Proceedings of Symposia in Pure Mathematics
Volume 47 (1987)

Some Representations of Special Linear Groups

L. G. KOVÁCS

1. Introduction. Let p be a prime, q either ∞ or a power of p, and F_q a field of characteristic p and order q. Denote by M the multiplicative semigroup $\mathrm{Mat}_r^{\times}(F_q)$ of all r-by-r matrices over F_q, by G the group $\mathrm{GL}_r(F_q)$ of the units of M, and by S the special linear subgroup $\mathrm{SL}_r(F_q)$ of G. For an arbitrary field F containing F_q, let U stand for the (commutative) polynomial algebra $F[x_1, \ldots, x_r]$, and consider U graded as usual: $U = \bigoplus U_d$ where U_d is the space of homogeneous polynomials of degree d. In particular, U_1 is the F-space with basis $\{x_1, \ldots, x_r\}$, so M has a natural action on U_1; this extends (uniquely) to an action of M on all of U by graded algebra endomorphisms. Consider U an M-module (G-module, S-module) accordingly.

This paper is concerned with the submodule structure of U. Obviously, each homogeneous component U_d is an M-submodule, and so is the sum of any set of the U_d. As is well known, in the characteristic 0 analogue of this setup, these would be the only S-submodules (let alone M-submodules). In prime characteristic there are other kinds of submodules as well, at least if one excludes (as I shall from now on) the rather trivial case $r = 1$. Namely, for each submodule Y, denote by Y^p the F-span of all the y^p with $y \in Y$: this is also a submodule (because on any commutative ring of characteristic p, the map $u \mapsto u^p$ is a ring endomorphism which commutes with all other ring endomorphisms), and for instance $0 < U_d^p < U_{dp}$ unless $d = 0$. Of course, sums and products of submodules are always submodules (the product YY' being as usual the set of all sums of products of the form yy' with $y \in Y$, $y' \in Y'$): so in particular

$$U_p U_1^{p^3} + U_1^p U_p^{p^2} \text{ is a submodule of } U_{p^3+p}.$$

The main results in the literature are due to Doty and to Krop.

For the case $q = \infty$, the S-submodules of U were determined in Doty's thesis [3] (Notre Dame, 1982; see also [4]). It can be deduced from his result that all S-submodules are of the kind illustrated above: indeed, each can be given a

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20C20.
This paper is in final form and no version of it will be submitted for publication elsewhere.

0082-0717/87 $1.00 + $.25 per page

canonical expression of that form. (Consequently, all S-submodules of U_d admit M as well.)

In the case $q < \infty$ the picture is much more complicated and correspondingly conclusive results seem to be completely out of reach. While one cannot hope to know all submodules, Krop was bold enough to ask whether the lattice they form is distributive. When $q = p$, he answered this in his thesis [**7**] (Chicago, 1983) and the subsequent papers [**8**, **9**], for the M-submodules of each U_d with $d \leq r$. (For some such d the answer is affirmative and for the others it is negative.) Some of his preliminary arguments work even better when $q = \infty$; for that case, he actually determined all M-submodules of the U_d with $d \leq r$.

The main result of this paper is a theorem in which q is arbitrary. It deals with certain quotients of the U_d, which include U_d itself when $d < q$. Instead of addressing the submodule structure directly, it describes (in their action) the quotients of the (semi)group algebras FM, FG, FS modulo the annihilators of the modules in question. The description is such that the submodule structure can be read off it very easily. In particular, the results of Doty and Krop for the case $q = \infty$ follow. The proof is elementary in the sense that it makes no appeal to the language (let alone to the theory) of algebraic groups.

It owes much to the long discussions and extensive correspondence I have had with Professor Krop. I am also indebted to Professor Warren Wong, for an elementary step which had kept eluding me (even at Arcata).

2. Results. Let e be a positive integer such that $p^e \leq q$, and let V be the quotient of U modulo the ideal generated by the p^eth powers:

$$V = U/U^{p^e}U.$$

This algebra inherits a grading from U, with

$$V_d \neq 0 \quad \text{if and only if } d \leq r(p^e - 1).$$

It will be convenient to state and prove our result in terms of the V_d. Of course, if $p^e > d$ then $U_d \cong V_d$; given d, one can always choose e this way when $q > d$. When $q < \infty$, the largest quotients of the U_d accessible to the present approach are the V_d with e chosen so that $p^e = q$.

An obvious F-basis in V_d is the set B of all monomials b such that

$$b = \prod x_i^{b(i)} \quad \text{with } 0 \leq b(i) < p^e \text{ and } \sum b(i) = d.$$

(Strictly, one should speak of the set of the cosets of these b, but I shall not be that pedantic.)

