Semigroup Algebras of the Full Matrix Semigroup Over a Finite Field
Author(s): L. G. Kovács
Source: *Proceedings of the American Mathematical Society*, Vol. 116, No. 4 (Dec., 1992), pp. 911-919
Published by: American Mathematical Society
Stable URL: http://www.jstor.org/stable/2159467
Accessed: 05/02/2015 00:44

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 4, December 1992

SEMIGROUP ALGEBRAS OF THE FULL MATRIX SEMIGROUP OVER A FINITE FIELD

L. G. KOVÁCS

(Communicated by Ronald Solomon)

ABSTRACT. Let M denote the multiplicative semigroup of all n-by-n matrices over a finite field F and K a commutative ring with an identity element in which the characteristic of F is a unit. It is proved here that the semigroup algebra $K[M]$ is the direct sum of $n+1$ algebras, namely, of one full matrix algebra over each of the group algebras $K[\mathrm{GL}(r, F)]$ with $r = 0, 1, \ldots, n$. The degree of the relevant matrix algebra over $K[\mathrm{GL}(r, F)]$ is the number of r-dimensional subspaces in an n-dimensional vector space over F.

For K a field of characteristic different from that of F, this result was announced by Faddeev in 1976. He only published an incomplete sketch of his proof, which relied on details from the representation theory of finite general linear groups. The present proof is self-contained.

1. THE RESULT

Theorem (Faddeev's Proposition). *Let M denote the multiplicative semigroup of all n-by-n matrices over a finite field F and K a commutative ring with an identity element in which the characteristic of F is a unit. Then the semigroup algebra $K[M]$ is the direct sum of $n+1$ algebras, namely, of one full matrix algebra over each of the group algebras $K[\mathrm{GL}(r, F)]$ with $r = 0, 1, \ldots, n$. The degree of the relevant matrix algebra over $K[\mathrm{GL}(r, F)]$ is the number of r-dimensional subspaces in an n-dimensional vector space over F.*

With K a field of characteristic different from that of F, this was Proposition 5 in Faddeev's paper [3]. While that proposition was introduced with the words "From all that has been said there follows", the sentence before that said that "The full proof" [of the previous proposition] "is complicated, and we omit it", and that proof has remained unpublished. The "route to the proof" described in [3] relied on details from the representation theory of finite general linear groups. The aim of this paper is to present a complete and self-contained proof of the result, in the generality stated above.

Faddeev's Proposition directly implies that $K[M]$ *is semisimple whenever K is a field whose characteristic does not divide the order of* $\mathrm{GL}(n, F)$: this had been conjectured by Munn already in 1973 (and verified for $n \leqslant 4$ in 1976; unpublished). Conversely, once $K[M]$ is known to be semisimple, the

Received by the editors April 16, 1991.
1991 *Mathematics Subject Classification.* Primary 16S36; Secondary 20M25.

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

explicit information given in Faddeev's Proposition is not hard to deduce (§§2 and 3 of this paper suffice). In a very recent paper [5], Okniński and Putcha conjecture much more generally (in the paragraph following Corollary 2.10) the semisimplicity of the monoid algebra of any finite monoid of Lie type over any field whose characteristic does not divide the order of the group of units of that monoid and prove it for the characteristic 0 case (Corollary 2.10). On the other hand, $K[M]$ is *never* semisimple when K is a field whose characteristic is a divisor of the order of $\mathrm{GL}(n, F)$, yet Faddeev's Proposition reveals its structure unless the characteristics of K and F are actually equal. In particular, one can see that $K[M]$ *is a symmetric algebra* (in the sense of Curtis and Reiner [2]) *whenever* K *is a field whose characteristic is not equal to that of* F.

The picture is completely different when K is a field and the two characteristics coincide. According to (7.2) of Glover [4], when $n = 2$ and F is a (finite) prime field, $F[M]$ has infinitely many isomorphism types of indecomposable modules, even though the relevant group algebras have only finitely many. Indeed, his (7.1d) shows that then there exist indecomposable projective $F[M]$-modules that have more than one minimal submodule and therefore cannot be injective; so, far from being symmetric, those $F[M]$ are not even quasi-Frobenius algebras. With too little evidence for a conjecture, let us raise at least a question: *Is the monoid algebra of a finite monoid of Lie type, over a field whose characteristic is different from that of the monoid, always a symmetric (or at least quasi-Frobenius) algebra*?

