

COMPUTING IN NILPOTENT MATRIX GROUPS

A. S. DETINKO AND D. L. FLANNERY

Abstract

We present algorithms for testing nilpotency of matrix groups over finite fields, and for deciding irreducibility and primitivity of nilpotent matrix groups. The algorithms also construct modules and imprimitivity systems for nilpotent groups. In order to justify our algorithms, we prove several structural results for nilpotent linear groups, and computational and theoretical results for abstract nilpotent groups, which are of independent interest.

1. *Preliminaries and background*1.1. *Computing in matrix groups*

This paper deals with the development of algorithms for matrix groups, currently a very active area of computational group theory. Early matrix group algorithms modified permutation group methods, using induced actions on the underlying vector space. The feasibility of such approaches is limited, as they can give rise to algorithms with running times that are exponentially dependent on the size of input data. And, of course, for infinite matrix groups these approaches cannot be used directly at all. The computational problems involved have motivated a new phase in the development of algorithms for matrix groups (for further historical remarks, see the survey [23]).

Nilpotency is an important group property. Methods for computing in finite nilpotent matrix groups are given in [18]. For a matrix group G over a finite field, or a finite matrix group G over an algebraic number field, Luks proves in [18, Theorem 3.1, Corollary 3.4] that one can test in polynomial time whether or not G is nilpotent. Also, in [18, §4.5] methods are proposed for testing membership, finding presentations, and solving other computational problems. The methods depend on finding a so-called ‘manageable representation’ for each term of a normal series of a nilpotent matrix group (see [18, p. 114] and [2]). A different way of testing nilpotency is described in [7, §2.3]; this is a Monte-Carlo polynomial-time algorithm for testing solubility and nilpotency of matrix groups over finite fields.

Aspects of computing in a nilpotent matrix group over an algebraic number field are considered in [3]. This research was prompted by the Tits alternative: a finitely generated matrix group either contains a free subgroup of rank 2, or is soluble-by-finite. In the former case, many basic computational problems are undecidable. So it is desirable to have an efficient algorithm for testing whether a finitely generated matrix group is soluble-by-finite. In [3, §6], Beals gives a polynomial-time algorithm for deciding whether a finitely generated matrix group over an algebraic number field is nilpotent-by-finite. Other computational problems have been solved for such groups (see [3, Theorem 1.5]). Some methods from [3] can be used for computing in nilpotent matrix groups, but most of the algorithms in [3] are practicable only if the groups are of small degree. Similar problems are dealt with

Received 15 September 2005, revised 23 January 2006; *published* 9 March 2006.

2000 Mathematics Subject Classification 20H30 (primary), 20D15 (secondary).

© 2006, A. S. Detinko and D. L. Flannery

in [11] and [19], where algorithms for polycyclic and polycyclic-by-finite matrix groups over number fields are described. Since finitely generated nilpotent groups are polycyclic, a broad range of algorithms for polycyclic groups is applicable to finitely generated nilpotent linear groups (see [17, 25]). In particular, [17] contains an algorithm for testing nilpotency of a polycyclically presented group.

The main objective of this paper is to introduce novel ways of computing in nilpotent matrix groups, based on standard linear group theory. Although we treat groups defined over a finite field, many of the concepts can be extended to finitely generated nilpotent groups over other fields, such as number fields. Thus we regard this paper as a starting point for further work on computing with nilpotent linear groups over an arbitrary field.

Our approach uses structural results for nilpotent linear groups [26, 27], methods for computing in associative algebras [21], and standard techniques of computational group theory [12]. We provide the following algorithms for a matrix group G over a finite field, defined by a generating set of matrices:

- testing nilpotency of G ,

and, if G is nilpotent,

- testing irreducibility of G ,
- constructing explicit nontrivial G -modules,
- testing primitivity of G , and
- constructing explicit nontrivial G -systems of imprimitivity.

Additionally, the final section of the paper discusses the construction of small-degree monomial (and hence permutation) representations of a nilpotent linear group.

Our algorithms are deterministic, and always return definitive answers, without exceptions. The basic themes driving all of our algorithms are a reduction to completely reducible groups, and the computation of a series of subnormal subgroups with abelian factors. For the irreducibility and primitivity testing algorithms, another theme is the construction of modules for abelian normal subgroups of an input nilpotent completely reducible matrix group.

Irreducibility testing of matrix groups over a finite field, and primitivity testing of absolutely irreducible matrix groups over a finite field, are studied in the papers [13, 14, 15]. Nilpotent primitive linear groups have a much more transparent structure than arbitrary primitive linear groups: see [27, Chapter VII], [9], and [8] (where the nilpotent primitive linear groups over a finite field are completely classified up to conjugacy); for instance, odd-order primitive nilpotent linear groups are cyclic. It therefore seems reasonable to develop algorithms for irreducibility and primitivity testing directly for nilpotent matrix groups, taking advantage of the special structure of these groups. There are several attractive features of our overall approach to irreducibility/primitivity testing of nilpotent matrix groups: it does not depend heavily on the ground field, and hence can be extended to finitely generated groups over infinite fields; primitivity testing does not require that input groups be absolutely irreducible; and irreducibility/primitivity testing and the construction of modules or imprimitivity systems are done in parallel. In fact, our algorithms for testing nilpotency, and those for testing irreducibility/primitivity, are all based on the same set of ideas and techniques. In the course of developing such algorithms we prove several auxiliary results on abstract and linear nilpotent groups (see Subsections 3.2 and 3.3), which are of independent interest.

1.2. Notation and terminology

As usual, $\text{GL}(n, \mathbb{F})$ is the group of $n \times n$ invertible matrices over a field \mathbb{F} . Let V be the underlying n -dimensional \mathbb{F} -vector space; note that the group $\text{GL}(V)$ of invertible \mathbb{F} -linear transformations on V is isomorphic to $\text{GL}(n, \mathbb{F})$. Elements of $\text{GL}(n, \mathbb{F})$ act on the left of V .

Throughout the paper, G is a subgroup of $\text{GL}(n, \mathbb{F})$ given by a generating set $\{g_1, \dots, g_r\}$ of matrices.

A G -submodule of V is a subspace U of V such that $GU \subseteq U$. When we talk of G -modules we can mean either G -submodules of V , or G -quotient modules of V : quotients U/W where $W \subseteq U$ are subspaces of V and $GU \subseteq U$.

Let $X \neq 0$ be a G -module. If X has no proper nonzero G -submodules, then X is *irreducible*; otherwise it is *reducible*. Let X_1, \dots, X_k be nonzero G -submodules of X such that $X = X_1 \oplus \dots \oplus X_k$. We say X is *decomposable* if $k > 1$, whereas X is *indecomposable* if no such nontrivial direct sum decomposition of X exists. If each X_i is an irreducible G -module, then X is *completely reducible*. Under our definitions, an irreducible G -module is completely reducible.

All of the above terminology is also applied to G itself: G is irreducible, reducible, completely reducible, indecomposable, decomposable, according as the G -module V is irreducible, reducible, completely reducible, indecomposable, decomposable, respectively.

Given an extension field \mathbb{E} of \mathbb{F} , it is possible to define V as an \mathbb{E} -vector space by ‘extension of scalars’, in such a way that $\text{GL}(n, \mathbb{F})$ embeds as a subgroup of $\text{GL}(n, \mathbb{E})$ acting on V . If G is irreducible as a subgroup of $\text{GL}(n, \mathbb{E})$ for every extension field \mathbb{E} of \mathbb{F} , then G is *absolutely irreducible*. In fact, G is absolutely irreducible if and only if G is irreducible as a subgroup of $\text{GL}(n, \bar{\mathbb{F}})$; $\bar{\mathbb{F}}$ the algebraic closure of \mathbb{F} .

A composition series of the G -module V gives rise to a basis of V by extending bases of terms in the series, and with respect to this basis each element g of G has block upper triangular form

$$\begin{pmatrix} a_1(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a_2(g) & \dots & a_{2k}(g) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_k(g) \end{pmatrix} \tag{1.1}$$

where the assignment $g \mapsto a_i(g)$, $1 \leq i \leq k$, defines an irreducible representation $G \rightarrow a_i(G) \leq \text{GL}(n_i, \mathbb{F})$, and the $a_{ij}(g)$ are $n_i \times n_j$ matrices over \mathbb{F} . In particular, G is completely reducible if and only if some such block upper triangular form for G has $a_{ij}(g) = 0$ for all $i \neq j$ and $g \in G$. We call $a_i(G)$ an *irreducible part* of G . Suppose that another block triangular form for G yields irreducible parts $b_i(G)$ of degree m_i . If $m_i = n_j$ and $x^{-1}b_i(g)x = a_j(g)$ for some $x \in \text{GL}(m_i, \mathbb{F})$ and all $g \in G$, then the irreducible parts $b_i(G)$, $a_j(G)$ are *equivalent*. By the Jordan–Hölder theorem, the multiset of irreducible parts of G (counting multiplicities) obtained from any block upper triangular form (1.1) of G is unique up to equivalence.

If $V = V_1 \oplus \dots \oplus V_m$ where $m > 1$ and the V_i are subspaces of V permuted by G under the usual left matrix multiplication action, then G is *imprimitive*, and $\{V_1, \dots, V_m\}$ is a G -system of imprimitivity. If no such decomposition of V exists, and G is irreducible, then G is *primitive*. We say G is *monomial* if it has an imprimitivity system of size n , for in this case G is conjugate by a change-of-basis matrix to a group of monomial matrices in $\text{GL}(n, \mathbb{F})$. Note that in our definition of imprimitivity, G need not be irreducible. However, if G is irreducible and imprimitive, then it acts transitively on an imprimitivity system

$\{V_1, \dots, V_m\}$, so that all the V_i are of equal dimension and m divides n ; also, m divides $|G|$ if G is finite.

Let S be any set of $n \times n$ matrices over \mathbb{F} . The *enveloping algebra* $\langle S \rangle_{\mathbb{F}}$ of S over \mathbb{F} is the smallest \mathbb{F} -subalgebra of the full $n \times n$ matrix algebra $\text{Mat}(n, \mathbb{F})$ containing S . A G -submodule W of V is said to be a *simple G -module* if $\langle G_W \rangle_{\mathbb{F}}$ is a simple algebra (here G_W is the restriction of G to W). For example, W is simple if G_W is irreducible. Let G_W be completely reducible; then $\langle G_W \rangle_{\mathbb{F}}$ is a semisimple algebra, and if the irreducible parts of G_W are all equivalent (the completely reducible G -module W has a single homogeneous component), then W is a simple G -module. Conversely, if $\langle G_W \rangle_{\mathbb{F}}$ is a semisimple algebra, then G_W is completely reducible. By Wedderburn theory, any semisimple algebra $A \subseteq \text{Mat}(n, \mathbb{F})$ is a direct sum of simple subalgebras, and those summands are the only minimal nonzero ideals of A .

For the rest of the paper, \mathbb{F} is a finite field of characteristic p .

With all elements of G in the form (1.1), we define a homomorphism $\gamma : G \rightarrow \text{GL}(n, \mathbb{F})$ by

$$\gamma : g \mapsto \text{diag}(a_1(g), a_2(g), \dots, a_k(g)).$$

The kernel of γ is a normal nilpotent subgroup of G ; actually it is a p -group, and if G itself is nilpotent then $\ker \gamma$ is the Sylow p -subgroup of G .

The group theory notation that we use is mainly standard, as in [20]. The normal closure of a subgroup K in a group H is written K^H . For a finite nilpotent group H and prime q dividing $|H|$, it will sometimes be convenient to denote the Sylow q -subgroup of H by H_q , and the Hall q' -subgroup by $H_{q'}$. In a q -group H , $\Omega_1(H)$ denotes the subgroup generated by all elements of order q .

2. Nilpotency of matrix groups

2.1. Reduction to completely reducible groups

The aim of this subsection is twofold: firstly, to show that we can always construct completely reducible G -submodules of V when G is nilpotent; and secondly to indicate the principal importance of the case that G is completely reducible when testing nilpotency of G . The completely reducible case is similarly important in our algorithms for testing irreducibility and primitivity of G , and constructing nontrivial G -modules or G -systems of imprimitivity for a nilpotent matrix group G .