It will be relevant to write each $b(i)$ to base p as

$$b(i) = \sum_{j<e} b(i,j)p^j \quad \text{with } 0 \leq b(i,j) < p \text{ for all } i, j,$$

and to write

$$d = \sum_{j<e} d(j)p^j \quad \text{with } 0 \leq d(j) < p \text{ except perhaps when } j = e - 1.$$

When performing the addition $\sum b(i) = d$ in base p arithmetic, the amount $c_k(b)$ carried to the column of digits with place value p^k is given by

$$\sum_i \sum_{j<k} b(i,j)p^j = c_k(b) + \sum_{j<k} d(j)p^j \quad \text{whenever } 0 \le k < e.$$

The sequence $c_0(b), \ldots, c_{e-1}(b)$ will be called the *carry pattern* of b. Define a binary relation $\succ$ on B by setting

$$b \succ b' \quad \text{if } c_k(b) \ge c_k(b') \text{ for all } k.$$

Let (b, b') denote the F-linear transformation on V_d which maps b to b' and annihilates all monomials other than b. Refer to the homomorphism of M into $\mathrm{End}_F V_d$ given by the action of M on V_d.

THEOREM. *The subalgebra of* $\mathrm{End}_F V_d$ *spanned by the image of* S *contains the image of* M. *The set of the* (b, b') *with* $b \succ b'$ *is an* F*-basis for this subalgebra.*

The proof of the Theorem will be sketched in the next two sections. Here we discuss some consequences and related results: their deductions (either from the Theorem or from its proof) will be left to the reader.

For a start, let us domesticate the Theorem by paraphrasing its second part as follows. The relation $\succ$ is obviously reflexive and transitive; hence it is easy to see that there exist linear orders $\ge$ on B which are compatible with $\succ$ in the sense that $b \ge b'$ and $b' \succ b$ imply $b \succ b'$. Think of $\mathrm{End}_F V_d$ as acting on the right, and identify it with the full matrix algebra of the relevant size, with reference to the basis B (linearly ordered as indicated). The transformation (b, b') then appears as the matrix whose entries are all 0 except for the b, b' entry which is 1. The subalgebra in question becomes the algebra of *all* "blocked" matrices in which certain specified blocks consist of zeros. All blocks above the diagonal, but no blocks on the diagonal, are required to vanish. As in any such algebra, the nonvanishing blocks graph a partial order on the set of the diagonal blocks. Here the set of the diagonal blocks is bijective with the set, P say, of all carry patterns obtained in base p arithmetic while writing d as a sum of r summands $b(i)$ with $0 \le b(i) < p^e$, the partial order matching that defined on P componentwise.

It will be useful to be familiar with another isomorphic copy of this poset. That consists of all sequences $\beta(0), \ldots, \beta(e-1)$ of integers such that $0 \le \beta(j) \le r(p-1)$ and $\sum \beta(j)p^j = d$, the partial order being given by

$$\beta \ge \beta' \quad \text{if and only if } \sum_{j<k} \beta(j)p^j \ge \sum_{j<k} \beta'(j)p^j \text{ for all } k.$$

The relevant order-isomorphism is induced by the mapping of B onto this poset which takes b to the β defined by $\beta(j) = \sum b(i,j)$: the isomorphism maps the carry pattern of b to this β. The relations

$$\sum_{j<k} \beta(j)p^j = c_k(b)p^k + \sum_{j<k} d(j)p^j$$

show that the latter map is well defined, one-to-one, and order-preserving. To see that it is also surjective, given any β define b by $b(i) = \sum b(i,j)p^j$ where

$$b(i,j) = \left\{ \begin{array}{ll} p-1 & \text{if } i < \\ \beta(j) - (p-1)[\beta(j)/(p-1)] & \text{if } i = \\ 0 & \text{if } i > \end{array} \right\} 1 + [\beta(j)/(p-1)],$$

note that $0 \leq b(i) < p^e$ and $\sum b(i) = d$ so $b \in B$, and check that the image of (the carry pattern of) this b is β. [For later reference observe also that, with respect to the lexicographic order on B (which need not be compatible with $\succ$), this b is the "highest" preimage of β.] It is straightforward to see that this poset (and hence also P) has a unique minimal element and a unique maximal element. Namely, define β_0 and β_1 inductively by requiring that $\beta_0(k)$ be minimal with respect to

$$\begin{aligned} &\beta_0(k) \geq 0, \\ &\beta_0(k)p^k \geq d - \sum_{j<k} \beta_0(j)p^j - r(p^e - p^{k+1}), \\ &\beta_0(k)p^k \equiv d - \sum_{j<k} \beta_0(j)p^j \mod p^{k+1}, \end{aligned}$$

and that $\beta_1(k)$ be maximal with respect to

$$\begin{aligned} &\beta_1(k) \leq r(p-1), \\ &\beta_1(k)p^k \leq d - \sum_{j<k} \beta_1(j)p^j \\ &\beta_1(k)p^k \equiv d - \sum_{j<k} \beta_1(j)p^j \mod p^{k+1}: \end{aligned}$$

then $\beta_0 \leq \beta \leq \beta_1$ for all β.