2. The semigroup

After noting that transposition of matrices is a rank-preserving antiautomorphism of M, coordinatefree language will be better suited to our arguments: so let V be an n-dimensional vector space over F and think of M as the semigroup of all linear maps $V \to V$, with the maps written on the right and composed accordingly (so $\lambda\mu$ means first λ, then μ).

For $r = 0, 1, \ldots, n$, let M^r denote the set of all maps of rank r in M and ε_r an arbitrary idempotent in M^r. Note that there is no choice about ε_0 (which must be the zero map on V, the only element of M^0) or about ε_n (which can only be the identity map on V). The intersection $M^r \cap \varepsilon_r M^r$ consists precisely of the elements of M with kernel $\ker \varepsilon_r$. For the moment, call two of these equivalent if their images are equal: there is then one equivalence class for each r-dimensional subspace U of V, consisting of all elements of M with kernel $\ker \varepsilon_r$ and image U. The equivalence class so corresponding to $\operatorname{im} \varepsilon_r$ is easily seen to be $M^r \cap \varepsilon_r M^r \varepsilon_r$, a subgroup of M, isomorphic to and henceforth referred to as $\mathrm{GL}(r, F)$. By left multiplication, this group permutes each equivalence class regularly. Further, $M^r \subseteq M^r \varepsilon_r M^r$. The straightforward verification of these simple facts concerning the semigroup M is left to the reader.

3. Some ring theory

All algebras considered here will be associative, but they will not be assumed to have identity elements.

Let KM^r be the free K-module with basis M^r turned into a K-algebra by defining multiplication so that the KM^r-product of two elements of M^r is their

M-product if that lies in M^r and 0 otherwise. Note that any rank-preserving antiautomorphism of M yields an antiautomorphism on the algebra KM^r so defined. Set $S^r = \bigcup_{s=0}^{r} M^s$: each S^r is an ideal in M, so each $K[S^r]$ is an ideal in $K[M]$; also, $K[S^0] = KM^0 \cong K$ while $K[S^r]/K[S^{r-1}] \cong KM^r$ whenever $0 < r \leqslant n$.

Subsequent sections of the paper will show that under the hypotheses of the theorem each KM^r does have an identity element. Here we show how the theorem can be derived from that. (When the semisimplicity of $K[M]$ is given, each ideal of $K[M]$, and hence also each KM^r, has an identity element, so the argument ends with this section.)

First, recall the simple fact that if an ideal in a ring with an identity element has an identity element of its own, then that ideal is a direct summand (that is, has an ideal as direct complement). Using this, an easy induction on r yields that $K[S^r] \cong \bigoplus_{s=0}^{r} KM^s$ for $r = 0, 1, \ldots, n$. (For $r = 0$ we have already seen this; when $0 < r \leqslant n$, the inductive hypothesis yields that $K[S^{r-1}]$ has an identity element and, therefore, it has a direct complement in $K[M]$, and then the intersection of $K[S^r]$ with that direct complement is isomorphic to $K[S^r]/K[S^{r-1}]$ and hence to KM^r.) In particular, $K[M]$ is isomorphic to the direct sum of the KM^r.

Second, recall that if R is any ring with an identity element and if e is an idempotent in R such that $ReR = R$, then R is isomorphic to the ring of eRe-endomorphisms of the left eRe-module eR (provided one writes these endomorphisms on the right of eR and composes them accordingly; see, for example, Propositions 4.11 and 21.2 and Exercise 21.6 in [1]). It follows from the observations in §2 above that these conditions are satisfied by $R = KM^r$ and $e = \varepsilon_r$, that with this choice we have $eRe = K[\mathrm{GL}(r, F)]$, and that as a left eRe-module eR is a direct sum of isomorphic copies of the regular eRe-module. Consequently, R is isomorphic to a full matrix algebra over the eRe-endomorphism ring of the regular eRe-module, that is, over eRe itself. The degree of this matrix algebra is the number of regular summands in the direct decomposition of eR, namely, the number of r-dimensional subspaces of V. This proves that the direct summand KM^r of $K[M]$ is a full matrix algebra of the required degree over $K[\mathrm{GL}(r, F)]$.