An element g of $\text{GL}(n, \mathbb{F})$ is *unipotent* if $(g - 1_n)^n = 0_n$, where 1_n and 0_n denote, respectively, the $n \times n$ identity and zero matrices. Since \mathbb{F} has characteristic p , g is unipotent if and only if $|g|$ is a p -power. If for some extension \mathbb{E} of \mathbb{F} , g is conjugate to $\text{diag}(a_1, \dots, a_n) \in \text{GL}(n, \mathbb{E})$, then g is *semisimple*. By Maschke's theorem, the semisimple elements of $\text{GL}(n, \mathbb{F})$ are precisely those of order not divisible by p . We should emphasise at the outset that for arbitrary $G \leq \text{GL}(n, \mathbb{F})$, the conditions that

- G is generated by semisimple matrices, and
- G is completely reducible

are not equivalent, but that when G is nilpotent, these two conditions do coincide (see results 2.2 – 2.4 below).

For each $g \in \text{GL}(n, \mathbb{F})$ there exist a unique semisimple matrix $g_s \in \text{GL}(n, \mathbb{F})$ and a unique unipotent matrix g_u such that $g = g_s g_u = g_u g_s$. This is called the *Jordan decomposition* of g ; g_s is the *semisimple part* of g , and g_u is the *unipotent part* of g .

LEMMA 2.1 (see [22, Corollary 1, p. 135]). *If $g \in \text{GL}(n, \mathbb{F})$ has order $p^e q$ and $\text{gcd}(p, q) = 1 = ap^e + bq$, then $g_u = g^{bq}$ and $g_s = g^{ap^e}$.*

The Jordan decomposition of g can be found by Lemma 2.1; see [6] for a method to compute the orders of elements of $\text{GL}(n, \mathbb{F})$ which is usually fast in practice (but is not polynomial time, as it can involve the factorisation of large integers). There are other means: in an appendix to [1] it is shown that the decomposition of g as $g_s + h$, where $h \in \langle g \rangle_{\mathbb{F}}$ is a nilpotent matrix, can be accomplished in polynomial time. We have $g_u = hg_s^{-1} + 1$.

Define subsets G_u and G_s of G by

$$G_u = \{g_u \mid g \in G\} \quad \text{and} \quad G_s = \{g_s \mid g \in G\}.$$

The next result follows from [22, p. 136].

LEMMA 2.2. *If G is nilpotent, then G_u is the Sylow p -subgroup of G , $G_s = G_{p'}$ is a completely reducible subgroup of G , and $G = G_u \times G_s$.*

COROLLARY 2.3. *Suppose that G is nilpotent. Let $g_{i(u)}$ and $g_{i(s)}$ be the unipotent and semi-simple parts of g_i , respectively. Then $G_u = \langle g_{1(u)}, \dots, g_{r(u)} \rangle$ and $G_s = \langle g_{1(s)}, \dots, g_{r(s)} \rangle$.*

LEMMA 2.4 (see [27, §29, Corollary 1]). *Suppose that G is nilpotent. Then G is completely reducible if and only if $G = G_s$.*

We now look at ways of constructing completely reducible G -submodules of V . Of course, if G is nilpotent and $G_u = 1$, then V itself is completely reducible. Let $H = \langle g_{1(u)}, \dots, g_{r(u)} \rangle$. Let W_i be the subspace of V consisting of all $g_{i(u)}$ -fixed points, and define $W = \bigcap_i W_i$. If G is nilpotent and $G_u \neq 1$, then $W \neq 0$ is the fixed point space $\text{Fix}(G_u)$ of G_u : this is a G -submodule of V , because G_s commutes with G_u ; also, W is completely reducible by Maschke's theorem, because the action of G on W has kernel containing the Sylow p -subgroup G_u of G . We proceed to calculate $\text{Fix}(H)$ in V/W , and so on, repeating until we find a proper G -submodule U of V such that $\text{Fix}(H)$ in V/U is V/U . If this recursion does not succeed in n iterations or less to find such a U , then G is not nilpotent. Success confirms that H is unipotent.

Another way to construct completely reducible G -submodules of V , related to the above, uses a correspondence between the structure of $\langle G \rangle_{\mathbb{F}}$ and the action of G on V . Let $R = \langle R_1, \dots, R_r \rangle_{\mathbb{F}}$, where $R_i = g_{i(u)} - 1_n$. Suppose that G is nilpotent; then the radical of $\langle G \rangle_{\mathbb{F}}$ is spanned by $\{gx \mid g \in G_s, x \in R\}$. Denote by R^k the ideal of R generated by all length- k products $x_1 \cdots x_k$, $x_i \in R$. Either $R = 0$ and so V is completely reducible, or we have a strictly descending chain $R \supset R^2 \supset \cdots \supset R^{m-1} \supset R^m = 0$ of ideals of R , where $m \leq n$, and

$$RV \supset R^2V \supset \cdots \supset R^{m-1}V \supset 0 \tag{2.1}$$

is a chain of G -modules. We can use (2.1) to write G in upper block triangular form (1.1): each quotient $R^iV/R^{i+1}V$ is annihilated by R and therefore is completely reducible. Note that $R^{m-1}V \subseteq \text{Fix}(G_u)$, the nullspace of R , and if $g \in G_u$ then the blocks $a_i(g)$ in (1.1) are all the identity; that is, G_u is upper unitriangular.

Sometimes the irreducible parts of G are equivalent. For example, this is certainly true if G is a p -group (all irreducible parts are trivial). Also note the following lemma.

LEMMA 2.5 (see [27, §29, Theorem 3]). *If G is nilpotent and indecomposable, then up to conjugacy in $\text{GL}(n, \mathbb{F})$, the elements of G have the form*

$$\begin{pmatrix} a(g) & c_{12}(g)a(g) & \dots & c_{1k}(g)a(g) \\ 0 & a(g) & \dots & c_{2k}(g)a(g) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a(g) \end{pmatrix}$$

where $G_1 = a(G) = a(G_s) \leq \text{GL}(n_1, \mathbb{F})$ is the irreducible part of G , and the $c_{ij}(g)$ are contained in the $\text{Mat}(n_1, \mathbb{F})$ -centraliser of G_1 (which is a field). Thus $\langle G_s \rangle_{\mathbb{F}}$ is simple.

COROLLARY 2.6. *If G has a representation (1.1) and $a_{ij}(g) \neq 0$ for some $g \in G$ and i, j , but either $n_i \neq n_j$, or $n_i = n_j$ and $a_i(g), a_j(g)$ are not conjugate in $\text{GL}(n_i, \mathbb{F})$, then G is not nilpotent.*

Now we explain how nilpotency testing reduces to the situation that G is given by a generating set of semisimple matrices (which certainly occurs for nilpotent completely reducible G , although remember that given such a generating set we cannot initially tell whether or not G is completely reducible). Suppose that we have computed $g_{i(u)}$ and $g_{i(s)}$ for all $i, 1 \leq i \leq r$ (for example, by Lemma 2.1). If either $[g_{i(u)}, g_{j(s)}] \neq 1_n$ for some i, j , or we fail to confirm by the method detailed after Lemma 2.4 that $H = \langle g_{1(u)}, \dots, g_{r(u)} \rangle$ is unipotent, then G is not nilpotent by Lemma 2.2. If G passes both of these tests, then H is a p -group and $[H, K] = 1$, where $K = \langle g_{1(s)}, \dots, g_{r(s)} \rangle$. We are then faced with testing nilpotency of K . At this stage, nilpotency of G is equivalent to nilpotency of K , for if K is nilpotent then so too is G , as the direct product of K and the p -group H . We give an algorithm later in Subsection 2.4 for testing nilpotency of a subgroup of $\text{GL}(n, \mathbb{F})$ input by a generating set of semisimple matrices (Algorithm 2).

2.2. Nilpotent completely reducible matrix groups

In this subsection we outline structural results for nilpotent completely reducible matrix groups.

The following lemmas hold over any field.

LEMMA 2.7. *If G is nilpotent and completely reducible, then every subgroup of G is completely reducible.*

Proof. (Cf. [27, §29, Theorem 5].) By Lemma 2.4, G consists of semisimple matrices, so every subgroup is completely reducible, by Maschke's theorem. □

LEMMA 2.8. *If G is completely reducible, then every subnormal subgroup is completely reducible.*

Proof. This is achieved by repeated application of Clifford's theorem. □

Let

$$1 = Z_0(H) \leq Z_1(H) = Z(H) \leq Z_2(H) \leq \dots$$

be the upper central series of a group $H \neq 1$. That is, $Z_i(H)/Z_{i-1}(H) = Z(H/Z_{i-1}(H))$, $i \geq 1$. The next two lemmas contain ideas that recur throughout the paper (see [18, §4.5]).

LEMMA 2.9. *For any group H , and any fixed $a \in Z_2(H)$, the assignment $h \mapsto [h, a]$ defines a homomorphism $\varphi_a: H \rightarrow Z(H) \cap [H, H]$.*

LEMMA 2.10. *Suppose that H is a nonabelian group such that $Z(H) \cap [H, H]$ is cyclic. Let $a \in Z_2(H) \setminus Z(H)$. Then there exists $h_a \in H$, $h_a \neq 1$, such that $H = \langle h_a, C_H(a) \rangle$.*

Proof. By Lemma 2.9, $H / \ker \varphi_a \cong \varphi_a(H)$ is cyclic, so H is generated by $\ker \varphi_a = C_H(a)$ and one other element. \square

Lemma 2.10 will be applied in practice to normal subgroups H of G . In that setting, the following procedure can be employed to find an element of $Z_2(H) \setminus Z(H)$.

Algorithm 1: SecondCentralElement(G, H)

Input: $G = \langle g_1, \dots, g_r \rangle \leq \text{GL}(n, \mathbb{F})$, $H = \langle h_1, \dots, h_s \rangle \trianglelefteq G$, H nonabelian.

$a := h_j \notin Z(H)$;
 while there exists g_i such that $[g_i, a] \notin Z(H)$ do
 $a := [g_i, a]$;
 return a .

As long as G is nilpotent, the loop is guaranteed to terminate in time that is polynomial in the nilpotency class of G (see [18, §4.5]). Always $a \in H \setminus Z(H)$, and at termination $a \in Z_2(H) \setminus Z(H)$. Indeed, at termination $[G, a] \leq Z(H)$, so that $\varphi_a(H)$ and $\ker \varphi_a = C_H(a)$ are normal subgroups of G for φ_a as in Lemma 2.9. Supposing that $Z(H) \cap [H, H]$ is cyclic, we have $\varphi_a(H) = \langle e_1, \dots, e_s \rangle = \langle e_a \rangle$ say, where $e_i = [h_i, a]$. Finding e_a is basically an order calculation, for if we know the orders $|e_i|$ then we know a generator of each Sylow subgroup of $\varphi_a(H)$, and a generator of the entire group is the product of these (the Sylow q -subgroup of $\varphi_a(H)$ is $\langle e_1^{\eta_1}, \dots, e_s^{\eta_s} \rangle = \langle e_i^{\eta_i} \rangle$ where $e_i^{\eta_i}$ is the q -part of e_i , and $e_i^{\eta_i}$ has maximal order among the $e_i^{\eta_i}$). Define $h_a = h_1^{\varepsilon_1} \dots h_s^{\varepsilon_s}$ to be the preimage of $e_a = e_1^{\varepsilon_1} \dots e_s^{\varepsilon_s}$ under φ_a . Then $H = \langle h_a, C_H(a) \rangle$.

The nilpotency class $\text{cl}(G)$ of G is the largest class of a Sylow subgroup of G . Let $t \neq p$ be prime. The class of a Sylow t -subgroup K of $\text{GL}(n, \mathbb{F})$ is known: by [5, C.3(a)] we know that $\text{cl}(K) \leq (t - 1)sn + n$ where t^s is the order of a Sylow t -subgroup of \mathbb{F}^\times . So when G is nilpotent,

$$n \cdot \max\{(t - 1)s + 1\} \tag{2.2}$$

is an upper bound for the number of rounds in which Algorithm 1 will terminate; if this bound is exceeded without termination, then we report that G is not nilpotent.

From now on in this subsection, G is irreducible unless stated otherwise.