The Theorem shows that V_d has the same submodules regardless of whether we consider it an M-, G-, or S-module. Indeed, since the basis it describes is independent of the choice of the subfield F_q in F (as long as F_q has at least p^e elements), the subalgebra spanned by the image of S contains even the image of $\mathrm{Mat}_r^\times(F)$ (with respect to the analogous action of $\mathrm{Mat}_r^\times(F)$ on V_d): consequently, all S-submodules of V_d admit $\mathrm{Mat}_r^\times(F)$ as well. The paraphrase makes it also immediate that all composition factors of V_d are absolutely simple and that the factors of any one composition series are pairwise nonisomorphic.

The theorem yields full knowledge of the submodule structure along the following lines. As the relevant subalgebra contains all the diagonal primitive idempotents (b,b), each submodule is spanned by the monomials it contains. A subset B' of B is the basis of a submodule if and only if

$$b' \in B' \text{ and } b' \succ b \in B \quad \text{imply } b \in B'.$$

Thus the submodule lattice of V_d is finite and distributive. A nonzero submodule is a joinirreducible element of this lattice if and only if it is generated by a single element of B: thus the poset of the nonzero joinirreducibles is isomorphic to the poset P of the carry patterns discussed above. Since any finite distributive

lattice is isomorphic to the (union/intersection) lattice of all filters (dual ideals) on the poset of the nonzero joinirreducibles, our submodule lattice is isomorphic to the lattice of all filters on P. We have seen that P has a unique maximal element and a unique minimal element: so V_d itself must be joinirreducible (and so have a unique maximal submodule) and must have a unique simple submodule. Further, each composition series of V_d is bijective with P in such a way that the factors of different series matched to the same carry pattern are isomorphic. (For basic facts on finite distributive lattices, see Aigner [1].)

Explicitly, let b be any element of B: the submodule generated by b has basis $\{b' \in B | b \succ b'\}$, and this is the joinirreducible submodule corresponding to the carry pattern of b. For any β in the isomorphic copy of P discussed above, set

$$V_\beta = \prod V_{\beta(j)}^{p^j}.$$

If β is chosen as the image of b (in the sense of that discussion), then V_β is the submodule generated by b. Further, the unique simple quotient of this module represents the isomorphism type of the composition factors corresponding to the carry pattern of b. It is not hard to deduce directly that this simple quotient is the twisted tensor product of the unique simple quotients of the $V_{\beta(j)}$. If b is the (lexicographically) highest preimage of β in B, then the $b(i)$ give the partition of d which customarily labels this isomorphism type of G-modules when $q = \infty$ (see for instance Green [**6**]). [When $q < \infty$ but F is infinite, our simple G-module is the restriction to G of the simple $\mathrm{GL}_r(F)$-module labelled by this partition. If F is finite, let $\overline{F}$ denote its algebraic closure and take the simple $\overline{F}\mathrm{GL}_r(\overline{F})$-module bearing this label: the restriction of this to $\overline{F}G$ is the module obtained from our simple FG-module by extension of scalars.] Conversely, let $b(1), \ldots, b(r)$ be any r-part partition of d and $b = \prod x_i^{b(i)}$: the simple G-module labelled by this partition occurs among the composition factors of V_d if and only if b is maximal (in lexicographic order) among the elements of B giving its carry pattern, and it is not hard to see that this condition is equivalent to $0 \leq b(j) < p^e$ and

$$\forall j.\ \exists\ k.\ [b(i,j) = p-1 \text{ if } i < k]\ \&\ [b(i,j) = 0 \text{ if } i > k]$$

where the $b(i,j)$ are the base p digits of the $b(i)$ as before.

An unusual feature of the submodule lattice of V_d is that all meets of joinirreducibles are joinirreducible. Differently put: to any b', b'' in B, there is a b in B such that $b'FM \cap b''FM = bFM$. Namely, define first $c(k)$ by

$$c(k) = \begin{cases} \min\{c_k(b'), c_k(b'')\} & \text{if } 0 \leq k < e, \\ 0 & \text{if } k = e, \end{cases}$$

and then β by $\beta(k) = d(k) + c(k+1)p - c(k)$; it is not hard to verify that any preimage of this β (for instance, the lexicographically highest preimage defined explicitly above) will do as b.