It remains then to prove that KM^r has an identity element. This will follow for all relevant K if it holds when K is the subring of the rational field generated by the integers and the reciprocal of the characteristic of F; in the sequel, K may as well denote this ring.

4. Some linear algebra

The expression of the identity element of KM^r as a linear combination of elements of M^r will involve only certain kinds of elements of M^r. In this section we establish some properties of the relevant elements. These are independent of the ring K; indeed, most of the argument does not even need the assumption that F is finite.

For any element μ of M, the subspaces $\operatorname{im}\mu$, $\operatorname{im}\mu^2$, ... form a descending chain that must, of course, become stationary. It will be convenient to write $\operatorname{im}\mu^\infty$ for the repeating member of that chain (without envisaging any map called μ^∞) and to call μ *semi-idempotent* if on $\operatorname{im}\mu^\infty$ it acts as 1. We shall

see in the next section that the identity element of KM^r involves only semi-idempotent maps.

Of course, the $\mathrm{GL}(V)$-conjugates of semi-idempotent maps are all semi-idempotent maps. For each μ in M, define the *rank sequence* $\sigma(\mu)$ *of* μ as $\operatorname{rk}\mu, \operatorname{rk}\mu^2, \ldots$ and note that the rank sequences of the $\mathrm{GL}(V)$-conjugates of μ all agree with $\sigma(\mu)$. This gives one half of the following.

Lemma 1. *If μ is a semi-idempotent map, then the semi-idempotent maps with rank sequence $\sigma(\mu)$ are precisely the $\mathrm{GL}(V)$-conjugates of μ.*

Proof. To see the second half, consider the Jordan normal form of μ. Use that $\operatorname{rk}\mu^i - \operatorname{rk}\mu^{i+1}$ is the number of nilpotent Jordan blocks of degree greater than i and that the nonnilpotent Jordan blocks of a semi-idempotent map are identity matrices. □

We shall also have to work with certain restrictions of semi-idempotent maps. To set these into context, consider first arbitrary *partial maps*: linear maps from subspaces of V into V. We take the view that any two partial maps have a composite, the domain of $\pi\rho$ consisting of all those elements of $\operatorname{dom}\pi$ whose image under π lies in $\operatorname{dom}\rho$. It is easy to see that this composition is an associative operation, so there is no ambiguity in speaking of powers π^i of any partial map π (and the powers of any one partial map commute with each other). Similarly, there is no problem in defining $\operatorname{im}\pi^\infty$ and $\sigma(\pi)$ [define $\operatorname{rk}\pi$ as $\dim(\operatorname{im}\pi)$], and it is easy to see that $\operatorname{im}\pi^\infty \subseteq \operatorname{dom}\pi$. We call π semi-idempotent if it acts on $\operatorname{im}\pi^\infty$ as 1. One of the facts we need to establish is the relevant analogue of Lemma 1.

Lemma 2. *If π is a one-to-one semi-idempotent partial map, then the one-to-one semi-idempotent partial maps with rank sequence $\sigma(\pi)$ are precisely the $\mathrm{GL}(V)$-conjugates of π.*

As in the deduction of Lemma 1, the only nontrivial part of the proof is to show that if two one-to-one semi-idempotent partial maps have the same rank sequence then they are $\mathrm{GL}(V)$-conjugate. We leave that to the end of this section.

From the general context of partial maps, we shall need one more observation. If π is a one-to-one partial map, it has an 'inverse' that we write as $\bar{\pi}$; so $\operatorname{dom}\bar{\pi} = \operatorname{im}\pi$, while $\pi\bar{\pi}$ and $\bar{\pi}\pi$ are identity maps with $\operatorname{dom}(\pi\bar{\pi}) = \operatorname{dom}\pi$ and $\operatorname{dom}(\bar{\pi}\pi) = \operatorname{im}\pi$. (Beware: π and $\bar{\pi}$ do not commute unless $\operatorname{dom}\pi = \operatorname{im}\pi$.) Of course if π is one-to-one then so is $\bar{\pi}$, and the 'inverse' of $\bar{\pi}$ is π itself. It is easy to verify that, for $i = 1, 2, \ldots$,

$$\pi^{i+1}\bar{\pi} \text{ is the restriction of } \pi^i \text{ to } \operatorname{dom}\pi^{i+1}, \tag{1}$$

$$\operatorname{im}\pi^{i+1}\bar{\pi} = \operatorname{im}\pi^i \cap \operatorname{im}\pi^i\bar{\pi}. \tag{2}$$

In one direction, the connection between semi-idempotent maps and the partial maps of Lemma 2 is provided by a simple observation.

