Abstract

This paper addresses various questions about pairs of similarity classes of matrices which contain commuting elements. In the case of matrices over finite fields, we show that the problem of determining such pairs reduces to a question about nilpotent classes; this reduction makes use of class types in the sense of Steinberg and Green. We investigate the set of scalars that arise as determinants of elements of the centralizer algebra of a matrix, providing a complete description of this set in terms of the class type of the matrix.

Several results are established concerning the commuting of nilpotent classes. Classes which are represented in the centralizer of every nilpotent matrix are classified—this result holds over any field. Nilpotent classes are parametrized by partitions; we find pairs of partitions whose corresponding nilpotent classes commute over some finite fields, but not over others. We conclude by classifying all pairs of classes, parametrized by two-part partitions, that commute. Our results on nilpotent classes complement work of Košir and Oblak.

Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

On types and classes of commuting matrices over finite fields

John R. Britnell and Mark Wildon

1. *General introduction*

Let $\mathbf{F}_q$ be a finite field, and let C and D be classes of similar matrices in $\mathrm{Mat}_n(\mathbf{F}_q)$. We say that C and D *commute* if there exist commuting matrices X and Y such that $X \in C$ and $Y \in D$. In this paper we are concerned with the problem of deciding which similarity classes commute.

A matrix is determined up to similarity by its rational canonical form. This however is usually too sharp a tool for our purposes, and many of our results are instead stated in terms of the *class type* of a matrix. This notion, which seems first to have appeared in the work of Steinberg [**14**], is important in Green's influential paper [**8**] on the characters of finite general linear groups. Lemma 2.1 of that paper implies that the type of a matrix determines its centralizer up to isomorphism; this fact is also implied by our Theorem 2.7, which says that two matrices with the same class type have conjugate centralizers.

The main body of this paper is divided into three sections. In §2 we develop a theory of commuting class types; the results of this section reduce the general problem of determining commuting classes to the case of nilpotent classes. A key step in this reduction is Theorem 2.8, which states that if similarity classes C and D commute, then any class of the type of C commutes with any class of the type of D.

Relationships between class types and determinants are discussed in §3. We provide a complete account of those scalars which appear as determinants in the centralizer of a matrix of a given type; this result, stated as Theorem 3.1, has appeared without proof in [**2**, §3.4], and as we promised there, we present the proof here. We also discuss the problem of determining which scalars appear as the determinant of a matrix of a given type. This problem appears intractable in general, and we provide only a very partial answer. But we identify a special case of the problem which leads to a difficult but highly interesting combinatorial problem, to which we formulate Conjecture 3.14 as a plausible solution.

In §4 we make several observations concerning the problem of commuting nilpotent classes; this is a problem which has attracted attention in several different contexts over the years, and there is every reason to suppose that it is hard. Among other results, we determine

---

2000 *Mathematics Subject Classification* 15A27 (primary), 15A15, 15A21 (secondary).

The research was supported in part by the Heilbronn Institute for Mathematical Research.

in Theorem 4.6 the nilpotent classes which commute with every other nilpotent class of the same dimension, and in Theorem 4.10 we classify all pairs of commuting nilpotent classes of matrices whose nullities are at most 2. We describe a construction on matrices which produces interesting and non-obvious examples of commuting nilpotent classes. This construction motivates Theorem 4.8, which says that for every prime p and positive integer r, there exists a pair of classes of nilpotent matrices which commute over the field $\mathbf{F}_{p^a}$ if and only if $a > r$. As far as the authors are aware, it has not previously been observed that the commuting of nilpotent classes, as parameterized by partitions, is dependent on the field of definition.

More detailed outlines of the results of §2, §3 and §4 are to be found at the beginnings of those sections.

1.1. *Background definitions*

We collect here the main prerequisite definitions concerning partitions, classes and class types that we require.

Partitions. We define a *partition* to be a weakly decreasing sequence of finite length whose terms are positive integers; these terms are called the *parts* of the partition. We shall denote the j-th part of a partition λ by $\lambda(j)$. The sum of the parts of λ is written as $|\lambda|$.

Given partitions λ and μ, we write $\lambda + \mu$ for the partition of $|\lambda| + |\mu|$ whose multiset of parts is the union of the multisets of parts of λ and of μ. We shall write 2λ for $\lambda + \lambda$, and similarly we shall define $t\lambda$ for all integers $t \in \mathbf{N}_0$. A partition μ will be said to be *t-divisible* if it is expressible as $t\lambda$ for some partition λ; if $s\lambda = t\mu$ then we may write $\mu = \frac{s}{t}\lambda$.

We shall require the *dominance order* $\trianglerighteq$ on partitions. For two partitions λ and μ we say that λ *dominates* μ, and write $\lambda \trianglerighteq \mu$ (or $\mu \trianglelefteq \lambda$) if

$$\sum_{i=1}^{j} \lambda(i) \geq \sum_{i=1}^{j} \mu(i)$$

for all $j \in \mathbf{N}$. (If i exceeds the number of parts in a partition, then the corresponding part is taken to be 0.)

Let λ be a partition with largest part $\lambda(1) = a$. The *conjugate partition* $\overline{\lambda}$ is defined to be $(\overline{\lambda}(1), \ldots, \overline{\lambda}(a))$, where $\overline{\lambda}(j)$ is the number of parts of λ of size at least j. It is a well-known fact (see for instance [**11**, 1.11]) that the conjugation operation on partitions reverses the dominance order; that is, $\lambda \trianglerighteq \mu$ if and only if $\overline{\mu} \trianglerighteq \overline{\lambda}$.

A geometric interpretation of the dominance order is developed by Gerstenhaber in [**5**] and [**6**]; the issues with which the latter paper is concerned are similar in many respects to those considered in §4 of the present paper, although Gerstenhaber's approach using algebraic varieties is very different.

Similarity classes. Let K be a field. A class of similar matrices in $\mathrm{Mat}_n(K)$ is determined by the following data: a finite set $\mathcal{F}$ of irreducible polynomials over K, and for each $f \in \mathcal{F}$ a partition λ_f of a positive integer, such that

$$n = \sum_{f \in \mathcal{F}} |\lambda_f| \deg f.$$

The characteristic polynomial of a matrix M in this class is $\prod_f f^{|\lambda_f|}$. There is a decomposition of V given by

$$V = \bigoplus_f \bigoplus_j V_f(j),$$

where M acts indecomposably on the subspace $V_f(j)$ with characteristic polynomial $f^{\lambda_f(j)}$. This decomposition is, in general, not unique. By a change of basis, we may express M as $\bigoplus_f \bigoplus_j P_f(j)$, where $P_f(j)$ is a matrix representing the action of M on $V_f(j)$; we say that $P_f(j)$ is a *cyclic block* of M.

If $\mathcal{F} = \{f_1, \ldots, f_t\}$ and the associated partitions are $\lambda_1, \ldots, \lambda_t$ respectively, then we shall define the *cycle type* of M to be the formal expression

$$\mathrm{cyc}(M) = f_1^{\lambda_1} \cdots f_t^{\lambda_t}.$$

The order in which the polynomials appear in this expression is, of course, unimportant.

Nilpotent classes. We shall denote by $N(\lambda)$ the similarity class of nilpotent matrices with cycle type f_0^λ, where $f_0(x) = x$. We denote by $J(\lambda)$ the unique matrix in upper-triangular Jordan form in the similarity class $N(\lambda)$.

If $\lambda = (\lambda(1), \ldots, \lambda(k))$ we shall omit unnecessary brackets by writing $N(\lambda(1), \ldots, \lambda(k))$ for $N(\lambda)$ and $J(\lambda(1), \ldots, \lambda(k))$ for $J(\lambda)$.

Class types. More general than the notion of similarity class is that of class type. If M is a matrix of cycle type $f_1^{\lambda_1} \cdots f_t^{\lambda_t}$, where for each i the polynomial f_i has degree d_i, then the *class type* of M is the formal string

$$\mathrm{ty}(M) = d_1^{\lambda_1} \cdots d_t^{\lambda_t}.$$

Here too, the order of the terms is unimportant.

Any string of this form will be called a *type*. The *dimension* of the type $d_1^{\lambda_1} \cdots d_t^{\lambda_t}$ is defined to be $d_1|\lambda_1| + \cdots + d_t|\lambda_t|$. We shall say that the type T is *representable* over a field K if there exists a matrix of class type T with entries in K; the dimension of such a matrix is the same as the dimension of the type. Clearly not all types are representable over all fields; for instance the type $1^\lambda 1^\mu 1^\nu$ is not representable over $\mathbf{F}_2$ since there are only two distinct linear polynomials over this field; similarly 3^λ is not representable over $\mathbf{R}$ since there are no irreducible cubics over $\mathbf{R}$.

Similar matrices have the same cycle type and the same class type, and so we may meaningfully attribute types of either kind to similarity classes.

We shall say that a class type T is *primary* if it is d^λ for some d and λ. Otherwise T is *compound*. If d^λ appears as a term in the type T, we say that d^λ is a *primary component* of T. We may also say that a matrix, a similarity class of matrices, or a cycle type is primary or compound, according to its class type, and we may refer to its primary components.

We have already defined what it means for two similarity classes to commute. We generalise this idea to types, as follows.

DEFINITION. Let S and T be class types. We say that S and T *commute* over a field K if there are matrices X and Y over K such that X has class type S, and Y has class type T, and X and Y commute.

The field K will not always be mentioned explicitly if it is clear from the context.

2. *Commuting types of matrices*

This section proceeds as follows. In §2.1 we prove several results relating the class type of a polynomial in a matrix M to the class type of M, leading up to Theorem 2.6: that two similarity classes have the same class type if and only if they contain representatives which are polynomial in one another. This result is then used in the proof of Theorem 2.8, which states that two similarity classes commute if and only if their class types commute.

Using Theorem 2.8, we proceed to reduce our original problem of deciding which similarity classes commute, first to the case of primary types in §2.2, and thence to the case of nilpotent classes in §2.3. At the end of §2.3 we give examples illustrating both steps of this reduction.

2.1. *Polynomials and commuting types*

If M is a matrix of primary class type d^λ then it has associated with it a single irreducible polynomial f such that its cycle type is f^λ. It is clear that $f(M)$ is nilpotent. The following lemma and proposition describe its associated partition.