The centraliser of G in $\text{Mat}(n, \mathbb{F})$ is an extension field \mathbb{D} of \mathbb{F} , so that $Z(G) \leq \mathbb{D}^\times$ is cyclic. Thus Lemma 2.10 and the preceding discussion are valid for $H = G$.

LEMMA 2.11 (see [28, 1.19, p. 12]). *G is isomorphic to an absolutely irreducible subgroup \tilde{G} of $\text{GL}(m, \mathbb{D})$, where $n = m|\mathbb{D} : \mathbb{F}|$. Moreover, \tilde{G} is primitive if G is primitive.*

LEMMA 2.12. *Let G be primitive. If A is an abelian normal subgroup of G , then A is cyclic.*

Proof. By Clifford's theorem, A is completely reducible with equivalent irreducible parts. Therefore $\langle A \rangle_{\mathbb{F}}$ is a field. \square

REMARK 2.13. Although \tilde{G} in Lemma 2.11 is irreducible over the algebraic closure $\bar{\mathbb{D}}$ of \mathbb{D} , if G is primitive then \tilde{G} may not be primitive over $\bar{\mathbb{D}}$. However, if \tilde{G} is primitive over $\bar{\mathbb{D}}$ then the image of an abelian normal subgroup A of G under the isomorphism $G \rightarrow \tilde{G}$ is diagonalisable, and so scalar, and thus A is central in G .

We can consider G to be an absolutely irreducible matrix group, by Lemma 2.11. This has useful implications when G is nilpotent; for example, we derive a strong restriction on the exponent of $Z_2(G)/Z(G)$.

LEMMA 2.14. *If G is nilpotent and $b \in Z_2(G)$, then $b^n \in Z(G)$.*

Proof. See [26, Lemma 19, p. 58]. □

LEMMA 2.15. *Suppose that G is nonabelian nilpotent. Let $a \in Z_2(G) \setminus Z(G)$. Then the following statements hold.*

- (i) *There exists $g_a \in G$ such that $[g_a, a] = e_a$ generates the cyclic group $\varphi_a(G) \leq Z(G)$, and $G = \langle g_a, C_G(A) \rangle$, where $A = \langle a \rangle^G = \langle a, e_a \rangle$.*
- (ii) *$G/C_G(A) \cong AZ(G)/Z(G)$.*
- (iii) *$|e_a| = |G : C_G(A)|$ divides n .*

Proof. We already know by Lemma 2.10 that $G = \langle g_a, C_G(a) \rangle$. Since e_a is central in G , $C_G(a) = C_G(A)$. Then statement (i) is clear.

As $G/C_G(A)$ and $AZ(G)/Z(G)$ are both cyclic, to prove part (ii) we have only to show that these groups have the same order. But this follows from the observation that $[g_a^l, a] = [g_a, a]^l = [g_a, a^l]$ for all $l \geq 1$. Then part (iii) is a consequence of (ii) and Lemma 2.14. □

To recap: after finding $a := \text{SecondCentralElement}(G, G)$, we calculate a generator e_a of the cyclic group $\varphi_a(G)$, and then $A = \langle a, e_a \rangle$ is a noncentral abelian normal subgroup of G . This procedure to construct A will be labelled `NoncentralAbelian(G, a)`. Let $g_a \in G$ be such that $\varphi_a(g_a) = e_a$. A generating set for $C_G(A)$ can be found from the generating set $\{g_1, \dots, g_r\}$ for G and the transversal $\{1, g_a, \dots, g_a^{r-1}\}$ for the cosets of $C_G(A)$ in G , by the classical result of Schreier [23, Lemma 1.1]. We call this procedure, which returns $C_G(A)$ in the form of a generating set, `Centraliser(G, A)`. If G is nilpotent, then the output of `Centraliser(G, A)` has size dividing rn .

In a special case, the above deliberations can be re-cast using Galois theory. Suppose that A is a nonscalar normal subgroup of G such that $\langle A \rangle_{\mathbb{F}}$ is a field (here G need not be irreducible, nor nilpotent). The multiplicative group of $\langle A \rangle_{\mathbb{F}}$ is completely reducible, with equivalent irreducible parts of degree $|\langle A \rangle_{\mathbb{F}} : \mathbb{F}1_n|$ dividing n . Also, $G/C_G(A)$ is isomorphic to a subgroup of $\text{Gal}(\langle A \rangle_{\mathbb{F}}/\mathbb{F}1_n)$, and so is cyclic of order dividing n . Let $A = \langle a \rangle$, and define the homomorphism $\theta : G \rightarrow \text{Aut}(A)$ by $\theta(g) : a \mapsto gag^{-1}$, $g \in G$. Let k_i be integers such that $\theta(g_i)(a) = a^{k_i}$, where $1 \leq k_i < |a|$ and $\text{gcd}(k_i, |a|) = 1$, $1 \leq i \leq r$. Choose a generator $a \mapsto a^{k_1^{e_1} \dots k_r^{e_r}}$ of the cyclic group $\langle \theta(g_1), \dots, \theta(g_r) \rangle \cong G/C_G(A)$, and set $g_a = g_1^{e_1} \dots g_r^{e_r}$. Then $G = \langle g_a, C_G(A) \rangle$. We label this procedure for later reference in the final algorithm of Section 3: `GaloisGenerator(G, A)` returns g_a for given A .

2.3. Abelian completely reducible matrix groups

Frequently in this paper we encounter an abelian completely reducible subgroup A of $\text{GL}(n, \mathbb{F})$ and wish to calculate the simple algebras (fields) $A_i \subseteq \langle A \rangle_{\mathbb{F}}$ such that $\langle A \rangle_{\mathbb{F}} = \bigoplus_i A_i$. These simple algebras can be found by a ‘cutting procedure’ as in [21, §3]. For

the sake of completeness, we give here details of this procedure, which takes as input any commutative semisimple algebra over a finite field, such as any subalgebra of $\langle A \rangle_{\mathbb{F}}$. It is assumed that we are able to compute efficiently an \mathbb{F} -basis for any subalgebra of $\langle A \rangle_{\mathbb{F}}$ given by an algebra generating set (see [21, p.223]), and also efficiently compute the factorisation into irreducibles of a polynomial over a finite field (see [21, p.224] or [12, §7.2]). We rely on the following lemma.

LEMMA 2.16. *Let $a \in \text{Mat}(n, \mathbb{K})$, where \mathbb{K} is any field.*

- (i) *The minimal polynomial of a over \mathbb{K} is irreducible if and only if $\langle a \rangle_{\mathbb{K}}$ is a field.*
- (ii) *$\langle a \rangle_{\mathbb{K}}$ is a direct sum of fields if and only if the minimal polynomial of a over \mathbb{K} has no repeated irreducible monic factors.*

Let B be any subalgebra of $\langle A \rangle_{\mathbb{F}}$, and let $\{a_1, \dots, a_m\}$ be an \mathbb{F} -basis of B . At the first stage of the procedure, we factorise the minimal polynomial $f(\xi)$ of a_1 over $\mathbb{F}_0 = \mathbb{F}$. If $f(\xi)$ is irreducible, then $\langle a_1 \rangle_{\mathbb{F}}$ is a field, \mathbb{F}_1 , and we move on to the next basis element a_2 ; that is, we replace \mathbb{F}_0 by \mathbb{F}_1 , a_1 by a_2 , and repeat. Otherwise we find $f(\xi) = h(\xi)\bar{h}(\xi)$ for nonconstant coprime \mathbb{F} -polynomials $h(\xi), \bar{h}(\xi)$. Note that $h(a_1) \neq 0, \bar{h}(a_1) \neq 0$ and $h(a_1)\bar{h}(a_1) = 0$. The identity polynomial is an \mathbb{F} -linear combination of $h(\xi), \bar{h}(\xi)$, so that $B = Bh(a_1) \oplus B\bar{h}(a_1)$ is a nontrivial decomposition of B into a direct sum of ideals. The cutting procedure is now applied to both of the \mathbb{F} -algebras $Bh(a_1)$ and $B\bar{h}(a_1)$. At any subsequent stage of the procedure we have B as a direct sum of algebras, each over some extension field of \mathbb{F} in B . Thus B will ultimately be returned as a direct sum of \mathbb{F} -extension fields. These summands constitute the output of the above described recursion, which we label `Cutting(B)`.

2.4. Testing nilpotency

In this subsection, G is completely reducible unless stated otherwise. We also assume that Algorithm 1 terminates in a number of rounds not greater than that specified by (2.2), for all normal subgroups H of G . (If termination is not achieved thus for some H , then we will know that G is not nilpotent.) Whenever this procedure is invoked, its first argument is always fixed as our original input group G .

To test nilpotency of G , we attempt to construct a short subnormal series of G with abelian factors, adapting a normal series proposed by Luks [18, §4.5]. If we find G to be nilpotent, then our method will have computed its Sylow subgroups as well. In the next section, a series of such type will also be used to test primitivity and irreducibility of nilpotent matrix groups.

Let G be nonabelian, and find $a \in Z_2(G) \setminus Z(G)$ via `SecondCentralElement(G, G)`. Denote $\varphi_a(G) = \langle [g_i, a] : 1 \leq i \leq r \rangle$ by E_a , and $\langle a \rangle^G = \langle a, E_a \rangle$ by A . Although $E_a \leq Z(G)$ is abelian, it is not necessarily cyclic. However, it is possible to get essential reductions to the cyclic situation. Let

$$V = V_1 \oplus \dots \oplus V_k \tag{2.3}$$

be the decomposition of V into a direct sum of irreducible G -submodules V_i . Then G is nilpotent if and only if the restriction G_{V_i} of G to V_i is nilpotent for all $i, 1 \leq i \leq k$. The restriction of $Z(G)$ to V_i is contained in $Z(G_{V_i})$, so that $(E_a)_{V_i}$ is cyclic.

LEMMA 2.17. *If G is nilpotent, then $G/\mathbf{C}_G(A) \cong E_a$ is an abelian group that can be generated by $n/2$ elements, each of order not greater than n .*

Proof. If $\dim(V_i) = 1$, then $(E_a)_{V_i} = [G, a]_{V_i} = [G_{V_i}, a_{V_i}] = 1$. Let m be the number of 1-dimensional V_i . Then $n \geq m + 2(k - m)$, implying that E_a can be generated by $k - m \leq n/2$ elements. Also, as $a_{V_i} \in Z_2(G_{V_i})$ and G_{V_i} is an irreducible nilpotent linear group over \mathbb{F} , $|(E_a)_{V_i}| \leq n$ by Lemma 2.14. \square

We need to know the primary invariant form of E_a . Lemma 2.17 limits the primes that can appear in this form.