Lemma 3. *If μ is a semi-idempotent map and if π is the restriction of μ to a subspace of V that avoids $\ker\mu$, then π is a one-to-one semi-idempotent partial map whose rank sequence is majorized by that of μ,*

$$\dim(\operatorname{im}\pi^i) \leqslant \dim(\operatorname{im}\mu^i) \quad \textit{for } i = 1, 2, \ldots.$$

Proof. If π is a restriction of μ, then $\operatorname{im}\pi^i \subseteq \operatorname{im}\mu^i$ for $i = 1, 2, \ldots, \infty$. □

In the other direction, we have to work harder.

Lemma 4. *If π is a one-to-one semi-idempotent partial map, then it is the restriction of at least one semi-idempotent map μ with rank sequence equal to that of π; moreover, when F is finite, the number of such μ is a power of the characteristic of F.*

These four lemmas together will imply what we need for the next section.

Lemma 5. *Let π be a one-to-one semi-idempotent partial map and τ a nonincreasing sequence of nonnegative integers. When F is finite, the number of semi-idempotent maps μ that on $\operatorname{dom}\pi$ agree with π and that have rank sequence τ, depends only on $\sigma(\pi)$ and τ. This number is 0 unless $\sigma(\pi)$ is majorized by τ, and it is a power of the characteristic of F whenever $\sigma(\pi) = \tau$.*

Proof. Let T be the set of the μ in question, and let T' be defined similarly with reference to another one-to-one semi-idempotent partial map π' but the same sequence τ. If $\sigma(\pi) = \sigma(\pi')$, then there is a γ in $\mathrm{GL}(V)$ such that $\gamma^{-1}\pi\gamma = \pi'$, and for any such γ we also have that $\gamma^{-1}T\gamma = T'$. □

It remains to prove Lemmas 2 and 4. We start with the latter.

Proof of Lemma 4. Dimension count shows that if μ is one of the desired maps then $\ker\mu$ complements $\operatorname{dom}\pi$ and therefore determines μ (as the only linear map that annihilates $\ker\mu$ and acts on $\operatorname{dom}\pi$ as π). We prove also that in this case

$$\operatorname{im}\pi^i = \operatorname{im}\pi^{i+1}\bar{\pi} \oplus (\ker\mu \cap \operatorname{im}\pi^i) \quad \text{for } i = 1, 2, \ldots .$$

To this end, note first that the two summands on the right-hand side lie in $\operatorname{dom}\pi$ and $\ker\mu$, respectively, so they are disjoint; by (2), their sum lies in $\operatorname{im}\pi^i$. Next, $\sigma(\pi) = \sigma(\mu)$ and $\operatorname{im}\pi^i \subseteq \operatorname{im}\mu^i$ together give that in fact $\operatorname{im}\pi^i = \operatorname{im}\mu^i$. As $\dim(\operatorname{im}\pi^{i+1}\bar{\pi}) = \dim(\operatorname{im}\pi^{i+1})$ and $\dim(\ker\mu \cap \operatorname{im}\mu^i) = \dim(\operatorname{im}\mu^i) - \dim(\operatorname{im}\mu^{i+1})$, it follows that the dimension of this sum is equal to that of $\operatorname{im}\pi^i$, and the displayed equation is established.

Conversely, let U be any complement to $\operatorname{dom}\pi$ such that

$$\operatorname{im}\pi^i = \operatorname{im}\pi^{i+1}\bar{\pi} \oplus (U \cap \operatorname{im}\pi^i) \quad \text{for } i = 1, 2, \ldots . \tag{3}$$

Of course, π is a restriction of the unique linear map μ_U that annihilates U and acts on $\operatorname{dom}\pi$ as π. By induction on i, it follows from $V = U \oplus \operatorname{dom}\pi$ and (3) that $\operatorname{im}\mu_U^i = \operatorname{im}\pi^i$ for $i = 1, 2, \ldots, \infty$; so the rank sequences of μ_U and π agree and, as $\operatorname{im}\pi^\infty \subseteq \operatorname{dom}\pi$ and π is semi-idempotent, μ_U is semi-idempotent.