LEMMA 2.1. *Let M be a matrix of cycle type f^λ, where $\deg f = d$. For each j, let m_j be the number of parts of λ of size j. Then*

$$dm_j = (\operatorname{null} f(M)^j - \operatorname{null} f(M)^{j-1}) - (\operatorname{null} f(M)^{j+1} - \operatorname{null} f(M)^j).$$

Proof. Let P be a cyclic block of M. If the dimension of P is dh then the characteristic polynomial of P is f^h. If $j \geq h$, then $\operatorname{null} f(P)^j = dh$; otherwise $\operatorname{null} f(P)^j = dj$.

Since M is a direct sum of cyclic blocks of dimensions $d\lambda(1), d\lambda(2), \ldots$, it follows that

$$\operatorname{null} f(M)^j = \sum_{h \leq j} dhm_h + \sum_{h > j} djm_h,$$

and hence

$$\operatorname{null} f(M)^{j+1} - \operatorname{null} f(M)^j = \sum_{h>j} dm_h.$$

This implies the lemma. □

PROPOSITION 2.2. *Let M be a matrix of primary type d^λ. If the cycle type of M is f^λ then $f(M)$ is nilpotent of type $1^{d\lambda}$.*

Proof. Since $f(M)$ is nilpotent, it is primary and its associated polynomial, $f_0(x) = x$, is linear. The result is now immediate from Lemma 2.1. □

We use the preceding proposition to give some information about the type of $F(M)$, where M is a primary matrix and F is any polynomial. The following lemma will be required.

LEMMA 2.3. *Let M and N be nilpotent matrices with associated partitions μ and ν respectively. Then $\mu \trianglelefteq \nu$ if and only if* $\operatorname{rank} M^j \leq \operatorname{rank} N^j$ *for all $j \in \mathbf{N}$.*

Proof. The rank of M^j is equal to the sum of the j smallest parts of the conjugate partition $\overline{\mu}$. The rank of N^j can be calculated similarly in terms of $\overline{\nu}$. It follows easily that $\operatorname{rank} M^j \leq \operatorname{rank} N^j$ for all j if and only if $\overline{\mu} \trianglerighteq \overline{\nu}$. The lemma now follows from the fact that the dominance order $\trianglerighteq$ is reversed by conjugation of partitions. □

PROPOSITION 2.4. *Let X be a primary matrix of class type d^λ with entries from a field K, and let $F \in K[x]$ be any polynomial. The type of $F(X)$ is e^μ for some e dividing d, and some partition μ such that $e|\mu| = d|\lambda|$ and $e\mu \trianglelefteq d\lambda$.*

Proof. Let the cycle type of X be f^λ where f is an irreducible polynomial of degree d. If α is a root of f in a splitting field, then the eigenvalues of $F(X)$ are the conjugates over K of $F(\alpha)$. Hence $F(X)$ is of primary type, and if $g \in K[x]$ is the irreducible polynomial associated with $F(X)$, then the degree of g divides d. Let e^μ be the type of $F(X)$.

Let $Y = F(X)$. We observe that $g(Y) = (g \circ F)(X)$ is a nilpotent matrix, and hence f divides $g \circ F$; let $g \circ F = kf$. By Proposition 2.2, $f(X)$ has type $1^{d\lambda}$, while $g(Y)$ has type $1^{e\mu}$. For each $i \in \mathbf{N}_0$ we have $g(Y)^i = k(X)^i f(X)^i$ and hence $\operatorname{im} g(Y)^i \subseteq \operatorname{im} f(X)^i$. It follows that $\operatorname{rank} g(Y)^i \leq \operatorname{rank} f(X)^i$ for every $i \in \mathbf{N}$. Now from Lemma 2.3 we see that $e\mu \trianglelefteq d\lambda$, as required. □

When K is a finite field, Proposition 2.4 has the following partial converse.

PROPOSITION 2.5. *If X is a primary matrix of class type d^λ with entries from $\mathbf{F}_q$, and D is a similarity class of matrices also of this class type, then there is a polynomial $F \in \mathbf{F}_q[x]$ such that $F(X) \in D$.*

Proof. Let $f \in \mathbf{F}_q[x]$ be the irreducible polynomial associated with X. Suppose that the additive Jordan–Chevalley decomposition of X is $\overline{X} + N$, where $\overline{X}$ is semisimple and N is nilpotent; recall that $\overline{X}$ and N can be expressed as polynomials in X. Without loss of generality, we may suppose that

$$\overline{X} = \mathrm{diag}(P, \ldots, P),$$

where the cyclic block P has minimum polynomial f.

Let g be the irreducible polynomial associated with the similarity class D, and let α and β be roots of f and g respectively in $\mathbf{F}_{q^d}$. There exists a polynomial $G \in \mathbf{F}_q[x]$, coprime with f, such that $G(\alpha) = \beta$. If we define

$$Q = G(P),$$

then Q has minimum polynomial g. Let

$$\overline{Y} = \mathrm{diag}(Q, \ldots, Q).$$

Then $\overline{Y} = G(\overline{X})$, and since $\overline{X}$ is polynomial in X, it follows that $\overline{Y}$ is too. Moreover, if we set $Y = \overline{Y} + N$, then Y is polynomial in X, and it is clear that Y lies in the similarity class D. □

Let C and D be similarity classes of $\mathrm{Mat}_n(\mathbf{F}_q)$. We say that D is *polynomial in* C if there exists a polynomial F with coefficients in $\mathbf{F}_q$ such that $F(X) \in D$ for all $X \in C$.

THEOREM 2.6. *Let C and D be similarity classes of $\mathrm{Mat}_n(\mathbf{F}_q)$. The classes C and D have the same type if and only if C and D are polynomial in one another.*

Proof. We observe that applying a polynomial to a matrix cannot increase its number of primary components. So if C and D are polynomial in one another, then they have the same number of components. Moreover there is a pairing between the primary components $C_1, \ldots, C_t$ of C and $D_1, \ldots, D_t$ of D such that C_i and D_i are polynomial in one another for all i. It will therefore be sufficient to prove the result in the case that both C and D are primary. Suppose that $\mathrm{ty}(C) = d^\lambda$ for some $d \in \mathbf{N}$ and some partition λ. It follows from Proposition 2.4 that D has class type e^μ where e divides d and $e\mu \trianglelefteq d\lambda$. By symmetry we see that $e = d$ and $\lambda = \mu$, as required.

For the converse, suppose that $\mathrm{ty}(C) = \mathrm{ty}(D)$. Let $T_1, T_2, \ldots, T_t$ be the primary components of $\mathrm{ty}(C)$, and let $X = \mathrm{diag}(X_1, \ldots, X_t)$ be an element of C such that $\mathrm{ty}(X_i) = T_i$ for all i. Let the minimum polynomial of the block X_i be $f_i^{a_i}$, where f_i is irreducible. By Proposition 2.5, there exist polynomials $F_1, \ldots, F_t \in \mathbf{F}_q[x]$ such that $\mathrm{diag}(F_1(X_1), \ldots, F_t(X_t)) \in D$. By the

Chinese Remainder Theorem, there exists a polynomial $F \in \mathbf{F}_q[x]$ such that

$$F(x) \equiv F_i(x) \bmod f_i^{a_i}(x) \quad \text{for all } i.$$

And now we see that $F(X) \in D$, as required. □

It was proved by Green [**8**, Lemma 2.1] that the type of a matrix determines its centralizer up to isomorphism. Using Theorem 2.6 we may prove the following stronger result.

THEOREM 2.7. *Let X and Y be matrices in $\mathrm{Mat}_n(\mathbf{F}_q)$ with the same class type. Let $\mathrm{Cent}\, X$ and $\mathrm{Cent}\, Y$ be the centralizers in $\mathrm{Mat}_n(\mathbf{F}_q)$ of X and Y respectively. Then $\mathrm{Cent}\, X$ and $\mathrm{Cent}\, Y$ are conjugate by an element of $\mathrm{GL}_n(\mathbf{F}_q)$.*

Proof. By Theorem 2.6 there exist polynomials F and G such that $F(X)$ is conjugate to Y and $G(Y)$ is conjugate to X. Now the centralizer $\mathrm{Cent}\, F(X)$ is a subalgebra of $\mathrm{Cent}\, X$ which is conjugate to $\mathrm{Cent}\, Y$; similarly the centralizer $\mathrm{Cent}\, G(Y)$ is a subalgebra of $\mathrm{Cent}\, Y$ which is conjugate to $\mathrm{Cent}\, X$. Since $\mathrm{Cent}\, X$ and $\mathrm{Cent}\, Y$ are finite, it is clear that $\mathrm{Cent}\, X = \mathrm{Cent}\, F(X)$ and that $\mathrm{Cent}\, Y = \mathrm{Cent}\, G(Y)$, which suffices to prove the theorem. □

An obvious corollary of Theorem 2.6, which has been stated in [**3**, §3.2], is that classes of the same type commute. We are now in a position to establish a stronger result. Recall that types S and T are said to commute if there exist commuting matrices X and Y with types S and T respectively.

THEOREM 2.8. *Let C and D be similarity classes of matrices over $\mathbf{F}_q$. Then C and D commute if and only if $\mathrm{ty}(C)$ and $\mathrm{ty}(D)$ commute.*

Proof. One half of the double implication is trivial, since if the similarity classes commute then by definition the class types do. For the other half, notice that if $\mathrm{ty}(C)$ and $\mathrm{ty}(D)$ commute then there exist commuting similarity classes C' and D' such that $\mathrm{ty}(C') = \mathrm{ty}(C)$ and $\mathrm{ty}(D') = \mathrm{ty}(D)$. Let X' and Y' be commuting matrices from C' and D' respectively. Then there exist polynomials F and G such that $F(X') \in C$ and $G(Y') \in D$, and clearly $F(X')$ and $G(Y')$ commute. □

We remark that Theorems 2.6, 2.7 and 2.8 do not hold for matrices over an arbitrary field. There are counterexamples in $\mathrm{Mat}_2(\mathbf{Q})$, for instance. Let $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$ be distinct quadratic extensions of $\mathbf{Q}$. Let C and D be the similarity classes of rational matrices with characteristic polynomials $x^2 - \alpha$ and $x^2 - \beta$ respectively; then $\mathrm{ty}(C) = \mathrm{ty}(D) = 2^{(1)}$. Since the eigenvalues α and β are not polynomial in one another, it is clear that neither are C and D. Moreover,

the classes C and D do not commute. It is for this reason that our consideration of commuting types is for the most part restricted to matrices with entries from a finite field.