COROLLARY 2.18. *Each prime dividing $|E_a|$ is not greater than n .*

Proof. Let $\{x_1, \dots, x_s\}$ be a generating set for E_a , where $|x_i| \leq n$ for all i . The order of the abelian group E_a then divides $\prod_{i=1}^s |x_i|$. A prime divisor q of $|E_a|$ must divide some $|x_i|$; hence $q \leq n$. \square

We may not have a decomposition of V into irreducible G -submodules. However, V is completely reducible as an E_a -module, so let the V_i in (2.3) be the E_a -homogeneous components of V . We now describe how to obtain a transversal for the cosets of $C_G(A)$ in G . Each V_i is a sum of isomorphic irreducible E_a -submodules of V , and the V_i are pairwise nonisomorphic simple E_a -modules. The simple components S_i in a semisimple decomposition $\langle E_a \rangle_{\mathbb{F}} = \bigoplus_i S_i$ may be efficiently calculated by the cutting procedure in Subsection 2.3, thereby yielding the E_a -homogeneous components $V_i = S_i V$ of V ; here it is crucial that E_a is an abelian completely reducible subgroup of $\text{GL}(n, \mathbb{F})$. If U is an irreducible E_a -submodule of V and $g \in G$, then gU is an irreducible E_a -submodule of V isomorphic to U . Therefore $gV_i = V_i$, and (2.3) is a direct sum of G -modules. Since $\langle (E_a)_{V_i} \rangle_{\mathbb{F}}$ is a field, $(E_a)_{V_i}$ is cyclic. As in the proof of Lemma 2.17, we may argue that $(E_a)_{V_i} = 1$ if $\dim(V_i) = 1$, so that $E_a \leq \times_i (E_a)_{V_i}$ can be generated by up to $n/2$ elements. With a generator for each $(E_a)_{V_i}$ in hand, the elements of E_a as words in the $e_l = [g_l, a]$ are easily found. For instance, supposing that $\dim(V_1) > 1$, we first find a representative b_1 for a generator of the cyclic group $E_a/B \cong (E_a)_{V_1}$, where $B = E_a \cap \times_{j \neq 1} (E_a)_{V_j}$ is the kernel of the projection homomorphism $E_a \rightarrow (E_a)_{V_1}$. Hence $T = \{1, b_1, \dots, b_1^{m-1}\}$, $m = |E_a/B|$, is a transversal for the cosets of B in E_a . The Schreier lemma [23, Lemma 1.1] then says that

$$e_1 \bar{e}_1^{-1}, \dots, e_r \bar{e}_r^{-1}, b_1^m$$

generate B ; here \bar{x} is the element of T such that $B\bar{x} = Bx$. After applying the same process to B in place of E_a and $B' = B \cap \times_{j \neq 2} (E_a)_{V_j}$ in place of B to find a generator $b_2 B'$ of $B/B' \cong B_{V_2}$, and so on, we eventually get a generating set b_1, b_2, \dots, b_k for E_a such that

$$E_a = \{b_1^{i_1} b_2^{i_2} \dots b_k^{i_k} \mid 0 \leq i_j < m_j\}$$

where m_j is the order of $b_j \bmod \langle b_{j+1}, \dots, b_k \rangle$. By calculating the prime factorisation of each order $|b_j|$ we can even find the primary invariant form of E_a . The preimage of this form under $\varphi_a : G \rightarrow E_a$ is a transversal for the cosets of $C_G(A)$ in G , and then the Schreier lemma once more yields generators for $C_G(A)$.

The import of the above is that definitions of the procedures labelled in Subsection 2.2 can be extended to G with noncyclic centre, and we are able to construct: (i) an abelian normal subgroup $A = \text{NoncentralAbelian}(G, a)$ of G such that $A \leq Z_2(G)$, $A \not\leq Z(G)$, for any $a \in Z_2(G) \setminus Z(G)$, and (ii) a generating set for $C_G(A)$, $\text{Centraliser}(G, A)$. These are the basic steps in a recursive procedure to construct a series of G with abelian factors. Indeed, set $A_1 = A$ and $C_{A_1} = C_G(A_1)$; if C_{A_1}/A_1 is abelian, then

$$\langle 1_n \rangle \triangleleft A_1 \leq C_{A_1} \triangleleft G$$

is such a series. Otherwise, since C_{A_1} is completely reducible and a nonabelian normal subgroup of G , after replacing G by C_{A_1} we can find an abelian normal subgroup A_2 of C_{A_1} such that $A_1 < A_2 \leq Z_2(C_{A_1})$, $A_2 \not\leq Z(C_{A_1})$, and C_{A_1}/C_{A_2} is abelian, where C_{A_2} denotes the centraliser of A_2 in C_{A_1} . Apart from C_{A_2}/A_2 , each factor of consecutive terms in the following series is abelian:

$$\langle 1_n \rangle \triangleleft A_1 \triangleleft A_2 \trianglelefteq C_{A_2} \triangleleft C_{A_1} \triangleleft G.$$

After l iterations we have the series

$$\langle 1_n \rangle \triangleleft A_1 \triangleleft A_2 \triangleleft \dots \triangleleft A_l \trianglelefteq C_{A_l} \triangleleft \dots \triangleleft C_{A_2} \triangleleft C_{A_1} \triangleleft G \quad (2.4)$$

where the A_i are abelian and C_{A_i} is the centraliser of A_i in $C_{A_{i-1}}$. Each factor of consecutive terms in (2.4) is abelian, except possibly C_{A_i}/A_i . To obtain C_{A_i} from $C_{A_{i-1}}$ and A_i from A_{i-1} , first calculate $a_i = \text{SecondCentralElement}(G, C_{A_{i-1}})$. Then

$$A_i = \langle A_{i-1}, \text{NoncentralAbelian}(C_{A_{i-1}}, a_i) \rangle = \langle A_{i-1}, a_i, \varphi_{a_i}(C_{A_{i-1}}) \rangle,$$

so that, since A_{i-1} and $\varphi_{a_i}(C_{A_{i-1}})$ are central in $C_{A_{i-1}}$, $C_{A_i} = \text{Centraliser}(C_{A_{i-1}}, A_i)$ is the centraliser of a_i in $C_{A_{i-1}}$. Recall then from the discussion after Lemma 2.10 that C_{A_i} is normal in G if $C_{A_{i-1}}$ is. Hence all terms C_{A_i} in (2.4) are normal in G . The same is not true of the A_i ; A_i is only certain to be normal in $C_{A_{i-1}}$. Construction of (2.4) is summarised below.

Algorithm 2: TestSeries(G, l)

Input: $G = \langle g_1, \dots, g_r \rangle \leq \text{GL}(n, \mathbb{F})$ nonabelian, $l \geq 2$ an integer.

```

 $A_0 := \langle 1_n \rangle;$ 
 $C_{A_0} := G;$ 
for  $0 \leq i \leq l - 1$  do
  while  $C_{A_i}/A_i$  is nonabelian do
     $a_{i+1} := \text{SecondCentralElement}(G, C_{A_i});$ 
     $A_{i+1} := \langle A_i, \text{NoncentralAbelian}(C_{A_i}, a_{i+1}) \rangle;$ 
     $C_{A_{i+1}} := \text{Centraliser}(C_{A_i}, A_{i+1});$ 
  return  $A_{i+1}, C_{A_{i+1}}.$ 

```

For nilpotent G , Lemma 2.17 constrains the size and number of generators of each factor $C_{A_{i-1}}/C_{A_i}$ in (2.4). We similarly seek a bound on l .

LEMMA 2.19. *If A is an abelian completely reducible subgroup of $\text{GL}(n, \mathbb{F})$ then the \mathbb{F} -dimension of $\langle A \rangle_{\mathbb{F}}$ is not greater than n .*

Proof. $\langle A \rangle_{\mathbb{F}}$ is contained in a direct sum of fields, whose \mathbb{F} -dimensions sum to n . □

LEMMA 2.20. *In any series (2.4), $l \leq n - 1$.*

Proof. For all i , $2 \leq i \leq l$, we must have $\langle A_i \rangle_{\mathbb{F}} \neq \langle A_{i-1} \rangle_{\mathbb{F}}$, because otherwise $C_{A_{i-1}} \leq C_{A_i}$. Thus $\dim \langle A_i \rangle_{\mathbb{F}} > \dim \langle A_{i-1} \rangle_{\mathbb{F}}$. Also $\dim \langle A_1 \rangle_{\mathbb{F}} > 1$, since $\langle A_1 \rangle_{\mathbb{F}} = \mathbb{F}1_n$ contradicts $A_1 \not\leq Z(G)$. By induction, then, $\dim \langle A_i \rangle_{\mathbb{F}} \geq i + 1$. Hence $l \leq n - 1$ by Lemmas 2.8 and 2.19. □

COROLLARY 2.21. `TestSeries`(G, l) returns a series of G with abelian factors for some $l < n$.

Corollary 2.21 is startling at first sight, as it says that G is soluble, which was never one of our assumptions. But recall that we did make an assumption about the time in which `SecondCentralElement`($G, -$) terminates. For this condition to be satisfied, it is sufficient, but not necessary, that G be nilpotent. Apart from the bounds provided by Lemma 2.17, which impinge on efficiency estimates, nowhere else in the reasoning leading up to Corollary 2.21 is nilpotency of G required. Thus in constructing (2.4), for some $l < n$ we discover either that G is not nilpotent, or that G is soluble. In the latter case, the abelian series of G obtained can be used to do much more than just nilpotency testing — see Remark 2.24 below.

The next issue to address is an exponential growth of the number of generators for the terms C_{A_i} of (2.4). This can be avoided by proceeding as in [18, §4.2]. Relying on the fact that each C_{A_i} is normal in G , the idea is to store for C_{A_i} not a full generating set, but rather a generating set for a subgroup of C_{A_i} whose normal closure in G is C_{A_i} .

Suppose that G/C_{A_1} is cyclic: this is the key case, especially later in Section 3 where we consider irreducibility and primitivity testing of nilpotent matrix groups. Say $G/C_{A_1} = \langle gC_{A_1} \rangle$ and $|G : C_{A_1}| = m$. By Schreier,

$$\left\{ g^i \overline{g_j g_j^{-1}}^{-1} \mid 0 \leq i \leq m-1, 1 \leq j \leq r \right\}$$

is a generating set for C_{A_1} , where \bar{x} denotes the representative of xC_{A_1} in the transversal $\{g^i \mid 0 \leq i \leq m-1\}$ for the cosets of C_{A_1} in G . It is not difficult to see that C_{A_1} is the normal closure in G of the subgroup with generating set

$$\{g_j \bar{g}_j^{-1}, g^m \mid 1 \leq j \leq r\}. \tag{2.5}$$

We expand (2.5) to a full generating set for C_{A_1} by adding the conjugate of each element $g_j \bar{g}_j^{-1}$ by each power g^i of g , $1 \leq i \leq m-1$. More generally, we have the following proposition.

PROPOSITION 2.22. *Suppose that $C_{i-1} = \langle h_1, \dots, h_s \rangle^G$ and C_{i-1} has a subgroup C_i normal in G such that $C_{i-1}/C_i = \langle hC_i \rangle$ is cyclic of order m . For $x \in C_{i-1}$ denote by \bar{x} the element of $\{1, h, \dots, h^{m-1}\}$ such that $xC_i = \bar{x}C_i$. Then $C_i = B^G$ where B is the subgroup of C_i generated by*

$$\left\{ h_j \bar{h}_j^{-1}, g_k h g_k^{-1} \overline{g_k h g_k^{-1}}^{-1}, h^m \mid 1 \leq j \leq s, 1 \leq k \leq r \right\}.$$

Proof. Given $x \in C_{i-1}$, define $\omega(x)$ to be the element $x\bar{x}^{-1}$ of C_i . Note that $\omega(x) = x$ if $x \in B^G$. Since $\overline{xy} \in \bar{x}\bar{y}\langle h^m \rangle$, it follows that $\omega(xy) \in \omega(x)\omega(y)\bar{x}^{-1}B^G$, so that

$$\omega(x), \omega(y) \in B^G \implies \omega(xy) \in B^G \tag{2.6}$$

for all $x, y \in C_{i-1}$. In particular $\omega(g_k h^l g_k^{-1}) = \omega((g_k h g_k^{-1})^l) \in B^G$, $1 \leq l \leq m-1$.

We next show that $\omega(ghg^{-1}) \in B^G$ for all $g \in G$ by induction on the word length of g . This is trivially true if g is a generator g_k , so write $g = g_k u$ and assume that $\omega(uhu^{-1}) \in B^G$. Set $\overline{uhu^{-1}} = h^l$, meaning that $uhu^{-1} = h^l z$ for some $z \in B^G$. Therefore

$$\omega(ghg^{-1}) = \omega(g_k h^l g_k^{-1} \cdot z^{g_k^{-1}}) \in B^G$$

by (2.6).

Suppose that $\overline{h_j} = h^{l_j}$; then

$$\omega(gh_jg^{-1}) = \omega(h_j)g^{-1}\omega(gh^{l_j}g^{-1}) \in B^G.$$

Consequently, $\omega(x) \in B^G$ for all $x \in C_{i-1}$, and so all Schreier generators $\omega(h^l x)$ of C_i are in B^G , as required. \square

By Proposition 2.22, $C_{A_i} = B_i^G$ where the subgroup B_i has generating set of size $i(r+1)$. For fixed input G and all factors $C_{A_{i-1}}/C_{A_i}$ cyclic, this is only linear growth in the size of generating sets for the B_i with increasing i (up to maximum size $(n-1)(r+1)$, by Corollary 2.21). If $C_{A_{i-1}}/C_{A_i}$ is noncyclic, then we must include in a generating set for B_i commutators of transversal elements, as well as the usual power relators. For example, suppose that $G/C_{A_1} = \langle gC_{A_1} \rangle \times \langle hC_{A_1} \rangle$, $|gC_{A_1}| = l$, $|hC_{A_1}| = m$. Then

$$C_{A_1} = \langle g_j \overline{g_j}^{-1}, g^l, h^m, [g, h] : 1 \leq j \leq r \rangle^G.$$

Since $C_{A_{i-1}}/C_{A_i}$ can be generated by at most $n/2$ elements, $C_{A_i} = B_i^G$ where $B_i \leq C_{A_i}$ is generated by at most $i(r+n(n+2)/8)$ elements.

