)/u, \quad \text{and so, using (5.3),} \\ &= ((-x_2^{p-1}u + x_1z_2)^{k+1}v_1^{p-k-1} - (x_2z_1 + x_1^{p-1}u)^{p-k}v_2^k)/u \\ &\equiv [(x_1z_2)^{k+1}v_1^{p-k-1} - (x_2z_1)^{p-k}v_2^k]/u, \end{aligned}$$

since all other terms have a factor u which cancels with the u in the denominator, and a factor v_1 or v_2, which is congruent to zero modulo I,

$$\begin{aligned} &= z_1^{p-k-1}z_2^k(x_1^p z_2 - x_2^p z_1)/u, \quad \text{since } x_i z_i = v_i \\ &= z_1^{p-k-1}z_2^k(u^p - x_1^{p-1}x_2^{p-1}u)/u \quad \text{by (5.1)} \\ &\equiv z_1^{p-k-1}z_2^k u^{p-1}. \end{aligned}$$

□

Corollary 5.7. *No factor $u^j n_k$ is in J for $0 \le j \le p-1$, and, in addition, $\{u^{p-1}n_k \mid 1 \le k \le p-2\}$ is linearly independent modulo J.*

Proof. The element $z_1^{p-k-1}z_2^k u^{p-1}$ is in $\mathscr{A}$: in particular its image in R_2^P modulo I is not zero so the image of $u^{p-1}n_k$ in R_2^S modulo J is not zero.

We further observe that the image modulo J of $\{u^{p-1}n_k\}$ is linearly independent since $\{z_1^{p-k-1}z_2^k u^{p-1}\}$ is linearly independent modulo I and we have $J \subset I$. □

Now any element of $\mathscr{C}$ is a factor modulo J of either $(u_1u_2)^{p-1}$ (since $u^{p-1} \equiv u_1u_2$) or $u^{p-1}n_k$ (for some k). Thus $\mathscr{C} \cap I = \emptyset$.

The proof of Theorem 5.2 is easily finished using the arguments given above. We give a brief sketch. Consider a linear relation modulo J :

$$\sum a(i,j)u_1^i u_2^j + \sum b(k,\ell,m)u_1^k u_2^\ell u^m + \sum c(r,s)n_r u^s.$$

We compare exponent sequences (i,j) and (k,ℓ,m) lexicographically (using only the first two entries in the latter sequences) as above. If a smallest such sequence occurs in the first collection of terms we proceed as in Corollary 5.4; otherwise we proceed as in Corollary 5.5. If all coefficients in the first two terms are 0 we apply Corollary 5.7.

6. 2-Dimensional vector invariants of $G = Gl_2(\mathbf{F}_p)$

It is not difficult to proceed on from the invariants of $S = Sl_2(\mathbf{F}_p)$ to those of $G = Gl_2(\mathbf{F}_p)$.

Proposition 6.1. *The set $v_1^r v_2^s \mathscr{C}$ for $0 \le r,s \le p-2$ is a free basis for R_2^S over $R_2^{G^2}$.*

Proof. R_2^S is free over $R_2^{G^2}$ of rank $p(p^2-1)(p-1)^2$ by Proposition 3.1(4). This is the size of our basis. We finish the proof by observing that $v_1^r v_2^s$, $0 \le r,s \le p-2$, is a free basis for $R_2^{S^2}$ over $R_2^{G^2}$ using Proposition 3.1(5). □

Theorem 6.2. *R_2^G is a free $R_2^{G^2}$ module on the set*

$$\mathscr{S} = \begin{cases} u_1^i u_2^j v_1^r v_2^s, & 0 \le i,j \le p-1, \quad 0 \le r,s \le p-2, \\ & \text{and} \quad i+j+r+s \equiv 0 \pmod{p-1}; \\ u_1^i u_2^j u^k v_1^r v_2^s, & 0 \le i,j \le p-2, \quad 1 \le k \le p, \quad 0 \le r,s \le p-2, \\ & \text{and} \quad i+j+k+r+s \equiv 0 \pmod{p-1}; \\ n_k u^i v_1^r v_2^s, & 1 \le k \le p-2, \quad 0 \le i \le p-1, \quad 0 \le r,s \le p-2, \\ & \text{and} \quad i+r+s \equiv 0 \pmod{p-1}. \end{cases}$$

Proof. We begin by observing that a set of right coset representatives for S in G consists of two copies of the diagonal matrices $g_z = \left(\begin{smallmatrix} z & 0 \\ 0 & 1 \end{smallmatrix}\right)$. As in Remark 3.1 we

define an epimorphism of R_2^G-modules $Tr : R_2^S \to R_2^G$ by the rule

$$Tr(f) = \frac{1}{[G:S]} \sum_{\alpha \in \mathbf{F}_p^*} g_\alpha(f) = -\sum_{\alpha \in \mathbf{F}_p^*} g_\alpha(f).$$

Consequently, it suffices to prove that the image of $v_1^r v_2^s \mathscr{C}$ for $0 \leq r,s \leq p-2$ lies in the $R_2^{G'}$-module spanned by the $(p^2-1)(p^2-p)$ elements of $\mathscr{L}$.

It is routine to verify that

$$g_\alpha(v_i) = \alpha v_i, \qquad g_\alpha(u) = \alpha u, \qquad g_\alpha(u_i) = \alpha u_i, \qquad g_\alpha(n_k) = n_k.$$

The proof now follows exactly as in Theorem 4.1. □

Acknowledgements

We would like to thank the referee of an earlier version of this paper for many useful and constructive remarks.

References

[1] H.E.A. Campbell and I.P. Hughes, On the vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of David Richman, Adv. in Math., to appear.
[2] H.E.A. Campbell and I.P. Hughes, Rings of invariants of certain p-groups over the field $\mathbf{F}_p$, J. Algebra, submitted.
[3] H.E.A. Campbell and I.P. Hughes, Upper triangular invariants as modules over the Dickson invariants, Math. Ann., to appear.
[4] H.E.A. Campbell, I.P. Hughes and R.D. Pollack, Vector invariants of symmetric groups, Canad. Math. Bull. 33 (1990) 391–397.
[5] H.E.A. Campbell, I.P. Hughes and R.D. Pollack, Rings of invariants and p-Sylow subgroups, Canad. Math. Bull. 34 (1991) 42–47.
[6] L.E.J. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. AMS 12 (1911) 75–98.
[7] M.Hochster, The invariant theory of commutative rings, Contemp. Math. 43 (1985) 161–179.
[8] W.C. Krathwohl, Modular invariants of two pairs of cogredient variables, Amer. J. Math. 36 (1914) 449–460.
[9] H.Mùi, Modular invariant theory and the cohomology algebras of the symmetric groups, J. Fac. Sci. Univ. Tokyo Sec. IA 22(3) (1975) 319 369.
[10] D.R. Richman, On vector invariants over finite fields, Adv. in Math. 81 (1990) 30–65.
[11] J.-P. Serre, Algèbre Locale-Multiplicitiés, Lecture Notes in Mathematics, Vol. 11 (Springer, Berlin, 1965).
[12] W.M. Singer, The transfer in homological algebra, Math. Z. 202 (1989) 493–523.
[13] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. AMS 1 (1979) 475–511.
[14] H.Weyl, Classical Groups (Princeton Univ. Press, Princeton, NJ, 2nd ed., 1953).