2.2. *Reduction to primary types*

The next step in our strategy is to reduce the question of which class types commute to the corresponding question about primary types. This is accomplished in Proposition 2.9 below.

We shall need the following two definitions.

DEFINITION. A *separation operation* on a type T is the replacement of a primary component d^λ of T by $d^\mu d^\nu$, where $\lambda = \mu + \nu$. A *separation* of T is a type obtained from T by repeated applications of separation operations.

DEFINITION. Let S and T be types. We shall say that S and T *commute componentwise* over a field K if the primary components of S and T can be ordered so that $S = c_1^{\lambda_1} \cdots c_t^{\lambda_t}$ and $T = d_1^{\mu_1} \cdots d_t^{\mu_k}$, where $c_i^{\lambda_i}$ commutes with $d_i^{\mu_i}$ over K for each i.

This definition, it should be noted, does not preclude the possibility that types S and T commute componentwise, even if one or both of them cannot be represented over the field K. For example, $1^{(1,1,1)}$ commutes componentwise with $1^{(1)}1^{(1)}1^{(1)}$ over $\mathbf{F}_2$ according to the definition, even though the latter type is not representable. The examples at the end of §2.3 illustrate why this freedom is desirable.

PROPOSITION 2.9. *Let S and T be types which are representable over a finite field $\mathbf{F}_q$. Then S and T commute over $\mathbf{F}_q$ if and only if there exist separations $S^\star$ of S and $T^\star$ of T such that $S^\star$ and $T^\star$ commute componentwise.*

Proof. Let X and Y be commuting matrices with entries from $\mathbf{F}_q$, whose types are S and T respectively. It is well known and easy to show that there exists a decomposition $V = V_1 \oplus \cdots \oplus V_t$ such that both X and Y act as transformations of primary type on each of the summands V_i. Suppose that the action of X on V_i has type $c_i^{\lambda_i}$, and the action of Y has type $d_i^{\mu_i}$. Then it is clear that the primary types $c_i^{\lambda_i}$ and $d_i^{\mu_i}$ commute, that $c_1^{\lambda_1} \cdots c_t^{\lambda_t}$ is a separation of S and that $d_1^{\mu_1} \cdots d_t^{\mu_t}$ is a separation of T.

For the converse, suppose that the primary types $c_i^{\lambda_i}$ and $d_i^{\mu_i}$ commute, that $c_1^{\lambda_1} \cdots c_t^{\lambda_t}$ is a separation of S and that $d_1^{\mu_1} \cdots d_t^{\mu_t}$ is a separation of T. Then, from Theorem 2.8, it follows that for any choice of irreducible polynomials f_i of degree c_i and g_i of degree d_i, the classes $f_i^{\lambda_i}$ and $g_i^{\mu_i}$ commute. If X_i and Y_i are commuting representatives of these respective classes, then the matrices $X = \operatorname{diag}(X_1, \ldots, X_t)$ and $Y = \operatorname{diag}(Y_1, \ldots, Y_t)$ commute. Now each primary type $c_i^{\lambda_i}$ derives (under separation operations) from a particular component of S. If we select our polynomials f_i in such a way that blocks deriving from the same component of S have the

same polynomial, then we find that $\mathrm{ty}(X) = S$. Similarly we can choose the polynomials g_i so that $\mathrm{ty}(Y) = T$, and it follows that S and T commute. □

2.3. *Reduction to nilpotent classes*

We now complete the reduction of our general problem of commuting classes to the case of nilpotent classes. Recall that we denote by $N(\lambda)$ the similarity class of nilpotent matrices with cycle type f_0^λ, where $f_0(x) = x$. Recall also that a partition is said to be t-divisible if it is $t\nu$ for some partition ν.

THEOREM 2.10. *Let $S = c^\lambda$ and $T = d^\mu$ be primary types of the same dimension. Let $h = \mathrm{hcf}(c, d)$ and $\ell = \mathrm{lcm}(c, d)$. Then S and T commute over $\mathbf{F}_q$ if and only if λ is $\frac{d}{h}$-divisible, μ is $\frac{c}{h}$-divisible, and the nilpotent classes $N(\frac{h}{d}\lambda)$ and $N(\frac{h}{c}\mu)$ commute over $\mathbf{F}_{q^\ell}$.*

Proof. Suppose that S and T commute over $\mathbf{F}_q$. Let X and Y be commuting elements of $\mathrm{Mat}_n(\mathbf{F}_q)$ with cycle types f^λ and g^μ respectively, where $\deg f = c$ and $\deg g = d$. Let $\alpha_1, \dots, \alpha_c$ be the roots of f and $\beta_1, \dots, \beta_d$ the roots of g in the extension field $\mathbf{F}_{q^\ell}$. Over this extension field, it is easy to see that the cycle types of X and Y are given by

$$\mathrm{cyc}(X) = (x - \alpha_1)^\lambda \cdots (x - \alpha_c)^\lambda,$$
$$\mathrm{cyc}(Y) = (x - \beta_1)^\mu \cdots (x - \beta_d)^\mu.$$

Let $W = \mathbf{F}_{q^\ell}^n$, and let W_{ij} denote the maximal subspace of W on which $X - \alpha_i I$ and $Y - \beta_j I$ are both nilpotent. (So $W = \bigoplus_{ij} W_{ij}$.) Let λ_{ij} and μ_{ij} be the partitions such that the type of X on W_{ij} is $1^{\lambda_{ij}}$ and the type of Y on W_{ij} is $1^{\mu_{ij}}$. Then clearly $\sum_{j=1}^d \lambda_{ij} = \lambda$ for all i, while $\sum_{i=1}^c \mu_{ij} = \mu$ for all j.

Since X and Y have entries in $\mathbf{F}_q$, it follows that the Frobenius automorphism $\xi \mapsto \xi^q$ of $\mathbf{F}_{q^\ell}$ induces an isomorphism between the $\mathbf{F}_{q^\ell}\langle X, Y\rangle$-modules V_{ij} and $V_{i'j'}$ whenever $i - j \equiv i' - j' \bmod h$. Hence

$$\lambda_{ij} = \lambda_{i'j'} \text{ and } \mu_{ij} = \mu_{i'j'} \text{ whenever } i - j \equiv i' - j' \bmod h.$$

Therefore the partitions λ_{ij} for $i \in \{1, \dots, c\}$ and $j \in \{1, \dots, d\}$ are determined by the partitions λ_{1k} for $k \in \{1, \dots, h\}$, and since

$$\lambda = \frac{d}{h} \sum_{k=1}^{h} \lambda_{1k},$$

it follows that λ is $\frac{d}{h}$-divisible. Similarly, μ is $\frac{c}{h}$-divisible.

Now clearly the actions of X and Y on the subspace $\bigoplus_{k=1}^h V_{1k}$ commute. The type of X on this submodule (defined over $\mathbf{F}_{q^\ell}$) is $1^{\lambda_{11}} \cdots 1^{\lambda_{1h}}$, which is a separation of $1^{\frac{h}{d}\lambda}$. Similarly the type of Y on the submodule is a separation of $1^{\frac{h}{c}\mu}$. Hence, by the 'if' direction of Proposition 2.9,

the types $1^{\frac{h}{d}\lambda}$ and $1^{\frac{h}{c}\mu}$ commute over $\mathbf{F}_{q^\ell}$. In particular, it follows from Theorem 2.8 that the nilpotent classes $N(\frac{h}{d}\lambda)$ and $N(\frac{h}{c}\mu)$ commute over this field.

For the converse, let $\lambda' = \frac{h}{d}\lambda$ and $\mu' = \frac{h}{c}\mu$, and suppose that the nilpotent classes $N(\lambda')$ and $N(\mu')$ commute over $\mathbf{F}_{q^\ell}$. We shall denote by m the integer $|\lambda'|$, which of course is equal to $|\mu'|$. Let α and β be elements of $\mathbf{F}_{q^\ell}$ whose degrees over $\mathbf{F}_q$ are c and d respectively. Since $N(\lambda')$ and $N(\mu')$ commute over $\mathbf{F}_{q^\ell}$, so do the classes with cycle types $(x-\alpha)^{\lambda'}$ and $(x-\beta)^{\mu'}$. Let X and Y be commuting elements of these respective classes. Let ϕ be an embedding of the matrix algebra $\mathrm{Mat}_m(\mathbf{F}_{q^\ell})$ into $\mathrm{Mat}_{\ell m}(\mathbf{F}_q)$; then it is not hard to see that $\phi(X)$ has class type c^λ and $\phi(Y)$ has class type d^μ. It follows that these types commute over $\mathbf{F}_q$. □

It is worth noting that Theorem 4.8 below implies that the references to particular fields in the statement of Theorem 2.10 are essential. The following special case of the theorem, however, does not depend on the field of definition.

PROPOSITION 2.11. *Let $d, k \in \mathbf{N}$. The types $d^{(k)}$ and $1^{(k,\dots,k)}$ commute over any field.*

Proof. If the field in question is finite, then the proposition follows from Theorem 2.10. For it suffices to show that the type $\frac{1}{d}(k,\dots,k) = (k)$ commutes with itself over $\mathbf{F}_{q^d}$, and certainly this is the case.

A straightforward modification of the last paragraph of the proof of Theorem 2.10 would allow us to deal with arbitrary fields; however we prefer the following short argument involving tensor products. Let f be an irreducible polynomial of degree d and let P be the companion matrix of f. The type $d^{(k)}$ is represented by the $dk \times dk$ matrix

$$P^{(k)} = \begin{pmatrix} P & I & & \\ & P & I & \\ & & \ddots & \ddots \\ & & & P \end{pmatrix}.$$

Let $J = J(k)$ be the k-dimensional Jordan block with eigenvalue 1. It is clear that $P^{(k)}$ commutes with the tensor product $I \otimes J$ (which is obtained from the matrix above by substituting I for each occurrence of P). And $I \otimes J$ is conjugate to $J \otimes I = \mathrm{diag}(J,\dots,J)$, which has type $1^{(k,\dots,k)}$. Hence the types $d^{(k)}$ and $1^{(k,\dots,k)}$ commute. □

We end this section with two examples of how the steps in our reduction can be carried out, which illustrate the various results of this section.