Calculation of the abelian terms A_i in (2.4) depends on calculating $\varphi_{a_i}(C_{A_{i-1}}) = \varphi_{a_i}(B_{i-1})^G$. So suppose that we have a generating set for an abelian subgroup H of G and wish to calculate the primary invariant form of H^G , given that H^G is also abelian. First we calculate an \mathbb{F} -basis of $\langle H \rangle_{\mathbb{F}}$. The G -closure $\langle H^G \rangle_{\mathbb{F}}$ of $\langle H \rangle_{\mathbb{F}}$ may be found by successively adding g_i -conjugates of basis elements to the original \mathbb{F} -basis. This process is capped by the upper bound n on $\dim_{\mathbb{F}}(\langle H^G \rangle_{\mathbb{F}})$. Note also that the H -homogeneous components of V are H^G -modules. Given the discussion after Corollary 2.18, we confine attention to the case that $\langle H^G \rangle_{\mathbb{F}}$ is a field. But in that case H^G is cyclic, so $H^G = H$.

Suppose that all factors of consecutive terms in (2.4) are abelian. We have seen that in constructing this abelian series we produce generators in primary invariant form for each A_i and each factor $C_{A_{i-1}}/C_{A_i}$. Thus (2.4) can be refined to a series

$$\langle 1_n \rangle = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_m = G \quad (2.7)$$

with all factors cyclic, $H_i/H_{i-1} = \langle h_i H_{i-1} \rangle$ say.

LEMMA 2.23. *Suppose that H_{i-1} is nilpotent and $p_1, \dots, p_s, q_1, \dots, q_t$ are the primes in the primary invariant forms $H_{i-1,p_1} \times \dots \times H_{i-1,p_s}$ of H_{i-1} and $\langle h_{i,q_1} \rangle \times \dots \times \langle h_{i,q_t} \rangle$ of $\langle h_i \rangle$. Then H_i is nilpotent if and only if $[H_{i-1,p_j}, h_{i,q_k}] = 1_n$ for all $p_j, q_k, p_j \neq q_k$.*

Proof. Since H_{i-1,p_j} is the Sylow p_j -subgroup of H_{i-1} , and H_{i-1} is normal in H_i , each H_{i-1,p_j} is normal in H_i .

If H_i is nilpotent and $p_j \neq q_k$, then $H_{i-1,p_j}, \langle h_{i,q_k} \rangle$ lie in different Sylow subgroups of H_i , and therefore they centralise each other.

Suppose that $[H_{i-1,p_j}, h_{i,q_k}] = 1_n$ for all $p_j \neq q_k$. Let $I = \{p_1, \dots, p_s\} \cap \{q_1, \dots, q_t\}$. A Sylow p_j -subgroup of H_i is $\langle h_{i,p_j}, H_{i-1,p_j} \rangle$ or H_{i-1,p_j} according as $p_j \in I$ or $p_j \notin I$ respectively, and $\langle h_{i,q_k} \rangle$ is a Sylow q_k -subgroup of H_i if $q_k \notin I$. Clearly then every Sylow subgroup of H_i is normal in H_i , and so H_i is nilpotent. \square

REMARK 2.24. The series (2.7) yields a polycyclic generating sequence h_1, \dots, h_m for G . Using this sequence and (2.7) we may write down a polycyclic presentation for G (see [25, pp. 394–395]), thus gaining access to numerous algorithms for polycyclically presented groups (see, for example, [12, Chapter 8]).

Lemma 2.23 affords a method for testing nilpotency of any subgroup G of $\mathrm{GL}(n, \mathbb{F})$ with a series (2.7). Testing can begin at the term in (2.7) that corresponds to A_l in (2.4). This method additionally finds the Sylow subgroups of G , if G is nilpotent. Certain Sylow subgroups we can identify beforehand as abelian.

LEMMA 2.25. *Let $q \neq p$ be a prime greater than n . A q -subgroup H of $\mathrm{GL}(n, \mathbb{F})$ is abelian.*

Proof. By Maschke's theorem, H is completely reducible. Consider an irreducible part L of H ; by Lemma 2.11 this is isomorphic to an irreducible linear q -group \tilde{L} over the algebraic closure $\bar{\mathbb{F}}$ of \mathbb{F} . Then \tilde{L} is monomial over $\bar{\mathbb{F}}$, and since $q > n$, \tilde{L} is a group of diagonal matrices over $\bar{\mathbb{F}}$. So each irreducible part of H is abelian, implying that H itself is abelian. \square

COROLLARY 2.26. *Let $q \neq p$ be a prime greater than n . If G is nilpotent, then the Sylow q -subgroup of G is central.*

Hence the q -parts of the generators of G can be excised in nilpotency testing of G (see also [18, §5], and cf. Corollary 2.18).

Now we are in a position to state a nilpotency testing algorithm for G generated by semisimple matrices; we are relaxing the condition that G is completely reducible, although remember that G will indeed be completely reducible if it is nilpotent. At the end of Subsection 2.1 we explained how such an algorithm allows nilpotency testing of an arbitrary nonabelian subgroup of $\mathrm{GL}(n, \mathbb{F})$.

Algorithm 3: IsNilpotent(G)

Input: $G = \langle g_1, \dots, g_r \rangle \leq \mathrm{GL}(n, \mathbb{F})$ nonabelian, g_i semisimple matrices.

$\pi :=$ the set of primes less than or equal to n .

1. Calculate the π -part $g_{i,\pi}$ and the π' -part $g_{i,\pi'}$ of each generator g_i of G . Set $G_\pi = \langle g_{1,\pi}, \dots, g_{r,\pi} \rangle$ and $G_{\pi'} = \langle g_{1,\pi'}, \dots, g_{r,\pi'} \rangle$.
 2. If $G_{\pi'} \not\leq \mathbf{Z}(G)$ then by Corollary 2.26 report ' G is not nilpotent'. Else go to the next step.
 3. Run TestSeries($G_\pi, n - 1$). If this procedure does not terminate with an abelian series of G_π then by Corollary 2.21 report ' G is not nilpotent'. Else go to the next step.
 4. Test nilpotency of G_π using Lemma 2.23 and refinement of the abelian series computed in the previous step. If G_π is not nilpotent, or the characteristic p of \mathbb{F} is in π and a p -element of G_π is detected, then report ' G is not nilpotent'. Else report ' G is nilpotent', for $G_{\pi'}$ is abelian and $G = G_\pi \times G_{\pi'}$ from step (2).
-

The basic steps in Algorithm 3 comprise the construction of abelian subnormal subgroups of G and their centralisers, which in turn use algorithms for cutting up a commutative semisimple algebra into its simple components, and for computing the primary invariant form of abelian groups. The overall efficiency of Algorithm 3 is justified by various bounds on the lengths of series, and the order and number of generators of series factors. These

bounds are expressible in terms of the degree n , the size q of the field \mathbb{F} , and the number of generators r , of the input completely reducible group G .

Let G be nilpotent. The construction of abelian subnormal subgroups of G calls Algorithm 1 (SecondCentralElement($G, -$)), which terminates in a number of rounds l not greater than the nilpotency class of G ; hence $l \leq qn$ (see (2.2)). The number of group operations needed to construct each abelian subnormal subgroup depends on the size of a generating set for a related subgroup of G (whose normal closure in G is a centraliser at the previous stage), a number which is never more than $n(r + n(n + 2)/8)$, by virtue of Lemma 2.20 and Proposition 2.22. Hence the computation of abelian subnormal subgroups is polynomial-time in n, q, r . Constructing centralisers is also a polynomial-time process, because of the above bound on the number of generators, and also bounds on the length of transversals which we use in the algorithm to compute Schreier generators (see Lemmas 2.15 and 2.17). We repeat the construction of abelian subnormal subgroups and centralisers at most $n - 1$ times (Lemma 2.20).

In several stages of the algorithm (constructing transversals in Centraliser(G, A), and steps (1) and (4) of Algorithm 3) we should compute the order of an element g of G or a factor group. By [6], computing orders uses on average $O(n^3 \log q)$ field operations. But in Algorithm 3 we will know, or can readily find, k such that $|g|$ divides k and all prime divisors of k are less than or equal to n (cf. Lemma 2.15 and Corollary 2.18). Hence, we can apply the OrderBounded function from [12, pp. 72–73], which calculates $|g|$ in time at most $O((\log k)^3)$.

Also note that in step (4) of Algorithm 3 all primes dividing the order of $g \in G_\pi$ are less than or equal to n , and that an upper bound on the power of a prime dividing $|g|$ is $\log_2 |\text{GL}(n, \mathbb{F})| \leq n^2 \log_2 q$ ([18, §4.4]). By the above bounds on the number of generators of terms in the abelian series, we need only to calculate orders for a number of group elements which depends polynomially on n, q and r .

Our procedures use computation in finite fields and elementary computational linear algebra. The reader may consult [12, §7.1–7.3] for necessary algorithms in those areas, such as algorithms for computing minimal polynomials and the prime factorisation of polynomials over \mathbb{F} . Prime factorisation of a polynomial $f(\xi)$ over \mathbb{F} can be done with a deterministic algorithm whose complexity is a polynomial in $p, \log_p q$, and $\deg(f)$; see [21, p. 224]. Since in our procedures $\deg(f) \leq n$ always, we have algorithms that are polynomial in n, p , and $\log_p q$. This is not polynomial in the input size. However, there exist randomised (Las Vegas) algorithms for factorising polynomials over finite fields which are polynomial in the input size, so these would be preferred in practice if the characteristic p of \mathbb{F} is large (again, see [21, p. 224]).

3. Irreducibility and primitivity testing of nilpotent matrix groups

In this section we develop algorithms for testing whether a nilpotent subgroup G of $\text{GL}(n, \mathbb{F})$ is irreducible or primitive. Our algorithms also construct, in parallel, proper nonzero G -submodules of V if G is reducible, and a G -system of imprimitivity if G is imprimitive.

We point out that the nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$ have been completely classified up to $\text{GL}(n, \mathbb{F})$ -conjugacy, in [8, 9]. The paper [8] contains an algorithm that returns the classification as a list of generating sets of matrices, for any input n and \mathbb{F} . We borrow from [8, 9] in parts of our primitivity testing algorithm (see Subsection 3.3).

Suppose that G is nilpotent. If $G_u \neq 1$, then G is reducible, but not completely reducible.

Indeed, we have seen after Lemma 2.4 how to compute a proper nonzero G -submodule W of V : $W = \text{Fix}(G_u)$ is a completely reducible proper G -submodule of V on which G_u acts trivially. This fulfils one of our primary goals, namely constructing nontrivial G -modules in the case that G is reducible. In our ongoing discussion of irreducibility and primitivity testing of G , we may therefore assume that $G_u = 1$, so that G is completely reducible and $\langle G \rangle_{\mathbb{F}}$ is semisimple. This assumption holds for the entire section. As we will see, with this assumption in place, module construction need only ever be undertaken for abelian matrix groups.

Our approach to all of the computational problems in this section is to lift knowledge about abelian normal subgroups of G to knowledge about G . If we know a *noncyclic* abelian normal subgroup N of G , then primitivity testing of G ends by Lemma 2.12, but irreducibility testing could continue. That is, there are at least two different N -homogeneous components of V (remember that N is abelian: modules for completely reducible abelian linear groups can be constructed by Subsection 2.3), and the set of all components furnishes either a proper nonzero G -submodule of V — if the permutation action of G on the set of components is intransitive — or a G -system of imprimitivity. In the latter situation, irreducibility testing goes down to a strictly smaller degree by the following theorem.