These observations have reduced the lemma to the claim that $\operatorname{dom}\pi$ does have complements U satisfying (3) and that when F is finite the number of such complements is a power of the characteristic of F.

Let k be chosen so that $\operatorname{im}\pi^k = \operatorname{im}\pi^\infty$. If U is one of the desired complements of $\operatorname{dom}\pi$, it gives rise to a descending chain of subspaces U_i defined by

$$U_i = U \cap \operatorname{im}\pi^i, \tag{4}$$

which obviously have the following properties:

(5) $$U_k = U_{k+1} = \cdots = 0;$$

(6) U_i/U_{i+1} is a complement to $(U_{i+1}+\operatorname{im}\pi^{i+1}\bar{\pi})/U_{i+1}$ in $\operatorname{im}\pi^i/U_{i+1}$ whenever $i = 1, 2, \ldots$;

(7) $$U/U_1 \text{ is a complement to } (U_1 \oplus \operatorname{dom}\pi)/U_1 \text{ in } V/U_1.$$

Conversely, let $U, U_1, U_2, \ldots$ be a descending chain of subspaces of V satisfying these three conditions: we prove next that then U is a complement of the desired kind and (4) holds. To this end, use downward induction on i to show that $U_i \cap \operatorname{im}\pi^i\bar{\pi} = 0$ for $i = k+1, k, \ldots, 1$. The inductive step is that, when $k > i > 0$,

$$\begin{aligned} U_i \cap \operatorname{im}\pi^i\bar{\pi} &= U_i \cap (U_{i+1}+\operatorname{im}\pi^i\bar{\pi}) \cap \operatorname{im}\pi^i\bar{\pi} \quad \text{because } \operatorname{im}\pi^i\bar{\pi} \leqslant U_{i+1}+\operatorname{im}\pi^i\bar{\pi} \\ &= U_{i+1} \cap \operatorname{im}\pi^i\bar{\pi} \quad \text{by (6)} \\ &= U_{i+1} \cap \operatorname{im}\pi^i \cap \operatorname{im}\pi^i\bar{\pi} \quad \text{because } U_{i+1} \leqslant \operatorname{im}\pi^i \\ &= U_{i+1} \cap \operatorname{im}\pi^{i+1}\bar{\pi} \quad \text{by (2)} \\ &= 0 \quad \text{by the inductive hypothesis.} \end{aligned}$$

Using (7) and one other similar step, namely,

$$U \cap \operatorname{dom}\pi = U \cap (U_1 + \operatorname{dom}\pi) \cap \operatorname{dom}\pi = U_1 \cap \operatorname{im}\pi\bar{\pi} = 0,$$

we see that U is indeed a complement to $\operatorname{dom}\pi$ in V. Since (6) directly gives that $\operatorname{im}\pi^i = U_i + \operatorname{im}\pi^{i+1}\bar{\pi}$, and since $U \cap (U_i + \operatorname{im}\pi^{i+1}\bar{\pi}) = U_i + (U \cap \operatorname{im}\pi^{i+1}\bar{\pi})$ by Dedekind's Law, (3) and (4) now follow.

We have proved that if one takes (5) as a definition, chooses $U_{k-1}, \ldots, U_1$ in that order subject only to (6), and finally chooses U subject to (7), then the U so obtained is a complement to $\operatorname{dom}\pi$ that satisfies (3) and that each such complement is canonically obtained this way. When F is finite, the number of complements of a subspace in an F-space is always a power of the number of elements of F, so the total number of choices in this canonical construction is a power of the characteristic of F. This completes the proof of Lemma 4. □

In preparation for the proof of Lemma 2, we extend this argument as follows. Given π, let $k, U, U_1, U_2, \ldots$ be chosen as above; and recall that, by (3) and (4),

$$\operatorname{im}\pi^i = U_i \oplus \operatorname{im}\pi^{i+1}\bar{\pi} \quad \text{for } i = 1, 2, \ldots.$$

With $i = 1$, this gives

$$\operatorname{dom}\pi = \operatorname{im}\pi\bar{\pi} = (U_1 \oplus \operatorname{im}\pi^2\bar{\pi})\bar{\pi} = U_1\bar{\pi} \oplus \operatorname{im}\pi^2\bar{\pi}^2.$$