EXAMPLE. Let p, q, r, s and t be the following irreducible polynomials over $\mathbf{F}_2$:

$$\begin{array}{ll} \text{linear:} & p(x) = x,\ q(x) = x+1; \\ \text{quadratic:} & r(x) = x^2+x+1; \\ \text{cubic:} & s(x) = x^3+x+1,\ t(x) = x^3+x^2+1. \end{array}$$

Let C be the similarity class of matrices over $\mathbf{F}_2$ with cycle type $p^{(12,12)}q^{(2,2,2)}r^{(3)}s^{(1)}$ and let D be the similarity class with cycle type $r^{(7,5)}t^{(2,2,1)}$. We shall prove that C commutes with D.

By Theorem 2.8, this is equivalent to showing that the types

$$\begin{aligned} S &= 1^{(12,12)}1^{(2,2,2)}2^{(3)}3^{(1)}, \\ T &= 2^{(7,5)}3^{(2,2,1)} \end{aligned}$$

commute. This, in turn, will follow from Proposition 2.9, if we can show that S commutes componentwise with the separation $T^\star = 2^{(7,5)}3^{(2)}3^{(2)}3^{(1)}$ of T. (This example was chosen to make the point that it is not necessary that the separated types can be represented over $\mathbf{F}_2$.) By Theorem 2.10 we see that $1^{(12,12)}$ commutes with $2^{(7,5)}$ over $\mathbf{F}_2$ if and only if $1^{(6,6)}$ commutes with $1^{(7,5)}$ over $\mathbf{F}_4$; that this is the case follows from Proposition 4.7 below, which implies that the nilpotent classes $N(6,6)$ and $N(7,5)$ commute over $\mathbf{F}_4$. It is immediate from Theorem 2.10 that $1^{(2,2,2)}$ commutes with $3^{(2)}$, and that $2^{(3)}$ commutes with $3^{(2)}$. Hence S and $T^\star$ commute componentwise, and so C and D commute.

The converse directions of Proposition 2.9 and Theorem 2.10 can in principle be used as part of a argument that two similarity classes do not commute; again, results about commuting of nilpotent classes will generally be needed to complete such an argument. The following example is illustrative.

EXAMPLE. Let the polynomials p, q, r, s and t, the class C, and the type S be as in the previous example. Let D be the similarity class over $\mathbf{F}_2$ with cycle type $r^{(8,4)}t^{(2,2,1)}$. The class type of D is

$$T = 2^{(8,4)}3^{(2,2,1)}.$$

Suppose that a separation T^* of T commutes componentwise with a separation S^* of S; then one of $2^{(8)}$ or $2^{(8,4)}$ is a component of T^*. The first possibility is ruled out since S^* can have no component of dimension 16. The only possible component of S^* of dimension 24 is $1^{(12,12)}$, and so if our supposition is correct, then the primary types $2^{(8,4)}$ and $1^{(12,12)}$ must commute over $\mathbf{F}_2$. By Theorem 2.10, this is the case only if $1^{(8,4)}$ and $1^{(6,6)}$ commute. But by Proposition 4.9 below, the nilpotent classes $N(8,4)$ and $N(6,6)$ do not commute over any field. It follows that C and D do not commute.

3. *Types and determinants*

The main object of this section is to establish Theorem 3.1, concerning determinants of elements of centralizer algebras. The following definition is key.

DEFINITION. Let M be a matrix with class type $d_1^{\lambda_1} \cdots d_t^{\lambda_t}$. The *part-size invariant* of M is defined to be the highest common factor of all of the parts of the partitions $\lambda_1, \ldots, \lambda_t$.

THEOREM 3.1. *Let $M \in \mathrm{Mat}_n(\mathbf{F}_q)$ have part-size invariant k. The determinants which occur in the centralizer of M in $\mathrm{Mat}_n(\mathbf{F}_q)$ are precisely the k-th powers in $\mathbf{F}_q$.*

Part of the motivation for this investigation comes from the authors' paper [**2**] on the distribution of conjugacy classes of a group G across the cosets of a normal subgroup H, where G/H is abelian. The *centralizing subgroup* of a class C with respect to H was defined to be the subgroup $\mathrm{Cent}_G(g) \cdot H$, where $g \in C$ may be chosen arbitrarily. It was proved that if G is finite and G/H is cyclic, then the classes with centralizing subgroup K are uniformly distributed across the cosets of H in K.

Theorem 3.1 treats the case where $G = \mathrm{GL}_n(\mathbf{F}_q)$ and $H = \mathrm{SL}_n(\mathbf{F}_q)$. It is clear that the subgroups K lying in the range $H \leq K \leq G$ may be defined in terms of the determinants of their elements; specifically, the index $|K : H|$ is equal to the order of the subgroup of $\mathbf{F}_q^\times$ generated by the determinants of the matrices in K. Hence, in order to calculate the centralizing subgroup of a matrix, we must decide which determinants occur in its centralizer. The following corollary of Theorem 3.1 shows that the answer to this question depends only on the class type of the matrix concerned.

COROLLARY 3.2. Let $M \in \mathrm{GL}_n(\mathbf{F}_q)$ have part-size invariant k, and let $c = \mathrm{hcf}(q-1, k)$. The centralizing subgroup of the conjugacy class of M is the unique index c subgroup of $\mathrm{GL}_n(\mathbf{F}_q)$ containing $\mathrm{SL}_n(\mathbf{F}_q)$.

In §3.1 below we prove a special case of Theorem 3.1, namely that the determinants in the centralizer of a nilpotent matrix are k-th powers, where k is the part-size invariant. The proof of Theorem 3.1 is completed in §3.2. We end in §3.3 by discussing the natural—but surprisingly hard—question of which scalars can appear as the determinant of a matrix of a given type.

3.1. *Determinants in the centralizer of a nilpotent matrix*

In this section we let $M \in \mathrm{Mat}_n(\mathbf{F}_q)$ be a nilpotent matrix lying in the similarity class $N(\lambda)$. Let $A = \mathrm{Cent}\, M$ be the subalgebra of $\mathrm{Mat}_n(\mathbf{F}_q)$ consisting of the matrices that centralize M. We shall find the composition factors of $V = \mathbf{F}_q^n$ as a right A-module; using this result we

describe the determinants of the matrices of A. For some related results on the lattice of A-submodules of V, the reader is referred to [**7**, Chapter 14].

DEFINITION. For $v \in V$ we define the *height* of v, written $\mathrm{ht}(v)$, to be the least integer h such that $v \in \ker M^h$.

DEFINITION. We shall say that a vector $u \in V$ is a *cyclic vector* for M if u is not in the image of M.

The proof of the following well-known lemma is straightforward, and is omitted.

LEMMA 3.3. *An element $Y \in A$ is uniquely determined by its effect on the cyclic vectors of M. If $u_1, \dots, u_t$ are linearly independent cyclic vectors and $v_1, \dots, v_t$ are any vectors such that $\mathrm{ht}(v_i) \leq \mathrm{ht}(u_i)$ for every i, then there is an element $Y \in A$ such that $u_i Y = v_i$ for each i.*

As in Lemma 2.1, we let m_h be the number of parts of λ of size h. For $h \in \mathbf{N}_0$, we shall write V_h for $\ker M^h$.

PROPOSITION 3.4. *For each $h \in \mathbf{N}$, the subspace V_h is an A-submodule of V containing $V_{h+1}M + V_{h-1}$ as an A-submodule. Moreover if $m_h \neq 0$ then*

$$V_h \,/\, (V_{h+1}M + V_{h-1})$$

is a simple A-module of dimension m_h.

Proof. The proof of the first statement is straightforward, and we omit it; we shall outline a proof of the second statement.

Let $u_1, \dots, u_{m_h}$ be a maximal set of linearly independent cyclic vectors each of height h. It is not hard to see that $u_1, \dots, u_{m_h}$ span a complement in V_h to $V_{h+1}M + V_{h-1}$. By the previous lemma, for any vectors $v_1, \dots, v_{m_h}$ in V_h, there exists $Y \in A$ such that $u_i Y = v_i$ for each i. This implies that A acts as a full matrix algebra in its action on the quotient module $V_h/(V_{h+1}M + V_{h-1})$. Hence the quotient module is simple. □

For h such that $m_h \neq 0$, let $S_h = V_h/(V_{h+1}M + V_{h-1})$ be the simple A-module constructed in Proposition 3.4. If $h \neq h'$ and both S_h and $S_{h'}$ are defined, then by Lemma 3.3, it is possible to define a matrix $Y \in A$ such that Y acts as the identity on the cyclic vectors spanning S_h, and as the zero map on the cyclic vectors spanning $S_{h'}$. The simple modules S_h and $S_{h'}$ are therefore non-isomorphic as A-modules.

PROPOSITION 3.5. *The A-module V has a composition series in which the simple A-module S_h appears with multiplicity h.*

Proof. The action of the nilpotent matrix M on V_h induces a non-zero homomorphism of simple A-modules

$$\frac{V_h M^{i-1}}{V_{h+1}M^i + V_{h-1}M^{i-1}} \longrightarrow \frac{V_h M^i}{V_{h+1}M^{i+1} + V_{h-1}M^i}$$

for each i such that $1 \leq i \leq h-1$. This gives us h distinct composition factors of V_h, each isomorphic to S_h. It now follows from the Jordan–Hölder theorem that in any composition series of V, the simple module S_h appears at least with multiplicity h. Finally, by comparing dimensions using the equation

$$\dim V = n = \sum_h h m_h = \sum_h h \dim S_h,$$

we see that equality holds for each h, and that the A-module V has no other composition factors. □

PROPOSITION 3.6. *If M is nilpotent, and has part-size invariant k, then the determinants that appear in* Cent M *are k-th powers in $\mathbf{F}_q$.*

Proof. Given $Y \in \operatorname{Cent} M$ let Y_h denote the matrix in $\operatorname{Mat}_{m_h}(\mathbf{F}_q)$ which gives the action of Y on the simple A-module S_h. Using the composition series given by the previous theorem to compute $\det Y$ we get

$$\det Y = \prod_{\substack{h \\ m_h \neq 0}} (\det Y_h)^h.$$

Since the part-size invariant of m is the highest common factor of the set $\{h \mid m_h \neq 0\}$, we see that $\det Y$ is a k-th power. □

It is worth remarking that it is also possible to prove Proposition 3.5 in a way that gives the required composition series in an explicit form. We have avoided this approach in order to keep the notation as simple as possible. The following example indicates how to construct a suitable basis of V in a small case.