THEOREM 3.1. *Let \mathbb{K} be any field and W the underlying vector space for $\text{GL}(n, \mathbb{K})$. Suppose that H is a completely reducible subgroup of $\text{GL}(n, \mathbb{K})$, and N is a normal subgroup of H . Let $W = W_1 \oplus \cdots \oplus W_l$ be the decomposition of the completely reducible N -module W into N -homogeneous components W_i (hence $\mathcal{W} = \{W_1, \dots, W_l\}$ is a H -system of imprimitivity). Let $\text{Stab}_H(W_i) = \{h \in H \mid hW_i = W_i\}$ be the stabiliser in H of W_i . Then H is irreducible if and only if H acts transitively on \mathcal{W} , and W_i is an irreducible $\text{Stab}_H(W_i)$ -module for some, and hence every, i .*

Proof. There is nothing to prove if $l = 1$, so let $l \geq 2$.

Suppose that W_i is an irreducible $\text{Stab}_H(W_i)$ -module for some i . Suppose also that H is transitive on \mathcal{W} , so all of the stabilisers are conjugate and every W_i is an irreducible $\text{Stab}_H(W_i)$ -module. Let Z be the $\text{Mat}(n, \mathbb{K})$ -centraliser of H . Since Z centralises N , W_i is a Z -module for all i . The restriction Z_i of Z to W_i is a division algebra.

For each i , $2 \leq i \leq l$, H contains an element h_i such that $h_i W_1 = W_i$, so that, up to conjugacy, h_i is an $l \times l$ block monomial matrix with a single nonzero block x_i in column 1, at row i . If $z = \text{diag}(z_1, \dots, z_l) \in Z$, then $zh_i = h_i z$ implies that $z_i = x_i z_1 x_i^{-1}$. Thus Z is isomorphic to Z_1 , so is a division algebra. It follows that H is irreducible.

The converse is a standard statement, by Clifford's theorem (see [20, pp. 217–218]). \square

Theorem 3.1 is especially apt when G is nilpotent: finite nilpotent groups without a noncyclic abelian normal subgroup are of a very restricted kind, which we describe in Subsection 3.2.

To utilise Theorem 3.1 when $G \leq \text{GL}(n, \mathbb{F})$ has a known noncyclic abelian normal subgroup N , first we need to find the N -homogeneous components $\{W_i \mid 1 \leq i \leq l\}$ of V . This can be done using the cutting procedure of Subsection 2.3, which finds the simple components A_i of a commutative semisimple \mathbb{F} -algebra A . That is, each A_i is a field and an ideal of A , and $A = \bigoplus_i A_i$. If $A = \langle N \rangle_{\mathbb{F}}$ then the N -homogeneous components of V are the $W_i = A_i V$. Now we have a permutation representation $\rho : G \rightarrow \text{Sym}(l)$ arising from the action of G on the set of W_i . If $\rho(G)$ is intransitive then we stop, and return a proper nonzero G -submodule of V . Fix a value of i . Since $\ker \rho \leq \text{Stab}_G(W_i)$, the sets $G/\text{Stab}_G(W_i)$ and $\rho(G)/\rho(\text{Stab}_G(W_i))$ are bijective, so we obtain a transversal for the

cosets of $\text{Stab}_G(W_i)$ in G directly from a transversal for the cosets of $\rho(\text{Stab}_G(W_i))$ in the permutation group $\rho(G)$. Then the Schreier lemma yields generators for $\text{Stab}_G(W_i)$. By Theorem 3.1, G is irreducible if and only if $\text{Stab}_G(W_i)$ is irreducible in $\text{GL}(W_i)$.

Actually, to acquire nontrivial G -submodules or G -systems of imprimitivity in V , rather than a noncyclic abelian normal subgroup of G , we could ask more generally for any normal subgroup N with at least two inequivalent irreducible parts. The challenge then is to determine an imprimitivity system for G with at least two components. This task is manageable when N is abelian.

Let G be nilpotent, and let H be the product of all Sylow q -subgroups of G , where q ranges over the primes greater than n dividing $|G|$. Write $G = H \times K$. By Corollary 2.26, $H \leq \mathbf{Z}(G)$. We suppose that $H = \langle g \rangle$ is cyclic, for if H is noncyclic then G is reducible, and we get a proper nonzero G -submodule of V from the H -homogeneous components of V . If K is irreducible, then G is irreducible; likewise, if K is primitive, then G is primitive. Suppose that K is reducible, with irreducible module $0 \neq U < V$. For all i , $g^i U$ is an irreducible K -submodule of V isomorphic to U , and either U is a G -module, or the sum $W = \sum_{i=0}^{|H|-1} g^i U$ is direct. If $W = V$, then we surely have a G -system of imprimitivity; however Theorem 3.1 is of no help because this system constitutes just one K -homogeneous component. In all but this last case, then, and just as for nilpotency testing, for irreducibility and primitivity testing we can assume that the primes dividing $|G|$ are small: that is, no greater than n .

3.1. Abelian groups

In this subsection G is an abelian completely reducible subgroup of $\text{GL}(n, \mathbb{F})$.

It is well known that an abelian irreducible subgroup of $\text{GL}(n, \mathbb{F})$ is cyclic: its \mathbb{F} -enveloping algebra is a field. Therefore if G is noncyclic then it is reducible with at least two inequivalent irreducible parts, so $\langle G \rangle_{\mathbb{F}}$ is the direct sum of at least two different simple subalgebras, which can be found as in Subsection 2.3.

We turn now to questions about irreducibility and primitivity of completely reducible abelian subgroups of $\text{GL}(n, \mathbb{F})$. We first recall some facts about irreducible abelian linear groups.

LEMMA 3.2. *Suppose that $\langle G \rangle_{\mathbb{F}}$ is a field.*

- (i) *There is a single isomorphism type of irreducible G -submodule U of V .*
- (ii) *The \mathbb{F} -dimension of U is $|\langle G \rangle_{\mathbb{F}} : \mathbb{F}1_n|$, and divides n .*
- (iii) *G is irreducible if and only if $|\langle G \rangle_{\mathbb{F}} : \mathbb{F}1_n| = n$.*

LEMMA 3.3. *Let $G = \langle g \rangle \leq \text{GL}(n, \mathbb{F})$. Then the following statements are equivalent.*

- (i) *G is irreducible.*
- (ii) *$\langle G \rangle_{\mathbb{F}}$ is a field extension of \mathbb{F} of degree n .*
- (iii) *The characteristic polynomial of g is the minimal polynomial of g .*
- (iv) *$1, g, g^2, \dots, g^{n-1}$ are \mathbb{F} -linearly independent.*
- (v) *$\mathbb{C}_{\text{Mat}(n, \mathbb{F})}(g) = \langle g \rangle_{\mathbb{F}}$.*

Let $|\mathbb{F}| = q$. The largest order of an irreducible cyclic subgroup of $\text{GL}(n, \mathbb{F})$ is $q^n - 1$. A cyclic subgroup of this order, called a *Singer cycle*, is irreducible. For any n and q , Singer cycles always exist, and they form a single conjugacy class in $\text{GL}(n, \mathbb{F})$. It is possible to write

down explicitly a standard generator for any Singer cycle conjugacy class representative. By Lemma 3.2, a subgroup of a Singer cycle is irreducible if and only if it has order not dividing $q^m - 1$ for any m properly dividing n .

If $\text{Cutting}(\langle G \rangle_{\mathbb{F}})$ determines that $\langle G \rangle_{\mathbb{F}}$ is not a field, then G is reducible, and we have proper nonzero G -submodules of V . Suppose now that $\langle G \rangle_{\mathbb{F}}$ is a field. Thus G is cyclic, and knowing this fact and any generating set for G , it is easy to write down a single generator g of G . The \mathbb{F} -dimension of $\langle G \rangle_{\mathbb{F}}$ tells us whether or not G is irreducible, by Lemma 3.2(iii). Suppose that G is reducible. Take a direct decomposition $V_1 \oplus \cdots \oplus V_k$ of V into m -dimensional subspaces V_i , where $m = |\langle G \rangle_{\mathbb{F}} : \mathbb{F}1_n|$ is the degree of the minimal polynomial of g . Let $\langle h \rangle$ be an irreducible subgroup of $\text{GL}(m, \mathbb{F})$ such that $|h| = |g|$, and let $H = \langle \text{diag}(h, \dots, h) \rangle \leq \text{GL}(n, \mathbb{F})$. Then $xHx^{-1} = G$ for some $x \in \text{GL}(n, \mathbb{F})$ and xV_i is an irreducible G -submodule of V .

For the remainder of the subsection G is irreducible. Primitivity of G can be decided as in the next lemma.

LEMMA 3.4 (see [27, §15, Theorem 3]). *Let H be any irreducible subgroup of $\text{GL}(n, \mathbb{F})$. Then H is imprimitive if and only if for some proper divisor m of n , H contains a subgroup of index n/m which is the H -stabiliser of an m -dimensional subspace of V .*

The following procedure either reports that G is primitive, or returns a G -system of imprimitivity.

1. List the subgroups of G of index m for all $m < n$ dividing n .
2. Search in the list of step (1) for a subgroup H with a module U of dimension m (V is a direct sum of isomorphic irreducible H -modules by Lemma 3.2). If no such H exists, then G is primitive.
3. Assuming that suitable H and U were found in the previous step, test whether $H = \text{Stab}_G(U)$. If so, then G is imprimitive with imprimitivity system $\{U, gU, \dots, g^{m-1}U\}$ where $G = \langle g, H \rangle$. If $H \neq \text{Stab}_G(U)$ for all H, U then G is primitive.

Note that the calculations in steps (1)–(3) above are straightforward, because G is cyclic.

Primitivity of G can also be tested using an order criterion derived from Lemma 3.4: G is imprimitive if and only if $|G|$ divides $m(q^{n/m} - 1)$ for some prime divisor m of n (see [9, Proposition 2.8]). Thus in step (1) above we can restrict to prime m only.

3.2. Constructing abelian normal subgroups

If we ever detect an abelian normal subgroup N of G with at least two inequivalent irreducible parts, then $\text{Cutting}(\langle N \rangle_{\mathbb{F}})$ finds either a nonzero proper G -submodule of V , or a G -system of imprimitivity. For the purposes of irreducibility and primitivity testing of nilpotent linear groups, this observation prompts the abstract group-theory question: which finite nilpotent groups do not have a noncyclic abelian normal subgroup? Our answer to this question gives precise information about the isomorphism type of such groups, and hence (by Lemma 2.12) about the isomorphism type of nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$.

PROPOSITION 3.5. *Let H be a finite nonabelian nilpotent group. Then H does not have a noncyclic abelian normal subgroup if and only if $H = H_2 \times H_2'$ where the $2'$ -subgroup H_2' of H is cyclic and the Sylow 2-subgroup H_2 of H is one of the following: Q_8 when $|H_2| = 8$; dihedral or semidihedral or generalised quaternion when $|H_2| > 8$.*

Proof. It is a routine exercise to check that if H_2 is a 2-group as stated, then a maximal abelian normal subgroup of H_2 is cyclic. It follows that every abelian normal subgroup of H_2 — and thus of H if H_2 is cyclic — is cyclic.

Suppose that H does not have a noncyclic abelian normal subgroup. Then for every prime q dividing $|H|$, every abelian normal subgroup of H_q is cyclic. By [16, Satz 6.7, p. 304], this means that H_q is cyclic if q is odd, and H_q has a cyclic subgroup of index 2 if $q = 2$. Thus H_2 is cyclic. As a nonabelian 2-group with a cyclic maximal subgroup, H_2 is a dihedral or semidihedral or generalised quaternion, or a group with presentation

$$\langle a, x \mid x^2 = a^{2^{s-1}} = 1x^{-1}ax = aa^{2^{s-2}} \rangle, \quad s \geq 3;$$

see [20, 5.3.4, p. 141]. The last sort of group has a noncyclic abelian normal subgroup, namely $\langle a^{2^{s-2}}, x \rangle$. □

We next give some related results specifically about groups of prime power order.

LEMMA 3.6. *Let q be any prime. Suppose that H is a q -group with $[H, H]$ cyclic, and set $X = \mathbf{C}_H([H, H])$.*

- (i) *If $H \not\cong Q_8$ and X is noncyclic, then H has a noncyclic abelian normal subgroup N .*
- (ii) *Suppose that X is cyclic. If $q > 2$ then H is cyclic, and if $q = 2$ then either H is cyclic, or $|H| > 8$ and H is dihedral or generalised quaternion or semidihedral.*

Proof. Set $Z = \mathbf{Z}(X)$. We have $[X, X] \leq [H, H] \leq Z$ so that X is either abelian or has nilpotency class 2.