To state another unexpected fact, let r^* be any integer, $r^* > r$, and define G^*, S^*, U^*, V^* with reference to r^* in place of r. Then U is a subalgebra of U^* and V may be considered a subalgebra of V^*. Further, one may identify G with

a subgroup of G^* in such a way that the action of G on U is the restriction of the action of G^* on U^* and G fixes each of the new indeterminates $x_{r+1}, \dots, x_{r^*}$; of course then S becomes a subgroup of S^*. It will be seen from the proof of the Theorem that the S-submodules of V_d are just the intersections of V_d with the S^*-submodules of V_d^*. [In general, for U_d the analogue of this statement is false. For example, let $q = r = d = 2$ and $r^* = 3$: then $x_1^2 + x_1x_2 + x_2^2$ is fixed by G but $x_1^2 + x_2^2 \in U_2 \cap (x_1^2 + x_1x_2 + x_2^2)FS^*$. This also shows that the span of the image of G in $\mathrm{End}_F U_d$ need not contain the image of M.]

3. Proof of the Theorem: The plan. We begin with an elementary exercise on semigroups, leaving the completely bare-handed deductions to the reader. Let B be any set, C a subset of the cartesian square B^2 containing the diagonal $\{(b,b)|b \in B\}$, and write $C^{\mathrm{op}} = \{(b',b)|(b,b') \in B\}$. Define a semigroup on $\{0\} \cup B^2$ by letting 0 behave as zero and setting

$$(b_1,b_2)(b_3,b_4) = \begin{cases} (b_1,b_4) & \text{if } b_2 = b_3, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $\{0\} \cup C$ is a subsemigroup [equivalently, that C is the graph of a preorder, that is, of a transitive and reflexive binary relation, on B]. Then B can be partitioned so that $C \cap C^{\mathrm{op}}$ is the union of the cartesian squares of the parts [equivalently, $C \cap C^{\mathrm{op}}$ is the graph of an equivalence relation on B]. If $(b_0,b_1),(b_1,b_2),\dots,(b_{n-1},b_n)$ is a sequence of elements of $C \backslash C^{\mathrm{op}}$ such that the product of this sequence is not 0 [and hence equals (b_0,b_n)], then $b_0, b_1, \dots, b_n$ must be pairwise distinct. The set $\{0\} \cup C \backslash C^{\mathrm{op}}$ is an ideal in $\{0\} \cup C$; indeed, it is a nilpotent ideal when B is finite.

We shall use these facts only via the following application to algebras. Let B be finite, F any field, and FB the F-space with basis B. Identify each (b,b') in B^2 with the linear transformation on FB which maps b to b' and annihilates all basis vectors other than b. Write linear transformations on the right, so their composition agrees with the multiplication defined above on $\{0\} \cup B^2$. Note that B^2 is an F-basis for $\mathrm{End}_F FB$, and the span FC of C is a subalgebra of $\mathrm{End}_F FB$. Further, $F(C \backslash C^{\mathrm{op}})$ is the radical of FC, and $F(C \cap C^{\mathrm{op}})$ is a complement to that radical. If $B_1, \dots, B_l$ are the equivalence classes of the relation with graph $C \cap C^{\mathrm{op}}$, then $B = \bigcup B_j$ and $C \cap C^{\mathrm{op}} = \bigcup B_j^2$, so $FB = \oplus FB_j$ and $F(C \cap C^{\mathrm{op}}) = \bigoplus \mathrm{End}_F FB_j$. It follows that the factors of an FC-composition series of FB are absolutely simple and pairwise nonisomorphic.

Conversely, let W be a finite-dimensional F-space and A a (nonzero) subalgebra of $\mathrm{End}_F W$ such that the factors of a composition series of W as A-module are absolutely simple and pairwise nonisomorphic: one can show that then $A = FC$ for some suitable basis B of W and some suitable subsemigroup $\{0\} \cup C$, containing all the idempotents, of $\{0\} \cup B^2$. Namely, use 29.13 and 72.19 from Curtis and Reiner [2] to deduce that the radical of A is complemented by a direct sum of full matrix algebras whose degrees sum to $\dim W$, whence 1 can be written as the sum of $\dim W$ orthogonal idempotents in A, and B can be chosen so that these idempotents become the (b,b). Then $A = \bigoplus\bigoplus (b,b)A(b',b')$ where each

summand is of dimension at most 1 and so each nonzero summand contains the corresponding (b, b') : thus one may choose C as $A \cap B^2$, that is, as the set of all (b, b') such that $b' \in bA$. Note that if A' is a subalgebra of $\mathrm{End}_F W$ properly containing A, then A' is also spanned by its intersection with B^2 and so must contain a (b, b') which is not in A: then bA is an A-submodule which does not contain b' and so is not an A'-module.

We are now ready to describe the proof of the Theorem, leaving six technical steps for the next section. Take up the conventions of §2: in particular, from now on B is once more the fixed basis of V_d consisting of the "monomials." Let A denote the span of the image of S in $\mathrm{End}_F V_d$, and T the semigroup of the diagonal matrices in M.