EXAMPLE. Let $M \in \operatorname{Mat}_5(\mathbf{F}_q)$ be a nilpotent matrix in the similarity class $N(2,2,1)$. Let u_1, u_2 be cyclic vectors of M of height 2, and let v be a cyclic vector of M of height 1. Then with respect to the basis u_1, u_2, v, u_1M, u_2M of $\mathbf{F}_q^5$, the centralizer of M consists of all matrices

of the form

$$\begin{pmatrix} \alpha & \beta & \star & \star & \star \\ \gamma & \delta & \star & \star & \star \\ & & \zeta & \star & \star \\ & & & \alpha & \beta \\ & & & \gamma & \delta \end{pmatrix}$$

where gaps denote zero entries, and $\star$ is used to denote an entry we have no need to specify explicitly. The key to obtaining this matrix in the required form is to order the elements of the basis correctly. The following principles determine a suitable ordering on the basis: elements come in decreasing order of height; cyclic vectors come first among elements of the same height; if b_i comes before b_j then b_iM comes before b_jM.

3.2. *Proof of Theorem 3.1*

The proof has two steps. We first show that if M is a matrix with entries in $\mathbf{F}_q$ and part-size invariant k, then every k-th power in $\mathbf{F}_q$ appears as the determinant of a matrix in $\operatorname{Cent} M$. In the second, we use Proposition 3.6 to show that no other powers can appear.

We begin with the following lemma.

LEMMA 3.7. *Let $S(k)$ be the set of k-th powers in $\mathbf{F}_q$. Let $d \in \mathbf{N}$ and $\vartheta \in \mathbf{F}_q^\times$. Then the number of irreducible polynomials of degree d over $\mathbf{F}_q$ with constant term ϑ is*

$$\frac{1}{d(q-1)} \sum_{\substack{k \mid d \\ S(k) \ni \vartheta}} \mu(k) \operatorname{hcf}(q-1,k)(q^{d/k}-1).$$

This number is non-zero for all choices of d and ϑ and for all q.

Proof. We give an elementary proof of the existence of a polynomial with degree d and constant term ϑ. For the number of polynomials, see for instance [**1**, §5.2].

Let α be a generator of the multiplicative group $\mathbf{F}_{q^d}^\times$, and let $\beta = \mathfrak{n}(\alpha)$ where $\mathfrak{n} : \mathbf{F}_{q^d}^\times \to \mathbf{F}_q^\times$ is the norm homomorphism. It is clear that β generates $\mathbf{F}_q^\times$. Let c be such that $0 < c < q$ and $(-1)^d\vartheta = \beta^c$. Since $\mathbf{F}_{q^d}$ has no proper subfield of index less than q, and since the multiplicative order of α^c is at least $(q^d-1)/c$, it is easy to see that α^c cannot lie in a proper subfield of $\mathbf{F}_{q^d}$. It follows that the minimum polynomial of α^c over $\mathbf{F}_q$ has degree d and constant term ϑ, as required. □

PROPOSITION 3.8. *Let P be a matrix with class type $d^{(j)}$. Then for any $\vartheta \in \mathbf{F}_q$, there exists a matrix in $\operatorname{Cent} P$ with determinant ϑ^j.*

Proof. We may assume that ϑ is non-zero. By Lemma 3.7 there exists an irreducible polynomial f over $\mathbf{F}_q$ with degree d and constant term $(-1)^d\vartheta$. Let C be the similarity class containing P, and let D be the class of matrices with cycle type $f^{(j)}$. Since C and D have the same class type, it follows from Theorem 2.6 that they commute. Therefore P commutes with an element of D. It is clear from the construction of D that its elements have determinant ϑ^j, as required. □

We now extend Proposition 3.8 to a general matrix.

PROPOSITION 3.9. *If M is a matrix with part-size invariant k, then for any $\zeta \in \mathbf{F}_q$, there exists a matrix in* Cent M *with determinant ζ^k.*

Proof. Let $P_1, \ldots, P_s$ be the distinct cyclic blocks of M; so M is conjugate to $\bigoplus_i P_i$. For each i let the class type of the block B_i be $d_i^{h_i}$. By Proposition 3.8, for any scalars ϑ_i that we choose, there exist matrices $X_1, \ldots, X_s$ such that $X_i \in \operatorname{Cent} B_i$ for all i, and $\det X_i = \vartheta_i^{h_i}$. Thus M commutes with a conjugate of the matrix $\operatorname{diag}(X_1, \ldots, X_s)$, which has determinant $\prod_i \vartheta_i^{h_i}$.

It will therefore be enough to show that there exist non-zero scalars $\vartheta_1, \ldots, \vartheta_s$ such that $\prod_i \vartheta_i^{h_i} = \zeta^k$. But we know that $k = \operatorname{hcf}(h_1, \ldots, h_s)$, and so there exist integers a_i such that $k = \sum_i a_i h_i$; it follows that we can simply take $\vartheta_i = \zeta^{a_i}$ for all i. □

We now turn to the second step in the proof of Theorem 3.1.

PROPOSITION 3.10. *Let M be a matrix with part-size invariant k. The determinant of an element of* Cent M *is a k-th power in $\mathbf{F}_q$.*

Proof. Let M act on $V = \mathbf{F}_q^n$. For each irreducible polynomial f over $\mathbf{F}_q$ which divides the minimal polynomial of M, let V_f be the largest subspace of V on which $f(M)$ acts nilpotently. Then $V = \bigoplus V_f$, and each summand V_f is invariant under Cent M. It follows that if $Y \in \operatorname{Cent} M$ then $\det Y = \prod \det Y_f$, where Y_f is the restriction of Y to V_f. Therefore, it will be sufficient to show that $\det Y$ is a k-th power for each f.

Let $\lambda = (h_1, \ldots, h_s)$ be the partition associated with a given f in the rational canonical form of M. From the definition of the part-size invariant, each of the parts h_i is divisible by k. Let M_f be the restriction of M to V_f, and let $Y_f \in \operatorname{Cent} M_f$.

By Proposition 2.2, $f(M_f)$ is nilpotent with associated partition $d\lambda$, where d is the degree of f. It is clear, then, that the part-size invariant of $f(M_f)$ is k. Since Y_f is in the centralizer of $f(M_f)$, it follows from Proposition 3.6 that $\det Y_f$ is a k-th power in $\mathbf{F}_q$, as required. □

Combining the results of Propositions 3.9 and 3.10 gives Theorem 3.1.

3.3. *Determinants in classes of a given type*

It is natural to ask which determinants are represented among matrices of a given type. This question leads to a hard problem in arithmetic combinatorics, to which we have been able to find only a partial solution.

It is clear that if T is a type representable over the field $\mathbf{F}_q$, then there is a matrix of type T with zero determinant if and only if T has a primary component 1^λ for some λ. This leaves us to decide which non-zero determinants can arise. For primary types this question is easily answered.

LEMMA 3.11. *Let λ be a partition of $k \in \mathbf{N}$, let $d \in \mathbf{N}$, and let $\vartheta \in \mathbf{F}_q^\times$. There is an invertible matrix over $\mathbf{F}_q$ with type d^λ and determinant ϑ if and only if ϑ is a k-th power in $\mathbf{F}_q^\times$.*

Proof. If M is a matrix of type d^λ then M has characteristic polynomial f^k. The determinant of M is therefore a k-th power. That every k-th power in $\mathbf{F}_q^\times$ is obtained in this way follows easily from Lemma 3.7. □

The following pair of propositions establish a sufficient condition on a type for it to represent all non-zero determinants.

PROPOSITION 3.12. *Let $d \in \mathbf{N}$ be coprime with $q-1$, and let $T = d^{\lambda_1} \cdots d^{\lambda_t}$ be a type representable over $\mathbf{F}_q$. If $L = |\lambda_1| + \cdots + |\lambda_t|$ is also coprime to $q-1$, then every element of $\mathbf{F}_q^\times$ is the determinant of a matrix of type T.*

Proof. It is an easy consequence of Lemma 3.7 that if d is coprime with $q-1$, then there are the same number of irreducible polynomials of degree d with any non-zero constant term. It follows that, for a generator ϑ of the cyclic group $\mathbf{F}_q^\times$, there exists a permutation σ of the set of irreducible polynomials of degree d, such that $f^\sigma(0) = \vartheta f(0)$ for all f.

Let C be a similarity class of type T, whose members have determinant α. Consider the class C' obtained from C by applying the permutation σ to the irreducible polynomials which appear in its cycle type. It is easy to see that C' has the same type as C, and that the members of C' have determinant $\alpha\vartheta^L$, where L is as in the statement of the proposition. Now ϑ^L is a generator of $\mathbf{F}_q^\times$ since L is coprime with $q-1$, and so it is clear that by repeated applications of the permutation σ we can obtain any non-zero determinant of our choice. □

PROPOSITION 3.13. *Let T be a type representable over a finite field $\mathbf{F}_q$. For each d let L_d be the sum of the sizes of the partitions associated with the components of degree d in T.*

If dL_d is coprime with $q-1$ for any d, then every element of $\mathbf{F}_q^\times$ is a determinant of a matrix of type T.

Proof. This follows immediately from Proposition 3.12. □

It should be noted that Proposition 3.13 does not come close to giving a necessary condition for a type to contain all non-zero determinants. Finding conditions which are both necessary and sufficient appears to be a highly intractable problem.

A special case of considerable interest is that of *linear* types, of the form $1^{\lambda_1}\cdots 1^{\lambda_t}$. (These are precisely the types of triangular matrices over $\mathbf{F}_q$.) We make use of the following definition.

DEFINITION. Let A be an abelian group of order m (written multiplicatively) and let $\pi = (\pi_1, \ldots, \pi_m) \in \mathbf{Z}^m$. We say that an element $x \in A$ is *π-expressible* if there exists an ordering $g_1, \ldots, g_m$ of the elements of G such that $x = g_1^{\pi_1} \cdots g_m^{\pi_m}$.

The relevance of this definition to our problem is easily explained. Let T be the linear type $1^{\lambda_1}\cdots 1^{\lambda_t}$ where $t \leq q-1$. Let $\pi \in \mathbf{Z}^{q-1}$ be defined by

$$\pi = (|\lambda_1|, \ldots, |\lambda_t|, 0, \ldots, 0).$$

Then we observe that the non-zero determinants represented in T are precisely the π-expressible elements of $\mathbf{F}_q^\times$.