(i) Let X be noncyclic. If X is abelian, then N can be the characteristic subgroup X of H . We assume that X is nonabelian, so that it is class-2 nilpotent, and $X/[X, X]$ is abelian noncyclic. Define N_1 to be the noncyclic characteristic subgroup $\{h \in X \mid h^q \in [X, X]\}$ of X (hence N_1 is characteristic in H); that is, N_1 is the preimage in X of $\Omega_1(X/[X, X])$. If N_1 is abelian, then $N = N_1$ suffices.

Suppose that N_1 is nonabelian, and choose $a, b \in N_1$ such that $[a, b] \neq 1$. Since $a^q \in Z$ and N_1 has class 2, $[a, b]^q = [a^q, b] = 1$, so $[a, b]$ has order q . Since $[X, X]$ is a cyclic q -group, either $\langle a^q \rangle \leq \langle b^q \rangle$ or $\langle b^q \rangle < \langle a^q \rangle$. Without loss of generality put $a^q = c$, $c \in [X, X]$, and $b^q = c^s$ for some positive integer s . Let $d = a^s b^{-1}$; then $d \notin Z$ (if $d \in Z$, then $ad^{-1} = d^{-1}a$ implies that $[a, b] = 1$). Also

$$d^q = a^{sq} b^{-q} [b^{-1}, a^s]^{q(q-1)/2} = [b^{-1}, a^s]^{q(q-1)/2} = [b^{-1}, a]^{sq(q-1)/2} = [a, b]^{sq(q-1)/2}.$$

Hence $d^{2q} = 1$, $|d| = q$ if $q > 2$, and $d^q \in Z$. Define $N_2 = \langle d, Z \rangle$. Since $[H, H] \leq Z \leq N_2$, N_2 is normal in H . If $q > 2$ or $q = |d| = 2$, then N_2 is noncyclic, and we can take $N = N_2$. If $q = 2$, $|d| = 4$, and N_2 is cyclic, then $|Z| = 2$; in other words H is an extraspecial 2-group. The only extraspecial 2-group without a noncyclic abelian normal subgroup is Q_8 .

(ii) [4, Theorem 1] exhibits the q -groups K such that $\mathbf{C}_K(\Phi(K))$ is cyclic, where $\Phi(K) = K^q[K, K]$ is the Frattini subgroup of K . Here $K = K_0$, or K is a central product $K_0 \vee K_1$, where K_0 is a cyclic group or a 2-group of maximal class (that is, a dihedral or generalised quaternion or semidihedral), and K_1 is extraspecial. However if $K = K_0 \vee K_1$ then $\mathbf{C}_K([K, K])$ contains K_1 and so is noncyclic. □

All of the possibilities for H listed in Proposition 3.5 are metacyclic: each has a cyclic subgroup of index 2. A slightly longer list of groups results if we replace ‘normal’ by ‘characteristic’ in Proposition 3.5; essentially, we must also take central products with

extraspecial groups. The groups of prime power order with every abelian characteristic subgroup cyclic were known to P. Hall (see [16, Satz 13.10, p. 357]).

Proposition 3.5 shows that the strategy in irreducibility and primitivity testing of attempting to construct noncyclic abelian normal subgroups will definitely fail only for a small range of metacyclic nilpotent groups — which includes all the nilpotent primitive groups! Specialised techniques for testing metacyclic nilpotent subgroups of $GL(n, \mathbb{F})$ are developed in Subsection 3.3.

We may fail to construct noncyclic abelian normal subgroups of $G \leq GL(n, \mathbb{F})$ even if they do exist. In this event, we advance the algorithm by constructing another kind of abelian normal subgroup. The next lemma contains the basic idea.

LEMMA 3.7. *Let H be a nilpotent group, with a normal nonabelian subgroup C . Then H has an abelian normal subgroup in C but not in $Z(C)$.*

Proof. Because $H/Z(C)$ is nilpotent with nontrivial normal subgroup $C/Z(C)$, there is a nontrivial cyclic central subgroup $T/Z(C)$ of $H/Z(C)$ in $C/Z(C)$. Thus T is abelian, and it is certainly normal in H . \square

With the extra hypothesis that H/C is cyclic, we can show how to locate abelian normal subgroups of H as in Lemma 3.7. Two preliminary results are required.

LEMMA 3.8. *Let H be a finite nilpotent group of class 2 such that $[H, H]$ is cyclic. Then there is a subset $\{a_i, b_i \mid 1 \leq i \leq k\}$ of H such that*

$$\begin{aligned} [a_i, b_i] &\neq 1, \\ [a_i, a_j] &= [a_i, b_j] = [b_i, b_j] = 1, \end{aligned}$$

for all $i \neq j$, $1 \leq i, j \leq k$, and each element of H has a unique representation in the form

$$a_1^{e_1} b_1^{f_1} \dots a_k^{e_k} b_k^{f_k} z$$

for some $z \in Z(H)$ and $1 \leq e_i, f_i \leq |[a_i, b_i]|$.

Proof. Denote $Z(H)$ by Z . If e is the exponent of the abelian group H/Z , then for some $a \in H$, aZ has order e . The image of φ_a (see Lemma 2.9) is a cyclic group, say of order t . Thus $a^t \in Z$ and e divides t . Also $[a, b]^e = 1$ for all $b \in H$, implying that $t = e$. Hence there exist (non-commuting, so non-central) elements a_1 and b_1 of H such that $[a_1, b_1] = c$ has order e .

Since H has class 2, both $C_H(a_1)$ and $C_H(b_1)$ are normal subgroups of H . Set $C_H(a_1) \cap C_H(b_1) = A_1$. It is not hard to see that $|H : C_H(a_1)| = |H : C_H(b_1)| = e$ and thus

$$|H : A_1| = |H : C_H(a_1) \cap C_H(b_1)| \leq |H : C_H(a_1)| |H : C_H(b_1)| = e^2.$$

On the other hand, the cosets $a_1^{e_1} b_1^{f_1} A_1$ for e_1, f_1 ranging over $\{1, \dots, e\}$ are distinct, for

$$[a_1^{e_1} b_1^{f_1}, b_1] = c^{e_1}, \quad [a_1, a_1^{e_1} b_1^{f_1}] = c^{f_1},$$

and thus $a_1^{e_1} b_1^{f_1} = a_1^{e'_1} b_1^{f'_1}$ modulo A_1 implies that $c^{e_1} = c^{e'_1}$ and $c^{f_1} = c^{f'_1}$; that is, $e_1 = e'_1$ and $f_1 = f'_1$. Thus $|H : A_1| = e^2$ and $H = \langle a_1, b_1, A_1 \rangle$.

If A_1 is abelian, then $A_1 = Z$ and we stop: $k = 1$. Otherwise, we repeat the above with H replaced by A_1 (note that $Z \leq A_1$). Continuing in this fashion, we eventually obtain the desired generating set of H modulo Z . \square

Variations of the next result are used to great effect in work by Suprunenko; see for example [26, Chapter II]. This is also an instance of the famous Hall–Higman theorem [20, 9.3.2, p. 269].

LEMMA 3.9. *Let q be a prime, and let K be a nilpotent group containing a normal q -subgroup H of class 2 such that $[H, H]$ is cyclic and $H/[H, H]$ is elementary abelian. Let $\{a_i, b_i \mid 1 \leq i \leq k\}$ be a generating set of H modulo $Z := Z(H)$, as in Lemma 3.8, so that $\{a_i Z, b_i Z \mid 1 \leq i \leq k\}$ is a basis of the $\text{GF}(q)$ -space H/Z . Then for each $g \in K$ we can use this generating set to construct an element b_g of $H \setminus Z$ such that $[b_g, g] \in Z$.*

Proof. Note that an element b_g as stated surely exists. We must solve an eigenvector problem in H/Z : find exponents ε_i, η_i , not all trivial, such that $0 \leq \varepsilon_i, \eta_i \leq q - 1$ and

$$(ga_1g^{-1})^{\varepsilon_1}(gb_1g^{-1})^{\eta_1} \dots (ga_kg^{-1})^{\varepsilon_k}(gb_kg^{-1})^{\eta_k} = a_1^{\varepsilon_1}b_1^{\eta_1} \dots a_k^{\varepsilon_k}b_k^{\eta_k} \quad (3.1)$$

modulo Z . Say

$$\begin{aligned} ga_i g^{-1} &= a_1^{\alpha_{1i}} b_1^{\beta_{1i}} \dots a_k^{\alpha_{ki}} b_k^{\beta_{ki}} z_i \\ gb_i g^{-1} &= a_1^{\gamma_{1i}} b_1^{\delta_{1i}} \dots a_k^{\gamma_{ki}} b_k^{\delta_{ki}} z'_i \end{aligned}$$

for some $z_i, z'_i \in Z$. Then

$$[ga_i g^{-1}, b_j] = [a_j^{\alpha_{ji}}, b_j] = [a_j, b_j]^{\alpha_{ji}}$$

and

$$[ga_i g^{-1}, a_j] = [b_j^{\beta_{ji}}, a_j] = [b_j, a_j]^{\beta_{ji}}.$$

Since $[H, H]$ is cyclic, we can therefore determine all of the exponents α_{ji}, β_{ji} simply by evaluating commutators. That is, we will find

$$x = a_1^{\tilde{\alpha}_{1i}} b_1^{\tilde{\beta}_{1i}} \dots a_k^{\tilde{\alpha}_{ki}} b_k^{\tilde{\beta}_{ki}} \in H$$

such that $[x, a_j] = [ga_i g^{-1}, a_j]$ and $[x, b_j] = [ga_i g^{-1}, b_j]$ for all j , so that $x^{-1}ga_i g^{-1} \in Z$, and then the uniqueness statement of Lemma 3.8 permits us to equate exponents on x and $ga_i g^{-1}$. In the same way we can determine all γ_{ji}, δ_{ji} . Equation (3.1) then yields a system of linear equations in the ε_i, η_i , which we rearrange into a homogeneous system $Mv = 0$ over $\text{GF}(q)$. Specifically, $v = (\varepsilon_1, \dots, \varepsilon_k, \eta_1, \dots, \eta_k)^T$ and M is the 2×2 block matrix

$$\begin{pmatrix} \alpha - 1_k & \gamma \\ \beta & \delta - 1_k \end{pmatrix}$$

where α, β, γ and δ are the $k \times k$ matrices $(\alpha_{ij}), (\beta_{ij}), (\gamma_{ij})$ and (δ_{ij}) , respectively. Any nonzero solution of this system will provide a suitable element b_g . \square

If $K \leq \text{GL}(n, \mathbb{F})$ then b_g in Lemma 3.9 can be explicitly computed by the method used in the proof of that lemma.

Like all of the results presented so far in this subsection, the next proposition is true not just for linear nilpotent groups, but generally for abstract nilpotent groups. We state it in a form amenable to its application later in the paper.

PROPOSITION 3.10. *Let $G = \langle g, C \rangle$ be nilpotent, where C is a nonabelian normal subgroup of G . Then we can explicitly construct either an abelian normal subgroup of G in C but not in $Z(C)$, or a noncyclic abelian normal subgroup of G .*

Proof. Given the normal closure in C of a subgroup H , we find the normal closure in G of H directly as follows. Let $\{1, g, \dots, g^l\}$ be a transversal for the cosets of C in G . If we know a generating set $\{h_1, \dots, h_s\}$ for H^C , then

$$H^G = \langle g^j h_i g^{-j} : 1 \leq i \leq s, 0 \leq j \leq l \rangle.$$

Find $a \in Z_2(C) \setminus Z(C)$ by `SecondCentralElement`(G, C). The normal closure `NoncentralAbelian`(C, a) of $\langle a \rangle$ in C is contained in $Z_2(C)$. Let $A = \langle a \rangle^G$. Of course, $A \leq Z_2(C)$ and $A \not\leq Z(C)$. If A is abelian, then we are done.