When $q = \infty$ the first sentence of the Theorem can be obtained by a routine argument which we shall merely sketch. Each monomial is an eigenvector for each element of T, and to any two different monomials (of the same degree d) there is an element in $S \cap T$ whose eigenvalues on these monomials are different. It follows that each $(S \cap T)$-submodule of V_d is spanned by the elements of B that it contains; equivalently, that the span of the image of $S \cap T$ contains all the (b, b). Conversely, the image of T lies in the span of the (b, b), so we are done because S and T together generate M.

When $q < \infty$ we have to work harder. Let A' denote the span of the image of G. Step 1 is that A' contains all the (b, b). As we have seen, this implies that $A' = FC$ with $C = A' \cap B^2$. Let the B_j be chosen with reference to this C, so we have $V_d = \bigoplus FB_j$ and $F(C \cap C^{\mathrm{op}}) = \bigoplus \mathrm{End}_F FB_j$ as before. The pre-order graphed by C yields a partial order on the set of the B_j. As any partial order on any finite set, this can be extended to a linear order: let the B_j be indexed accordingly, so the $FB_1 \oplus \cdots \oplus FB_j$ form an FG-composition series in V_d. Step 2: no two factors of this composition series are FS-isomorphic. Step 3 is that these FG-composition factors are absolutely simple as FS-modules. Step 4: all FS-submodules of V_d admit G. The last sentence of the third paragraph of this section (applied perhaps with a different choice of B) would contradict this if we had $A' > A$: hence $A' = A$. In view of Step 1, the claim now follows as in the case of $q = \infty$.

This has not only proved the first sentence of the Theorem, but also reduced the proof of the second sentence to establishing that

$$b' \in bFM \quad \text{if and only if } c_k(b) \geq c_k(b') \text{ for all } k.$$

Let r^* be an integer, $r^* > r$; define M^*, G^*, S^*, U^*, V^* with reference to r^* in place of r. Then U is a subalgebra of U^*, and V may be considered a subalgebra of V^*. Further, one may embed M in M^* in such a way that the action of M on U remains unchanged while $x_{r+1}, \ldots, x_{r^*}$ are annihilated by M. In particular, the identity element of M becomes the diagonal matrix δ in M^* with 1 in the first r diagonal positions and 0 elsewhere, and then $M = \delta M^* \delta$. (Beware: this puts G into M^* as a group of singular matrices, *not* as a subgroup of G^*.) Then V_d is an M-submodule of the M^*-module V_d^*, and

it is easy to see that the M-submodules of V_d are precisely the intersections of V_d with the M^*-submodules of V_d^* [as $\delta^2 = \delta$ and $V_d^*\delta = V_d$, if $v \in V_d$ then $vFM = vF(\delta M^*\delta) = (vFM^*)\delta = V_d \cap vFM^*$].

(Before proceeding, we pause to justify the claim made in the last paragraph of §2. By now we know that if $v \in V_d$ then $vFM = vA = vFS$ and so similarly $vFM^* = vA^* = vFS^*$, hence also $vFS = V_d \cap vFS^*$. This conclusion no longer involves the action of G on $x_{r+1}, \ldots, x_{r^*}$, so it holds also when G is taken to fix these extra indeterminates.)

The outstanding claim will certainly follow if we can show that, for all b, b' in B^*,

$$b' \in bFM^* \quad \text{if and only if } c_k(b) \geq c_k(b') \text{ for all } k.$$

Instead of carrying asterisks into all subsequent formulas, we exploit this by assuming without any loss of generality that the number of available indeterminates is large compared to the degree d we are interested in. Indeed, to simplify typography we assume that U has further indeterminates y_{ij}, as well as the x_i, with i running at least to d and j running from 0 to $e-1$.

For each sequence $\beta(0), \ldots, \beta(e-1)$ of nonnegative integers with $\sum(\beta(j)p^j = d$ (so that in particular $\beta(j) \leq d$ for all j), set

$$V_\beta = \prod_{j=0}^{e-1} V_{\beta(j)}^{p^j} \quad \text{and} \quad \overline{\beta} = \prod_{j=0}^{e-1} \prod_{i=1}^{\beta(j)} y_{ij}^{p^j}.$$

Note that the monomials in V_d are precisely the monomials in $(x_1 x_2 \cdots x_d)M$: similarly, the monomials in $V_{\beta(j)}^{p^j}$ are the monomials in $(\prod_{i=1}^{\beta(j)} y_{ij}^{p^j})M$, and so the monomials in V_β are just the monomials in $\overline{\beta}M$. In particular, $V_\beta = \overline{\beta}FM$.

Let $b = \prod x_i^{b(i)} \in B$ with $b(i) = \sum b(i,j)p^j$ as before, and set $\beta(j) = \sum b(i,j)$. Step 5 is that $b \in \overline{\beta}M$ and $\overline{\beta} \in bFM$: consequently, $bFM = V_\beta$.