If A is an abelian group of exponent n then we observe that adding multiples of n to the entries of π does not affect π-expressibility in A; we may therefore assume that all of the entries of π satisfy $0 \leq \pi_i \leq n-1$. Similarly, reordering the entries of π cannot affect π-expressibility, and so we may suppose that they appear in decreasing order.

Numerical evidence obtained by the authors supports the following conjecture.

CONJECTURE 3.14. Let A be a cyclic group of order m. Let $\pi = (\pi_1, \ldots, \pi_m) \in (\mathbf{Z}/m\mathbf{Z})^m$, where $\pi_1 \geq \cdots \geq \pi_m$. Let π' be the partition obtained from π by subtracting π_m from each part (thereby ensuring that the last part is 0). Then every element of A is π-expressible unless one of the following holds:

(i) $\pi' = (m-r, r, 0, \ldots, 0)$ for some r, or
(ii) There exists an integer $p > 1$ which divides each part of π', and which also divides m.

This conjecture is known to be true in the case that m is a prime (see [**4**, Theorem 1.2]). For our purposes, we would like it to be true for $A = \mathbf{F}_q^\times$ for all q; that is, whenever $m+1$ is a power of a prime. This would provide a complete classification of the determinants occurring in linear types. In the very special case when $q = 2^r$ and $|\mathbf{F}_q^\times| = 2^r - 1$ is a Mersenne prime, the result of [**4**] already gives such a classification.

4. *Commuting nilpotent classes*

In §2 the question of which similarity classes of matrices over a finite field commute was reduced to the analogous problem for nilpotent classes. The question of which nilpotent classes commute with a given nilpotent class $N(\lambda)$ appears to be a very hard problem, and we shall not attempt to answer it in any generality. We shall, however, treat a variety of special cases, and make a number of observations which, so far as we have been able to determine, do not appear in the existing literature. Our approach is elementary, and leads to results which, for the most part, apply to matrices defined over an arbitrary field. (For some other recent results on the problem of commuting nilpotent classes over algebraically closed fields, obtained by the methods of Lie theory, the reader is referred to [**10**] and [**13**].)

Our results may be summarized as follows. Proposition 4.1 describes the nilpotent classes that commute with $N(\lambda)$ when λ has a single part. This result has appeared previously in [**12**]; our Proposition 4.2 is similar to, but slightly stronger than, the result which appears there as Proposition 2.

Similarly, we deal in Proposition 4.4 with the case that $\lambda = (n-1, 1)$ for some n, and in Proposition 4.5 with the case that $\lambda = (2, \dots, 2)$. Using these results we are able to classify those nilpotent classes that commute with every nilpotent class of the same dimension; this is Theorem 4.6.

We next establish a condition for the nilpotent classes $N(n, n)$ and $N(n+1, n-1)$ to commute; these classes are found to commute over any infinite field, and over the finite field $\mathbf{F}_{p^r}$ provided that $p(p^{2r}-1)/e$ does not divide n, where $e = 1$ if $p = 2$ and $e = 2$ otherwise. As well as augmenting our list of commuting classes, this result is particularly significant, since it demonstrates that commuting of classes is in some cases dependent on the field of definition. Finally, we use the results just mentioned to classify those commuting nilpotent classes whose associated partitions have no more than two parts; this result, stated as Theorem 4.10, is valid over any field.

The following definition will be useful in what follows.

DEFINITION. Let M be a nilpotent transformation of a space V. A *cyclic basis* for M is a basis B of V with the property that for each $v \in B$, either $vM = 0$, or else $vM \in B$.

Earlier in §3.1 we defined a cyclic vector for M to be a vector which is not in the image of M. Let $M \in N(h_1, \dots, h_k)$, and let B be a cyclic basis for M. Then B contains cyclic vectors $v_1, \dots, v_k$, where $\operatorname{ht} v_i = h_i$ for all i; in fact

$$B = \{v_i M^j \mid 1 \leq i \leq k, 0 \leq j < h_i\}.$$

By Lemma 3.3, an element of $\operatorname{Cent} M$ is determined by its action on $v_1, \dots, v_k$.

4.1. *Cyclic nilpotent classes and partition refinements*

Recall that $J(\lambda)$ is the unique upper-triangular matrix in Jordan form in the similarity class $N(\lambda)$. The next proposition describes which classes commute with $J(n)$. We shall use the well-known fact that the elements of the centralizer algebra Cent $J(n)$ are the polynomials in $J(n)$—see for example [**9**, Ch. III, Corollary to Theorem 17].

PROPOSITION 4.1. *Let $\lambda = (h_1, \ldots, h_k)$ be a partition of n. Then $J(n)$ commutes with a conjugate of $J(\lambda)$ if and only if $h_1 - h_k \leq 1$.*

Proof. Write E_i for the matrix whose (x, y)-th entry is 1 if $k = y - x$, and 0 otherwise. The matrices $E_0, E_1, \ldots, E_{n-1}$ form a basis for the centralizer algebra of $J(n)$. Let M be a non-zero nilpotent element of this algebra; then for some d in the range $0 < d \leq n - 1$ we can write

$$M = \sum_{i \geq d} \alpha_i E_i,$$

for scalars α_i, with $\alpha_d \neq 0$.

It is easy to check that null $M^s = \min(sd, n)$ for all integers s. Let h be the least integer such that $hd \geq n$. Then it follows from Lemma 2.1 that M is conjugate to $J(\lambda)$, where

$$\lambda = (h, \ldots, h, h - 1, \ldots, h - 1)$$

is the partition with $n - hd$ parts of size $h - 1$ and $(h + 1)d - n$ parts of size h. This establishes the proposition. □

The terminology in the first of the following definitions is borrowed from [**10**, §3].

DEFINITION. A partition is *almost rectangular* if its largest part differs from its smallest part by at most 1.

DEFINITION. Let λ and μ be partitions. We say that μ is a *refinement* of λ if μ is the disjoint union of subpartitions whose sizes are the parts of λ. We say that a refinement of λ is *almost rectangular* if all of the subpartitions involved are almost rectangular.

For instance, $(5, 3, 1) = (3 + 2, 2 + 1, 1)$ has $(3, 2, 2, 1, 1)$ as an almost-rectangular refinement. It is worth noting that while the relation given by "μ is a refinement of λ" is clearly transitive, the relation given by "μ is an almost rectangular refinement of λ" is not.

PROPOSITION 4.2. *Let μ_1 and μ_2 be partitions of n. If there exists a partition λ which has both μ_1 and μ_2 as almost rectangular refinements, then the conjugacy classes represented by the Jordan blocks $J(\mu_1)$ and $J(\mu_2)$ commute.*

Proof. Consider the subpartitions ν_1 of μ_1 and ν_2 of μ_2 whose parts combine to create a single part of λ of size h. Since ν_1 and ν_2 are almost rectangular, they yield Jordan blocks whose classes commute with that of $J(h)$. But the centralizer of $J(h)$ consists of polynomials in $J(h)$, and it follows that the classes of $J(\nu_1)$ and $J(\nu_2)$ have representatives which are polynomials in $J(h)$. So these representatives commute, and hence $J(\mu_1)$ and $J(\mu_2)$ have conjugates which commute. □

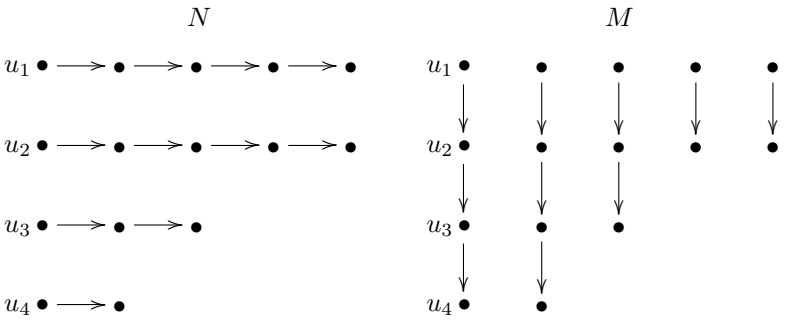
The preceding proposition is slightly more general than [**12**, Proposition 2], which states that the nilpotent classes $N(\lambda)$ and $N(\mu)$ commute if μ is an almost rectangular refinement of λ. It is noted in [**12**] that there exist examples of classes commuting that cannot be explained in this way. We remark that our Proposition 4.2 does not account for all commuting between classes, either. We illustrate this fact with the example and the proposition below; other examples will be seen in subsequent sections.

Example. There is no partition which has both $(2,2)$ and $(3,1)$ as an almost rectangular refinement, but the classes $N(2,2)$ and $N(3,1)$ commute over any field. We leave the proof of this to the reader, while remarking that it is a special case of any one of Propositions 4.4, 4.5 and 4.7 below.

Proposition 4.3. *Let λ be a partition, and let $\overline{\lambda}$ be its conjugate partition. Then the nilpotent classes with partitions λ and $\overline{\lambda}$ commute.*

Proof. Let $\lambda = (h_1, \ldots, h_k)$, where $h_1 \geq \cdots \geq h_k$. Let N be nilpotent of type λ, and let $u_1, \ldots, u_k$ be cyclic vectors for N, such that u_i has height h_i for all i. By Lemma 3.3 there is a unique matrix $M \in \operatorname{Cent} N$ such that $u_i M = u_{i+1}$ for all i, with $u_k M = 0$.

If $\lambda = (5,5,3,2)$, for instance, then the actions of N and M on the cyclic basis can be represented as follows:



It is easy to check that M is nilpotent, with associated partition $\overline{\lambda}$. □

In general there does not exist a partition which has both λ and $\overline{\lambda}$ as almost rectangular refinements, as is shown by the example illustrating the proof above, or by the case $\lambda = (4,1,1)$.

4.2. *Universally commuting classes*

The object of this section is to classify, in Theorem 4.6, the partitions to which the following definition refers.

DEFINITION. A partition λ of n is *universal* with respect to a field K if $N(\lambda)$ commutes with $N(\mu)$ over K for every partition μ of n.

The reference to the field in this definition is in fact redundant; it is a consequence of Theorem 4.6 that a partition which is universal with respect to one field is universal with respect to any field. To prove the theorem, we shall require the following two propositions.