Similarly, $\operatorname{im}\pi^2\bar{\pi}^2 = U_2\bar{\pi}^2 \oplus \operatorname{im}\pi^3\bar{\pi}^3$, and therefore $\operatorname{dom}\pi = U_1\bar{\pi} \oplus U_2\bar{\pi}^2 \oplus \operatorname{im}\pi^3\bar{\pi}^3$. After $k-1$ such steps, one concludes that

$$\operatorname{dom}\pi = \left(\bigoplus_{i=1}^{k-1} U_i\bar{\pi}^i\right) \oplus (\operatorname{im}\pi^\infty)\bar{\pi}^k.$$

Of course $\bar{\pi}$ acts on $\operatorname{im}\pi^\infty$ as 1, so the last summand is just $\operatorname{im}\pi^\infty$ and π acts on it as 1. The first summand is mapped by π into U, and each of the middle summands is mapped into its predecessor, $(U_i\bar{\pi}^i)\pi = U_i\bar{\pi}^{i-1} \subseteq U_{i-1}\bar{\pi}^{i-1}$ whenever $1 < i < k$.

Next, choose a basis B_k for the last summand $\operatorname{im}\pi^\infty$, a basis B_{k-1} for the second last summand $U_{k-1}\bar{\pi}^{k-1}$, and continue inductively: if $1 < i < k$ and we have already chosen a basis B_i for $U_i\bar{\pi}^i$, note that $B_i\pi$ is a linearly independent subset of $U_{i-1}\bar{\pi}^{i-1}$ and extend it to a basis B_{i-1} of this subspace. Finally, once B_1 is chosen, extend $B_1\pi$ to a basis B_0 of U and set $B = \bigcup_{i=0}^k B_i$. By the foregoing, the B so defined is a basis of V such that the semi-idempotent μ_U maps $(B \setminus \ker\mu_U)$ one-to-one into B. It is easy to see in general that if a basis has this property for some semi-idempotent, then that basis can be so ordered that the corresponding matrix of that semi-idempotent is in Jordan normal form. The conclusion that we shall use in the proof of Lemma 2 is that *each relevant π is the restriction of a semi-idempotent μ whose rank sequence equals that of π, and to which there is an ordered basis B such that the corresponding matrix of μ is in Jordan normal form and $B \setminus \ker\mu$ spans* $\operatorname{dom}\pi$. We shall also use tacitly that two matrices in Jordan normal form that correspond to one map can differ only in the order of their indecomposable blocks, so if one matrix corresponds to the map with respect to one ordered basis, the other matrix will also correspond to it with respect to a different order on the same basis.

Proof of Lemma 2. Let π and π' be partial maps of the relevant kind, with equal rank sequences: what we need to show is that there is a γ in $\mathrm{GL}(V)$ such that $(\operatorname{dom}\pi)\gamma = \operatorname{dom}\pi'$ and $(v\gamma)\pi' = (v\pi)\gamma$ for each v in $\operatorname{dom}\pi$. Choose μ to match π as above and μ' to match π' similarly; since these semi-idempotents have equal rank sequences, they have a common Jordan normal form. We know from our preparations that this common form will appear with respect to suitably ordered bases B and B', say, which are such that $B \setminus \ker\mu$ spans $\operatorname{dom}\pi$ and $B' \setminus \ker\mu'$ spans $\operatorname{dom}\pi'$. Explicitly, there is a matrix (f_{rs}) such that, with $B = \{b_1, \ldots, b_n\}$ and $B' = \{b'_1, \ldots, b'_n\}$, we have

$$b_r\mu = \sum f_{rs}b_s \quad \text{and} \quad b'_r\mu' = \sum f_{rs}b'_s.$$

Define γ by $b_r\gamma = b'_r$ for $r = 1, \ldots, n$; then clearly $\gamma\mu' = \mu\gamma$. It follows that $(\ker\mu)\gamma = \ker\mu'$, so $(B \setminus \ker\mu)\gamma = B' \setminus \ker\mu'$ and hence $(\operatorname{dom}\pi)\gamma = \operatorname{dom}\pi'$. Of course now also $(v\gamma)\pi' = v\gamma\mu' = v\mu\gamma = (v\pi)\gamma$ for each v in $\operatorname{dom}\pi$, and the proof of Lemma 2 is complete. □