Let β' be similarly defined from b'. Step 6: we have $b' \in bFM$ if and only if

$$\sum_{j<k} \beta(j)p^j \geq \sum_{j<k} \beta'(j)p^j \quad \text{for each } k.$$

Since $\sum_{j<k} \beta(j)p^j = c_k(b)p^k + \sum_{j<k} d(j)p^j$ and a similar expression holds with β' and b', the inequalities in Step 6 are equivalent to those we require. While elements of B can now involve indeterminates other than the x_i, none can involve more than d indeterminates; as i does range at least up to d and as M contains all permutations of the indeterminates in U, no generality was lost by taking b and b' in the form above. Thus Steps 1 to 6 will indeed complete the proof of the Theorem.

4. Proof of the Theorem: The deferred steps. STEP 1. Each (b, b) is the image of some element of the group algebra FG.

PROOF. Consider the case $p^e = q$. Let $b = \prod x_i^{b(i)} \in B$ and choose $q-1$ pairwise distinct nonzero scalars $f_1, \ldots, f_{q-1}$ in F_q. For each i, consider the

system of $q-1$ linear equations

$$\sum_{j=1}^{q-1} f_j^k x_{ij} = \begin{cases} 1 & \text{if } k \equiv b(i) \mod q-1, \\ 0 & \text{otherwise,} \end{cases} \qquad k \in \{1,\dots,q-1\}.$$

The determinant is a nonvanishing vandermondian, so there is a unique solution f_{ij} in F_q. Let d_{ij} denote the diagonal matrix in G with i,i entry f_j and all other diagonal entries 1, and consider the element δ_i of the group algebra FG defined by $\delta_i = \sum f_{ij} d_{ij}$. If $b' = \prod x_i^{b'(i)} \in B$ then $b' d_{ij} = f_j^{b'(i)} b'$ and so b' is fixed by δ_i if $b'(i) \equiv b(i) \mod q-1$ and annihilated otherwise. Since the δ_i commute with each other, their product δ fixes or annihilates b' according to whether $b'(i) \equiv b(i)$ for all i. [When $p^e < q$, one can choose p^e pairwise distinct nonzero scalars and solve systems of p^e simultaneous equations instead; as $b'(i) \equiv b(i) \bmod p^e$ for all i amounts to $b' = b$; in that case (b,b) is simply the image of δ and the proof ends here.]

As all permutations of the indeterminates belong to G, no generality is lost by restricting attention to b such that for suitable integers s,t one has that $r \geq s \geq t \geq 0$ and

$$b(i) \begin{cases} = q-1 & \text{if } 0 \leq i \leq t, \\ = 0 & \text{if } t < i \leq s, \\ \in \{1,\dots,q-2\} & \text{if } s < i \leq r. \end{cases}$$

Set $b^* = \prod_{i>s} x_i^{b(i)}$ and, for each t-element subset I of $\{1,\dots,s\}$, let $b_I = \prod_{i \in I} x_i^{q-1}$: the elements of B fixed by δ are precisely the $b_I b^*$. If $t = 0$ or $t = s$, then there is only one such I and so b is the only element of B fixed by δ : in this case (b,b) is just the image of δ. In the remaining case, $0 < t < s$. For each pair i,j of integers such that $1 \leq i \leq t < j \leq s$, consider the element g_{ij} of G which maps x_i to $x_i + x_j$ and fixes all other indeterminates, and the element h_{ij} which swaps x_i with x_j and fixes all other indeterminates. Now (b,b) is the image of $\prod\prod \delta(g_{ij}\delta - 1)h_{ij}$. Indeed, this product annihilates all elements of B other than the $b_I b^*$ (because δ already annihilates them), while

$$b_I g_{ij} \delta = \begin{cases} b_I + b_{I \setminus \{i\} \cup \{j\}} & \text{if } i \in I \text{ and } j \notin I, \\ b_I & \text{otherwise,} \end{cases}$$

so b_I is fixed by $\delta(g_{ij}\delta - 1)h_{ij}$ if $i \in I$ and $j \notin I$, and annihilated otherwise.

This completes the proof of Step 1. One may note that this step works mutatis mutandis if V_d is replaced by V/V_0 or $V/V_{r(q-1)}$ but not for V itself: indeed, if $p^e = q$ then V_0 and $V_{r(q-1)}$ are G-isomorphic (1-dimensional trivial) modules.

STEP 2. No two factors of the given FG-composition series of V_d are FS-isomorphic.

PROOF. This will be seen by comparing traces.

The claim, and the discussion leading up to it, behaves well under extension of scalars, so we may assume here that F is algebraically closed.

By a fundamental theorem, the subalgebra of the symmetric polynomials in U is the image of a one-to-one algebra endomorphism σ of U such that $x_1\sigma, \dots, x_r\sigma$

are the elementary symmetric polynomials. One can read off the standard proof of this theorem that if w is a symmetric polynomial whose degree in each indeterminate is smaller than n, say, then the total degree of the unique preimage $w\sigma^{-1}$ is smaller than n. Moreover, if w is homogeneous of degree d and $w\sigma^{-1}$ is written as $\sum w_i x_r^i$ with $w_i \in F[x_1, \ldots, x_{r-1}]$, then each $w_i\sigma$ is homogeneous of degree $d - ir$.