PROPOSITION 4.4. *Let λ be a partition of n. The matrix $J(n-1,1)$ commutes with a conjugate of $J(\lambda)$ if and only if one of the following holds:*

(i) *λ has a part of size 1, and if λ^- is obtained from λ by removing this part, then $J(n-1)$ commutes with a conjugate of $J(\lambda^-)$; Proposition 4.1 provides a classification in this case.*

(ii) *n is even, and all of the parts of λ are of size 2.*

(iii) *λ has a part of size 3, and its other parts are of size 1 or 2, with at least one part of size 1.*

(iv) *$n = 3$ and $\lambda = (3)$.*

Proof. The centralizer algebra of $J(n-1,1)$ has the basis

$$\{E_i \mid 0 \le i \le n-2\} \cup \{F, G, H\},$$

where

$$\sum_i \alpha_i E_i + \beta F + \gamma G + \delta H = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-2} & \beta \\ 0 & \alpha_0 & \alpha_1 & & \alpha_{n-3} & 0 \\ 0 & 0 & \alpha_0 & & \alpha_{n-4} & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & \alpha_0 & 0 \\ 0 & 0 & 0 & \dots & \gamma & \delta \end{pmatrix}.$$

A nilpotent element of this algebra must have $\alpha_0 = \delta = 0$. We suppose that M is such an element, and that M is non-zero. By Lemma 2.1 the partition λ associated with M is determined by the sequence of ranks of powers of M.

If $\alpha_i = 0$ for all $i < n-2$, then α_{n-2}, β and γ are the only entries that are possibly non-zero. It is easy to see that the rank sequence $(\operatorname{rank} I, \operatorname{rank} M, \operatorname{rank} M^2, \operatorname{rank} M^3)$ must be either $(n,2,1,0)$ or $(n,1,0,0)$. In the first case the partition associated with M is $(3,1^{n-3})$, which

is covered by either part (iii) or part (iv) of the lemma. In the second case the partition is $(2, 1^{n-2})$, which is covered by part (i) or part (ii).

Now suppose that there exists $i < n-2$ such that $\alpha_i \neq 0$. Let m be the least such i. If $m < (n-2)/2$ then it is not hard to see that the rank sequence is

$$(n, n-m-1, n-2m-1, \ldots, 0).$$

The partition λ given by this data has one more part of size 1 than the partition λ^- given by the data

$$(n-1, n-m-1, n-2m-1, \ldots, 0).$$

But λ^- corresponds to the rank sequence for an element of the centralizer algebra of $J(n-1)$, and so this case is covered by case (i) of the lemma. If $m > (n-2)/2$ then the same situation occurs if $\beta\gamma = 0$. But if β and γ are both non-zero then the rank sequence obtained is $(n-m-1, 1, 0)$. The corresponding partition λ is covered by part (iii) of the lemma.

The final case to analyse occurs when n is even and $m = (n-2)/2$. If $M^2 \neq 0$ then the situation of the previous paragraph applies. Otherwise the rank sequence is $(n, n/2, 0)$ and all of the parts of λ have size 2, as in part (ii) of the lemma. □

PROPOSITION 4.5. *Let λ be the partition of $2s$ which has s parts of size 2, and let μ be any partition of $2s$. Then $J(\lambda)$ commutes with a conjugate of $J(\mu)$.*

Proof. By a straightforward inductive argument, we may suppose that μ has no subpartition of even size. If μ has only one part then the result follows from Proposition 4.1; so we may assume that μ has exactly two parts, $s+t$ and $s-t$.

A cyclic basis for $N = J(\lambda)$ has the form $B = \{e_1, \ldots, e_s, f_1, \ldots, f_s\}$, where the vectors f_i are in the kernel of N, and $e_iN = f_i$ for all i. Let M be the matrix whose action is defined by $e_iM = e_{i+1}$, $f_iM = f_{i+1}$ for $1 \leq i < s$, and

$$e_sM = \begin{cases} f_{s-t+1} & \text{if } t > 0, \\ 0 & \text{otherwise,} \end{cases}$$
$$f_sM = 0.$$

It is easy to see that M commutes with N, hence it suffices to show that $M \in N(\mu)$. A basis for $\ker M$ is given by $\{f_s, e_s - f_{s-t}\}$, so $\operatorname{null} M = 2$. It follows that the partition associated with M has two parts, and since e_1 is a cyclic vector of height $s+t$, this partition must be $(s+t, s-t)$, as required. □

THEOREM 4.6. *The universal partitions are precisely those with no part greater than 2, together with $\lambda = (3)$.*

Proof. Suppose that λ has no part of size greater than 2. If all of the parts of λ have size 2, then $J(\lambda)$ commutes with all nilpotent classes, by Proposition 4.5. Otherwise λ has a subpartition λ_m of m for every $m \leq n$. Let μ be a partition of n with largest part m. Then since λ_m is an almost rectangular refinement of m, it follows from Proposition 4.1 that $J(\lambda_m)$ commutes with a conjugate of $J(m)$. Now if λ' denotes the partition obtained by deleting the parts of λ_m from λ, and if μ' is obtained by deleting a part of size m from μ, then we may suppose inductively that $J(\lambda')$ commutes with a conjugate of $J(\mu')$. It follows that $J(\lambda)$ commutes with a conjugate of $J(\mu)$.

Conversely, suppose that λ has largest part $h > 2$. If $J(\lambda)$ commutes with $J(n)$ then by Proposition 4.1 all of its parts have size h or $h-1$. Then we see from Proposition 4.4 that $J(\lambda)$ does not commute with a conjugate of $J(n-1,1)$, except in the single case that $\lambda = (3)$. □

4.3. *Commuting of classes $N(n,n)$ and $N(n+1,n-1)$*

The main object of this section is to prove Proposition 4.7 below, which gives a necessary and sufficient condition for the classes $N(n,n)$ and $N(n+1,n-1)$ to commute. This case is of particular interest because the field enters in an essential way. In Theorem 4.8 we use this proposition to show that for every prime p and positive integer r, there exists a pair of classes of nilpotent matrices which commute over the field $\mathbf{F}_{p^r}$ if and only if $s > r$.

Proposition 4.7 is motivated by a natural construction on matrices. Suppose that X and Y are commuting matrices over a field K, and let

$$D = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}, \qquad E = \begin{pmatrix} Y & I \\ 0 & Y \end{pmatrix}.$$

Clearly the matrices D and E commute. We may assume that X and Y (and hence D and E) are nilpotent; then this construction (and other similar ones) may in principal be used to find new cases of commuting nilpotent classes. The partition labelling the class of D is clearly 2λ, where λ labels the class of X. The partition labelling the class of E is harder to calculate, and depends on the characteristic of K.

We have no occasion to make systematic use of this construction in the present paper, but the following example is illustrative. Let $X = Y = J(n)$. Then $D \in N(n,n)$. The partition labelling the class of E is $(n+1,n-1)$ except in the case that $\operatorname{char} K$ divides n, in which case it is (n,n). It follows that $N(n,n)$ and $N(n+1,n-1)$ commute over fields of all but finitely many characteristics, the exceptions being the prime divisors of n. We note, however, that the present method gives no information about whether the classes commute in fields of these exceptional characteristics; this gives an indication that the following proposition is non-trivial.

PROPOSITION 4.7. *Let p be a prime, and let*

$$e = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{otherwise.} \end{cases}$$

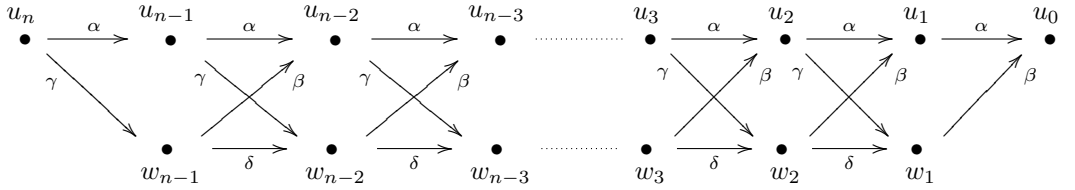
Then the nilpotent types (n, n) and $(n+1, n-1)$ commute over $\mathbf{F}_{p^r}$ if and only if n is not divisible by $p(p^{2r}-1)/e$.

Proof. Let M be nilpotent of type $(n+1, n-1)$, acting on a space V over $\mathbf{F}_{p^r}$. Take a cyclic basis $\{u_i, w_j \mid 0 \leq i \leq n,\ 1 \leq j \leq n-1\}$ for V, with $u_i M = u_{i-1}$ and $w_j M = w_{j-1}$ for all i and j. Let U_k and W_k denote the subspaces $\langle u_j \mid 0 \leq j \leq k \rangle$ and $\langle w_j \mid 1 \leq j \leq k \rangle$ respectively—we take $W_0 = \{0\}$ and $W_n = W_{n-1}$. Let V_k denote $U_k \oplus W_k$ for all k. For each pair (x, y) with $x \in V_{n-1}$ and $y \in V_{n-2}$, there is an unique nilpotent element Y of $\operatorname{Cent} M$ such that $u_n Y = x$ and $w_{n-1} Y = y$; it follows from Lemma 3.3 that all of the nilpotent elements of $\operatorname{Cent} M$ can be obtained in this way.

Let $Y \in \operatorname{Cent} M$ be nilpotent, and define $\alpha, \beta, \gamma, \delta$ by

$$u_n Y \in \alpha u_{n-1} + \gamma w_{n-1} + V_{n-2},$$
$$w_{n-1} Y \in \beta u_{n-2} + \delta w_{n-2} + V_{n-3}.$$

The reader may find helpful the following diagrammatic representation of Y.



The matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ describes the maps induced by Y,

$$\overline{Y}_k : \frac{V_k}{V_{k-1}} \longrightarrow \frac{V_{k-1}}{V_{k-2}},$$

where k is in the range $1 < k < n$. Outside of this range, the map $\overline{Y}_n$ has domain $\langle\, u_n + V_{n-1} \,\rangle$ of dimension 1, while $\overline{Y}_1$ has codomain $\langle u_0 \rangle$ of dimension 1. These maps are represented by the first row and the first column of A respectively.

CLAIM. *The kernel of Y has dimension 2 if and only if A is non-singular.*

Proof of Claim. If A is invertible, then the maps $\overline{Y}_k$ are injective for $k > 1$. It follows easily that if $v \in \ker Y$ then $v \in V_1$. It is now easy to check that $v \in \langle u_1, \beta u_2 - \alpha w_1 \rangle$ and so $\operatorname{null} Y = 2$ in this case.