5. Identity elements

We are now ready to seek the identity element, e say, of KM^r, as a K-linear combination of the semi-idempotents μ in M^r. Conjugation by elements of $\mathrm{GL}(V)$ provides algebra automorphisms of KM^r that must, of course, fix e; hence conjugate maps must have the same coefficient in this expression. It follows that the coefficient of μ in e will depend on μ only via the rank sequence

$\sigma(\mu)$. What we seek is, therefore, one element k_τ in K to each relevant sequence τ, such that $e = \sum_\mu k_{\sigma(\mu)}\mu$ is the identity element of KM^r. The e so defined is a right identity if and only if, whenever α and β are elements of M^r, the sum of the $k_{\sigma(\mu)}$ over the μ with $\alpha\mu = \beta$ is 1 if $\alpha = \beta$ and 0 otherwise. This condition amounts to a system of simultaneous linear equations with the k_τ as the *unknowns*. In any algebra that has an anti-automorphism, a right identity element is neecessarily two-sided (and unique), so all we have to prove is that this system has at least one solution in K.

While formally this system consists of one equation for each pair α, β, some of these equations may be vacuous and others may occur repeatedly. When $\{\mu \mid \alpha\mu = \beta\}$ is empty, in the corresponding equation all coefficients (on both sides) vanish. When this set is nonempty, we must have $\ker\alpha = \ker\beta$, and so there is a one-to-one partial map π with $\operatorname{dom}\pi = \operatorname{im}\alpha$ such that $\alpha\pi = \beta$; moreover, this π is the restriction of at least one semi-idempotent and therefore (by Lemma 3) it is semi-idempotent. The coefficient of k_τ in the corresponding equation is then the number of those semi-idempotent μ that on $\operatorname{dom}\pi$ agree with π and that have rank sequence τ. By Lemma 5, this number depends on α and β only via $\sigma(\pi)$, so the equations corresponding to pairs α, β with a common $\sigma(\pi)$ are all the same; call it the equation corresponding to $\sigma(\pi)$. Further by Lemma 5, the coefficient of k_τ in this equation is 0 unless τ majorizes $\sigma(\pi)$, and it is a power of the characteristic of F when $\tau = \sigma(\pi)$. Consequently, when the equations and the unknowns are listed according to lexicographic order on the set of the relevant sequences, the system is triangular and all the diagonal coefficients are powers of the characteristic of F. Since the latter are units in K, the system does have a solution in K, and therefore KM^r has an identity element (of this particular form).

This completes the proof of Faddeev's Proposition.

For a consequence mentioned in the introduction, we need to know also that if K is a field and G is a finite group then each full matrix algebra over $K[G]$ is a symmetric algebra. It is an easy exercise to check that mapping each matrix first to its trace and then to the coefficient of the identity element of G in that trace, provides the linear function ν required in Remark 1, §66 of [2].

Acknowledgments

I have benefited from several discussions on this subject with Professor Douglas Munn, the first in 1973. His semisimplicity proof for $n \leqslant 4$ went by explicitly calculating the identity elements of the KM^r with $r = 1, 2, n-1$ (any n). I am also indebted to Professor Louis Solomon, who showed me a preprint of [5] and some related work of his own, and to MSRI Berkeley for the meeting last December where Professor Solomon revived my interest in this topic.

References

1. Frank W. Anderson and Kent R. Fuller, *Rings and categories of modules*, Graduate Texts in Math., vol. 13, Springer-Verlag, New York, Heidelberg, and Berlin, 1974.
2. Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure Appl. Math., vol. 11, Interscience-Wiley, New York and London, 1962.

3. D. K. Faddeev, *Representations of the full matrix semigroup over a finite field*, Dokl. Akad. Nauk SSSR **230** (1976), 1290–1293; English transl., Soviet Math. Dokl. **17** (1976), 1483–1486.
4. D. J. Glover, *A study of certain modular representations*, J. Algebra **51** (1978), 425–475.
5. Jan Okniński and Mohan S. Putcha, *Complex representations of matrix semigroups*, Trans. Amer. Math. Soc. **323** (1991), 563–581.

Mathematics Institute of Advanced Study, Australian National University, GPO Box 4, Canberra 2601, Australia
E-mail address: kovacs@pell.anu.edu.au