For each B_j, define the polynomial u_j in U by requiring that $u_j\sigma$ be the sum of the (genuine) monomial preimages of the elements of B_j (in U): then each u_j is of total degree less than q. Consider the endomorphism ρ of U which maps x_r to 1 and fixes the other indeterminates. If $u_j = \sum w_i x_r^i$ as above, the $w_i\sigma$ are the homogeneous components (of the relevant degrees) of $u_j\rho\sigma$: hence u_j can be reconstructed from $u_j\rho$. Thus if $j \neq k$ then $u_j\rho \neq u_k\rho$ in $F[x_1, \ldots, x_{r-1}]$.

Given any $f_1, \ldots, f_{r-1}$ in F_q, define the polynomial φ as $x^r + (-1)^r + \sum f_j x^{r-j}$; write φ as a product of polynomials which are irreducible over F_q, and let s be the direct sum of the companion matrices of these irreducible factors. Then s is a completely reducible matrix whose characteristic polynomial is φ; in particular, $\det s = 1$ so $s \in S$. It follows that the trace of the matrix representing s on the composition factor $(FB_1 \oplus \cdots \oplus FB_j)/(FB_1 \oplus \cdots \oplus FB_{j-1})$ is the image of u_j under the homomorphism $U \to F$ which maps each of $x_1, \ldots, x_{r-1}$ to the corresponding f_i and maps x_r to 1. [For, s is conjugate in $\mathrm{GL}_r(F)$ to a diagonal matrix s' whose diagonal entries are the characteristic roots $\xi_1, \ldots, \xi_r$ of s; each element b of B is an eigenvector for s', with eigenvalue $\prod \xi_i^{b(i)}$, and so on.] Differently put: the trace is given by evaluating the polynomial function $u_j\rho$ (of $r-1$ variables) at $f_1, \ldots, f_{r-1}$. Since distinct polynomials of degree less than q define distinct polynomial functions on F_q, we conclude that distinct composition factors afford different traces and so cannot be FS-isomorphic.

STEP 3. All FG-composition factors of V_d are absolutely simple as FS-modules. (I am indebted to Professor Warren Wong for this step; see [**10**].)

PROOF. It suffices to show that if $q < \infty$ and F is algebraically closed, then each simple FG-module W is simple as FS-module. In turn, this is equivalent (see Theorem III.2.14 in Feit [**5**]) to the claim that each simple FS-module is isomorphic to all its G-conjugates. As the Brauer character determines the isomorphism type of a simple module, all we need show is that if two p'-elements of S are conjugate in G then they are already conjugate in S. To see this, we show that if h is such an element in S then $SC_G(h) = G$: that is, to each nonzero f in F_q there is a g in the centralizer $C_G(h)$ such that $\det g = f$. If this holds for some irreducible constituent of h, then it holds also for h, so it suffices to consider irreducible h. The centralizer of an irreducible h in the matrix algebra $\mathrm{Mat}_r(F_q)$ is a field of degree r over F_q; hence $C_G(h)$ is cyclic of order $q^r - 1$: let c be one of its generators, and γ one of the characteristic roots of c. The other characteristic roots are then the Galois conjugates of γ over F_q, and each must have multiplicative order $q^r - 1$. It follows that

$$\det c = \gamma^{1+q+\cdots+q^{r-1}}$$

and so $\det c$ has multiplicative order $q-1$. Thus each nonzero f in F_q is a power of $\det c$, that is, each such f is the determinant of some power g of c.

STEP 4. All FS-submodules of V_d admit G.

PROOF. This is an argument by contradiction. Let W be minimal among those FG-sections of V_d which have FS-submodules that do not admit G, let W_1 be minimal among these FS-submodules of W, and let W_2 be any simple FG-submodule of W. By the minimality of W_1, any maximal FS-submodule W_3 of W_1 must admit G, and then W/W_3 inherits the relevant properties of W, so by the minimality of W we must have $W_3 = 0$: thus W_1 is a simple FS-module. By the minimality of W used again and again, $(W_1 + W_2)/W_2$ must admit G and so $W_1 + W_2$ must be W. From Step 3 we know that W_2 is simple even as FS-module, so in fact $W = W_1 \oplus W_2$. Thus $W_1 \cong W/W_2$, so from Step 2 we know that W_1 and W_2 cannot be FS-isomorphic: hence W_1 and W_2 are the only simple FS-submodules of W. Since S is normal in G, the simple FS-submodules of W must be permuted by G. This contradicts the assumption that W_2 admits G but W_1 does not, and the proof is complete.