Conversely, suppose that A is singular. If $\alpha = \beta = 0$ then $V_1 \subseteq \ker Y$, and so $\operatorname{null} Y \geq 3$. So let us suppose that α and β are not both 0. Then there exists $z \in V_1$ such that $zY = u_0$. Since A is singular, the map $\overline{Y}_2$ has a non-trivial kernel, and it follows that there exists $v \in V_2 \setminus V_1$ such that $vY \in V_0 = \langle u_0 \rangle$. Say that $vY = \sigma u_0$; now we have a set of three kernel vectors, $\{u_0,\ \beta u_1 - \alpha w_1,\ v - \sigma z\}$, which is linearly independent since $v - \sigma z \notin V_1$. So $\operatorname{null} Y \geq 3$ in this case as well. □

The dimension of $\ker Y$ tells us the number of parts in the partition associated with the class of Y. This partition therefore has two parts if and only if the matrix A is non-singular. Note that since $Y^{n+1} = 0$, no part can be larger than $n + 1$, and therefore the only possible partitions are $(n + 1, n - 1)$ and (n, n). The former corresponds to the class of M itself, while the latter case occurs when $Y^n = 0$, which is the case if and only if $u_n \in \ker Y^n$.

Now we observe that

$$\begin{aligned} u_n Y^n &= \overline{Y}_1 \circ \overline{Y}_2 \circ \cdots \circ \overline{Y}_n (v_n + V_{n-1}) \\ &= u_0 R_1 A^{n-2} C_1 \ , \end{aligned}$$

where R_1 and C_1 are, respectively, the first row and the first column of A. So the partition of Y is (n, n) precisely when $R_1 A^{n-2} C_1 = (0)$, or equivalently, when the matrix A^n has a zero for its top left-hand entry.

CLAIM. *Every element of $\mathrm{GL}_2(\mathbf{F}_{p^r})$ is either a scalar matrix, or else is conjugate to a matrix with a zero for its top left-hand entry.*

Proof of Claim. Every quadratic polynomial over $\mathbf{F}_{p^r}$ is the characteristic polynomial of a unique similarity class of non-scalar matrices. Thus if X is a non-scalar matrix with characteristic polynomial $x^2 + \sigma x + \tau$, then X is conjugate to

$$\begin{pmatrix} 0 & 1 \\ -\tau & -\sigma \end{pmatrix},$$

as required. □

Now suppose that $\mathrm{GL}_2(\mathbf{F}_{p^r})$ contains a non-scalar element X which is an n-th power in the group. Then X has a conjugate X' with a zero for its top left-hand entry. Clearly X' is also an n-th power; by choosing a, b, c, δ to be the entries of an n-th root of X', we can construct a matrix Y in $\operatorname{Cent} M$ whose type is (n, n).

There exist non-scalar n-th powers in $\mathrm{GL}_2(\mathbf{F}_{p^r})$ provided that n is not divisible by the exponent of $\mathrm{PGL}_2(\mathbf{F}_{p^r})$. This exponent is $p(p^{2r}-1)/e$, and the proof of Proposition 4.7 is complete. □

REMARK. This argument also goes to show that the nilpotent types (n, n) and $(n-1, n+1)$ commute over any infinite field K, since the exponent of $\mathrm{PGL}_2(K)$ is infinite.

THEOREM 4.8. *Let p be a prime, and $r \geq 1$. There exist partitions λ and μ, such that $N(\lambda)$ commutes with $N(\mu)$ over the fields $\mathbf{F}_{p^a}$ for $a > r$, but not for $a \leq r$.*

Proof. We use a famous theorem of Zsigmondy [**15**] which states that if $k \geq 2$, $t \geq 3$, and $(k,t) \neq (2,6)$, then there is a prime divisor of $k^t - 1$ which does not divide $k^s - 1$ for any s such that $1 \leq s < t$.

Let $L = \mathrm{lcm}(\{p^{2s} - 1 \mid 1 \leq s \leq r\})$, and let $n = pL/e$. We observe that $p(p^{2a}-1)/e$ divides n whenever $a \leq r$. When $a > r$ we invoke Zsigmondy's Theorem with $(k,t) = (p, 2a)$, or with $(k,t) = (4,3)$ if $p = 2$ and $t = 3$; this tells us that $p^{2a} - 1$ has a prime divisor q which does not divide $p^{2s} - 1$ for $s < a$. Clearly q does not divide n, and so $p(p^{2a}-1)/e$ does not divide n. It now follows from Proposition 4.7 that the partitions (n, n) and $(n+1, n-1)$ have the property stated in the theorem. □

REMARK. The authors have found no case where the commuting of nilpotent classes depends on the field of definition in dimension less than 12. This is the dimension of the smallest example given by Proposition 4.7: that of $N(6,6)$ and $N(7,5)$, which commute over every field except $\mathbf{F}_2$.

4.4. *Classes corresponding to two-part partitions*

We end by establishing a result which, together with results already presented, will allow us to classify, over any field K, pairs of partitions (λ, μ) with at most two parts, such that $N(\lambda)$ and $N(\mu)$ commute over K. We note that classes with at most 2 parts are precisely those whose elements have nullity at most 2.

PROPOSITION 4.9. *Let $\lambda = (a, b)$ and $\mu = (c, d)$, where $a + b = c + d$ and $a > c \geq d > b$. If $N(\lambda)$ and $N(\mu)$ commute over a field K then $c = d$ and $a - b = 2$.*

Proof. The case that $c = d$ and $a - b = 2$ has been dealt with in Proposition 4.7 and the ensuing remark. We may therefore suppose that $a - b > 2$. Let $M \in N(\lambda)$, and let $\{v, vM, \ldots, vM^{a-1}, w, wM, \ldots, wM^{b-1}\}$ be a cyclic basis for M. Let $W = \ker M^{a-2}$; so W

is the span of all the basis vectors apart from v and vM. Suppose that Y is nilpotent and commutes with M; then it is not hard to see that $W \subseteq \ker Y^{a-2}$. Since Y is nilpotent we have $vY \in \alpha vM + W$ for some $\alpha \in K$.

Suppose first that $\alpha \neq 0$; then we see that $vY^{a-1} = \alpha^{a-1} vM^{a-1}$, while $vY^a = 0$. Hence v is a cyclic vector for Y of height a. It follows that if the partition associated with Y has only 2 parts then it must be λ.

Suppose alternatively that $\alpha = 0$, so $vY \in W$. We shall show that $\operatorname{null} Y \geq 3$, and so the partition associated with Y has more than 2 parts. First observe that vM^{a-2} and vM^{a-1} are in $\ker Y$, since $vM^{a-2}Y = vYM^{a-2} \in WM^{a-2} = \{0\}$. Furthermore it is easy to show that $vM^{a-3}Y$ and $wM^{b-1}Y$ both lie in $\langle vM^{a-1} \rangle$, and hence a non-zero linear combination of these two vectors lies in $\ker Y$. We have therefore found three linearly independent vectors in $\ker Y$, as required. □

The following theorem simply collects together elements of Propositions 4.1, 4.7 and 4.9; it requires no further proof.

THEOREM 4.10. *Suppose that λ and μ are partitions of n with at most two parts, and that $N(\lambda)$ and $N(\mu)$ commute over a field K. Assume without loss of generality that the largest part of λ is at least as large as the largest part of μ. Then one of the following holds.*

(i) $\lambda = \mu$.

(ii) $n = 2m$, $\lambda = (n)$ *and* $\mu = (m, m)$.

(iii) $n = 2m$, $\lambda = (m+1, m-1)$, $\mu = (m, m)$ *and, if K is finite then the exponent of* $\mathrm{PGL}_2(K)$ *does not divide* m.

(iv) $n = 2m+1$, $\lambda = (n)$ *and* $\mu = (m+1, m)$.

References

1. JOHN R. BRITNELL, 'Cyclic, separable and semisimple matrices in the special linear groups over a finite field', *J. London Math. Soc.* (2) 66 (2002) 605–622.

2. JOHN R. BRITNELL and MARK WILDON, 'On the distribution of conjugacy classes between the cosets of a finite group in a cyclic extension', *Bull. London Math. Soc.* 40 (5) (2008) 897–906.

3. JOHN R. BRITNELL and MARK WILDON, 'Commuting elements in conjugacy classes: An application of Hall's Marriage Theorem', *J. Group Theory*, to appear.

4. ANDRÁS GÁCS, TAMÁS HÉGER, ZOLTÁN LÓRÁNT NAGY and DÖMÖTÖR PÁLVÖLGYI, 'Permutations, hyperplanes and polynomials over finite fields', preprint.

5. MURRAY GERSTENHABER, 'On nilalgebras and linear varieties of nilpotent matrices III', *Ann. of Math.* 70 (1) (1959) 167–205.

6. MURRAY GERSTENHABER, 'On dominance and varieties of commuting matrices', *Ann. of Math.* 73 (2) (1961) 324–348.

7. ISRAEL GOHBERG, PETER LANCASTER and LEIBA RODMAN, *Invariant subspaces of matrices and applications* (Wiley, New York, 1986).

8. J. A. Green, 'The characters of the finite general linear groups', *Trans. Amer. Math. Soc.* 80 (2) 1955 402–447.
9. Nathan Jacobson, *Lectures in abstract algebra II: Linear Algebra* (Van Nostrand, 1953)
10. Tomaž Košir and Polona Oblak, 'On pairs of commuting nilpotent matrices', *Transformation Groups* 14 (1) (2009) 175–182.
11. I. G. Macdonald, *Symmetric functions and Hall polynomials* (Second Edition, Oxford University Press, Oxford, 1995).
12. Polona Oblak, 'The upper bound for the index of nilpotency for a matrix commuting with a given nilpotent matrix', *Linear and Multilinear Algebra* 56 (6) (2008) 701–711.
13. Dmitri I. Panyushev, 'Two results on centralisers of nilpotent elements', *J. Pure Appl. Algebra* 212 (2008) 774–779.
14. R. Steinberg, 'A geometric approach to the representations of the full linear group over a Galois field', *Trans. Amer. Math. Soc.* 71 (1951) 274–282.
15. K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. für Math. u. Phys.* 3 (1892) 265–284.

School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
United Kingdom

j.r.britnell@bristol.ac.uk
mark.wildon@bristol.ac.uk