STEP 5. $b \in \overline{\beta}M$ and $\overline{\beta} \in bFM$.

PROOF. The first claim is almost obvious: act on $\overline{\beta}$ by any matrix from M which maps, for each j, the first $b(1,j)$ of the y_{ij} to x_1, the next $b(2,j)$ of the y_{ij} to x_2, and so on.

The second claim is a little harder. Instead of spelling out a formal proof, we shall be content with demonstrating the key idea in action, proving the following related result: if no monomial in bFM involves more indeterminates than b itself, then each nonzero $b(i)$ is a power of p. Suppose not, and permute indeterminates if necessary to arrange that $b(1)$ is neither 0 nor a power of p, none of $b(2), \ldots, b(s)$ is 0, but $b(i) = 0$ whenever $i > s$. Let p^k be the largest p-power divisor of $b(1)$; then the (binomial) coefficient of $x^{b(1)-p^k}y^{p^k}$ in $(x+y)^{b(1)}$ is not divisible by p. Apply to b first the element of M which maps x_1 to $x_1 + x_{s+1}$ and fixes all indeterminates other than x_1, and then apply (b', b') where

$$b' = x_1^{b(1)-p^k} x_{s+1}^{p^k} \prod_{i=2}^{s} x_i^{b(i)} :$$

the result is a nonzero scalar multiple of b'. This proves that $b' \in bFM$, contrary to the fact that b' involves $s+1$ indeterminates, more than b does.

STEP 6. We have $b' \in bFM$ if and only if

$$\sum_{j<k} \beta(j)p^j \geq \sum_{j<k} \beta'(j)p^j \quad \text{for all } k.$$

PROOF. Suppose first that $b' \in bFM$. We know as a consequence of Step 5 that this means $b' \in V_\beta$ so b' is divisible (in the free commutative semigroup of all monomials) by the p^kth power of some monomial of degree $\sum_{j \geq k} \beta(j)p^{j-k}$. On the other hand, the largest p^kth power divisor of b' has degree $\sum_{j \geq k} \beta'(j)p^j$. In view of $\sum \beta(j)p^j = d = \sum \beta'(j)p^j$, the required inequality follows.

Conversely, suppose that the inequalities all hold. Both sides of the inequality involving k being congruent to d modulo p^k, we then have

$$\sum_{j<k} \beta(j)p^j = c(k)p^k + \sum_{j<k} \beta'(j)p^j$$

with nonnegative integers $c(k)$. [In fact, $c(k) = c_k(b) - c_k(b')$.] Then

$$\beta(k) + c(k) - c(k+1)p = \beta'(k) \geq 0 \quad \text{for all } k,$$

with $c(0) = c(e) = 0$. Let m_k be a matrix in M which leaves all indeterminates fixed except the last $c(k+1)p$ of $y_{1,k}, \ldots, y_{\beta(k)+c(k),k}$, maps each of the last p of these to $y_{\beta(k+1)+1,k+1}$, each of the second last p to $y_{\beta(k+1)+2,k+1}$, and so on. Starting with

$$\overline{\beta}m_0 = \prod_{i=1}^{\beta'(0)} y_{i0} \prod_{i=1}^{\beta(1)+c(1)} y_{i1}^p \prod_{j=2}^{e-1} \prod_{i=1}^{\beta(j)} y_{ij}^{p^j},$$

it is straightforward to see that $\overline{\beta}m_0m_1 \cdots m_{e-1} = \overline{\beta}'$. Thus Step 5 gives $b' \in \overline{\beta}'M \subseteq \overline{\beta}M \subseteq bFM$, and the proof is complete.

REFERENCES

1. Martin Aigner, *Combinatorial theory*, Grundlehren Math. Wiss., vol. 234, Springer-Verlag, 1979.

2. Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

3. Stephen R. Doty, *The submodule structure of Weyl modules for groups of type A_n*, Thesis, University of Notre Dame, May 1982.

4. ———, *The submodule structure of certain Weyl modules for groups of type A_n*, J. Algebra **95** (1985), 373–383.

5. Walter Feit, *The representation theory of finite groups*, North Holland, Amsterdam, 1982.

6. J. A. Green, *Polynomial representations of* GL_n, Lecture Notes in Math., vol. 830, Springer-Verlag, 1980.

7. Leonid Krop, *Tensor-type representations of* $\mathrm{Mat}_\infty(Z_p)$, Thesis, University of Chicago, June 1983.

8. ———, *On the representations of the full matrix semigroup on homogeneous polynomials*, J. Algebra **99** (1986), 370–421.

9. ———, *On the representations of the full matrix semigroup on homogeneous polynomials*, II, J. Algebra **102** (1986), 284–300.

10. Warren J. Wong, *On the irreducible modular representations of finite classical groups*, Thesis, Harvard University, 1959.

AUSTRALIAN NATIONAL UNIVERSITY, CANBERRA