Suppose that A is nonabelian, and hence class-2 nilpotent. We may assume that A is a q -group. Since A has class 2, a generating set for the abelian normal subgroup $[A, A]$ of G is easily written down as the set of commutators of pairs of generators of A . If $[A, A]$ is noncyclic then we are done, so let $[A, A]$ be cyclic. We have generators for the nontrivial group $A/[A, A]$, and can do membership testing in $[A, A]$ because it is cyclic, so we can find the noncyclic normal subgroup B of G in A such that $\Omega_1(A/[A, A]) = B/[A, A]$. If B is abelian, then we stop; otherwise by Lemma 3.9 we determine $b \in B \setminus Z(B)$ with $[b, g] \in Z(B)$. Since b is not in $Z(B)$, it cannot be in $Z(C)$.

Consider $D = \langle b \rangle^G \leq B$. Now $\langle b \rangle^C = \langle b, b_1, \dots, b_s \rangle$ for some $b_i \in Z(B)$. Hence

$$D = \langle g^j b g^{-j}, g^j b_i g^{-j} : 1 \leq i \leq s, 0 \leq j \leq l \rangle.$$

Every $g^j b_i g^{-j}$ is central in B , and because $[b, g] \in Z(B)$ implies that $g^j b g^{-j} \in bZ(B)$, every $g^j b g^{-j}$ commutes with every $g^k b g^{-k}$. That is, D is an abelian normal subgroup of G in C but not in $Z(C)$. \square

We give a name to the algorithm described in the proof of Proposition 3.10, which features significantly in the final irreducibility/primitivity testing algorithm.

Algorithm 4: `GoodAbelianNormal`(G)

Input: $G = \langle g, C \rangle \leq \text{GL}(n, \mathbb{F})$ nilpotent, $C \trianglelefteq G$ nonabelian.

Output: an abelian normal subgroup N of G , where N is noncyclic, or $N \leq C$ and $N \not\leq Z(C)$, constructed by the proof of Proposition 3.10.

A central task in Algorithm 4 is finding the element b , which in turn depends on computing the generating set in Lemma 3.8. To end this subsection, we discuss a possible way in which that computation can be substantially reduced.

Retain the notation and assumptions of Lemma 3.8, and suppose that H is a q -group for some prime q . Let $H = \langle h_1, \dots, h_s \rangle$. Then the Frattini subgroup $\Phi(H)$ of H is

$$\langle [h_i, h_j], h_i^q : 1 \leq i, j \leq s \rangle.$$

If $\Phi(H)$ is nonabelian, then we are unable to proceed further. However, if $\Phi(H)$ is abelian, then either it is noncyclic, and thus a noncyclic abelian normal subgroup of any group in which H is normal, or $\Phi(H)$ is cyclic. The isomorphism types of q -groups H such that $\Phi(H)$ is cyclic are given in [4, Theorem 2]. For example, if q is odd, then the possibilities for H are the nonabelian groups $E \times (G_0 \wr D)$ where E is elementary abelian, G_0 is cyclic or nonabelian with a cyclic maximal subgroup (see [20, 5.3.4, p. 141]), and D is 1 or an extraspecial group of exponent q . We focus on the case that H is extraspecial.

LEMMA 3.11. *Let H be an extraspecial q -group. If K is any nonabelian subgroup of H of order q^3 , then K is normal in H , and $H = KC_H(K)$.*

COROLLARY 3.12. *Let H be an extraspecial q -group of order q^{2k+1} , $k \geq 1$. Then we may construct a generating set $\{a_i, b_i \mid 1 \leq i \leq k\}$ of H such that*

$$\begin{aligned} Z(H) &= \langle [a_i, b_i] \rangle, \\ [a_i, a_j] &= [a_i, b_j] = [b_i, b_j] = 1, \end{aligned}$$

for all i and $j \neq i$.

Proof. We describe the first stages in a much simplified version of the recursive method used in the proof of Lemma 3.8.

Choose non-commuting generators a_1, b_1 of H ; then $H_1 = \langle a_1, b_1 \rangle$ is extraspecial of order q^3 . Let d be any other generator of H . By Lemma 3.11, $d = a_1^i b_1^j c$ for some $c \in C_H(H_1)$. Then i, j can be found directly because $Z(H) = \langle [a_1, b_1] \rangle$, $[a_1, d] = [a_1, b_1]^j$, and $[b_1, d] = [a_1, b_1]^{-i}$. We thereby obtain a generating set for $C \leq C_H(H_1)$ such that $H = H_1 C$, from which it follows that $C_H(H_1) = C$. If $C_H(H_1)$ is abelian, then $H = H_1$ and we are done. Otherwise, we replace H by the extraspecial group $C_H(H_1)$ and repeat the above. \square

3.3. Nilpotent metacyclic groups

This subsection is devoted to testing irreducibility and primitivity of nilpotent metacyclic subgroups $G = \langle g, A \rangle$ of $\text{GL}(n, \mathbb{F})$, where A is cyclic and a maximal abelian normal subgroup of G ; that is, $C_G(A) = A \neq G$. We further assume $\langle A \rangle_{\mathbb{F}}$ to be a field, so that the irreducible parts of A are pairwise equivalent. Any nilpotent primitive subgroup of $\text{GL}(n, \mathbb{F})$ is a metacyclic group of this form.

Note that $[G, G] \leq A$ is cyclic and $A \leq X := C_G([G, G])$. Either X is cyclic ($X = A$) or X is nonabelian ($X \neq A$). The Sylow q -subgroup X_q of X is $C_{G_q}([G_q, G_q])$.

LEMMA 3.13. (i) *If $G_{2'}$ is nonabelian, then G contains a noncyclic abelian normal subgroup.*

(ii) *Suppose that $G_{2'}$ is abelian. If X_2 is cyclic, or X_2 is noncyclic and $G_2 \cong Q_8$, then $|G : A| = 2$; otherwise, G contains a noncyclic abelian normal subgroup.*

Proof. (i) Let $G_q \leq G_{2'}$ be nonabelian. Since $[G_q, G_q]$ is cyclic, and X_q is noncyclic by Lemma 3.6(ii), we have by Lemma 3.6(i) that G_q contains a noncyclic abelian normal subgroup.

(ii) Here $G_{2'} \leq Z(G)$ and so $G_{2'} \leq A$. If X_2 is cyclic, then G_2 has an abelian subgroup of index 2 by Lemma 3.6(ii), and thus $|G : A| = 2$. Suppose that X_2 is noncyclic. If $G_2 \not\cong Q_8$, then G has a noncyclic abelian normal subgroup by Lemma 3.6(i). If $G_2 \cong Q_8$, then $G/A \cong G_2/(A \cap G_2)$ is a cyclic quotient of Q_8 , implying that $|G : A| = 2$. \square

Since G is metacyclic, X is very easy to calculate. If $\{1, g, \dots, g^{k-1}\}$ is a transversal for the cosets of A in G , and $A = \langle a \rangle$, then $[G, G] = \langle g^i [g, a] g^{-i} : 0 \leq i \leq k-1 \rangle$. Therefore $X = \langle g^j, a \rangle$ where j is the least integer in the range $1, \dots, k$ such that g^j commutes with $[g, a]$. (When we call on this subsection in the final algorithm in Subsection 3.4, k will divide n .) So we have an explicit generating set for X , and the proof of Lemma 3.6(i) gives instructions for calculating a noncyclic abelian normal subgroup of G as in Lemma 3.13. We label this procedure.

Algorithm 5: NoncyclicAbelian(G)

Input: $G = \langle g, A \rangle$ nilpotent, A maximal abelian normal in G , $\langle A \rangle_{\mathbb{F}}$ a field. Further, either G_2 is nonabelian, or $C_{G_2}([G_2, G_2])$ is noncyclic and $G_2 \not\cong Q_8$.

Output: an abelian noncyclic normal subgroup B of G , constructed by the method in the proof of Lemma 3.6(i) and the method for calculating $C_G([G, G])$ above.

For the rest of this subsection $|G : A| = 2$, $G = G_2 \times C$ where $C = G_2' \leq Z(G)$ is cyclic, $g \in G_2$, and $A = (A \cap G_2) \times C$. Under these assumptions, the characteristic p of \mathbb{F} must be odd: a completely reducible 2-subgroup of $\text{GL}(n, \mathbb{F})$ is trivial if $p = 2$.

Denote the field $\langle A \rangle_{\mathbb{F}}$ by Δ .

LEMMA 3.14. G is irreducible if and only if A is irreducible.

Proof. Suppose that A is reducible, with nonzero module $U \neq V$. By Lemma 3.2(i), $U \cong gU$ as A -modules. As $U + gU$ is a G -submodule of V , and obviously G is reducible if $U + gU \neq V$, we suppose that $V = U + gU$. Then $V = U \oplus gU$ and $\{U, gU\}$ is a G -system of imprimitivity (of no help to us in testing irreducibility of G , since it is made up of a single homogeneous component for the normal subgroup A). With respect to the basis afforded by U and gU ,

$$g = \begin{pmatrix} 0_m & g_1 \\ g_2 & 0_m \end{pmatrix}$$

for some $g_1, g_2 \in \text{GL}(m, \mathbb{F})$, and $A = \langle \text{diag}(a, a) \rangle$ where $\langle a \rangle := A_1$ is an irreducible cyclic subgroup of $\text{GL}(m, \mathbb{F})$. The relation $g^2 \in A$ implies that $g_1 g_2 = g_2 g_1 \in A_1$. Since g normalises A , it follows that $g_1 \in \text{N}_{\text{GL}(m, \mathbb{F})}(A_1)$ and $g_1^2 \in \text{C}_{\text{GL}(m, \mathbb{F})}(A_1) = \langle A_1 \rangle_{\mathbb{F}}^{\times}$. However $g_1 \notin \text{C}_{\text{GL}(m, \mathbb{F})}(A_1) = A_1$, for if g_1 centralised A_1 then g would centralise A . In particular, $n > 2$. Conjugation by g defines an element of $\text{Gal}(\Delta/\mathbb{F})$ of order 2, so the order m of this Galois group is even.

Replace G by G_2 . Since G is a nonabelian 2-group with a cyclic subgroup A of index 2, by [20, 5.3.4, p. 141] either G is generalised quaternion, or G splits over A . Thus we may suppose that $g^2 = \pm 1_n$ and so $g_2 = \pm g_1^{-1}$.

We claim that there exist $\xi_1, \xi_2 \in \langle A_1 \rangle_{\mathbb{F}}^{\times}$ such that $\xi_1 g_1^{-1} \xi_1 g_1^{-1} = 1_m$ and $\xi_2 g_1^{-1} \xi_2 g_1^{-1} = -1_m$. Conjugating G by

$$\begin{pmatrix} 1_m & -\xi \\ \xi^{-1} & 1_m \end{pmatrix} \tag{3.2}$$

where $\xi = \xi_1$ or $\xi = \xi_2$ then produces a visibly reducible group. To verify the claims, first note that conjugation by g_1 is a Galois automorphism σ of $\langle A_1 \rangle_{\mathbb{F}}/\mathbb{F}$ of order 2. Since $\alpha := g_1^2$ is σ -invariant, α is in the image of the norm map of the Galois extension $\langle A_1 \rangle_{\mathbb{F}}/\mathbb{E}$, where \mathbb{E} is the σ -invariant subfield; that is, $\alpha = \xi \sigma(\xi)$ for some $\xi \in \langle A_1 \rangle_{\mathbb{F}}$. Then

$$\alpha \xi g_1^{-1} \xi g_1^{-1} = \xi g_1 \xi g_1^{-1} = \xi \sigma(\xi) = \alpha$$

so $\xi g_1^{-1} \xi g_1^{-1} = 1_m$. The same reasoning goes through after changing α to $-\alpha$. □

We define a procedure `ModulesMetacyclic(G)` for determining G -modules when A (and thus G) is reducible. These are available from irreducible modules U for the cyclic

group A : either $U + gU < V$ is a G -module (which must be true if n is not divisible by 4), or xU is a G -module where x is the product of (3.2) and the change-of-basis matrix afforded by $\{U, gU\}$.

Lemma 3.14 warrants yet another reduction: A can be assumed irreducible, so that G is irreducible, and we are left to test primitivity of G .

We now re-state some material from [8]. Given that A is irreducible, then n is even, say $n = 2m$, and the $\text{Mat}(n, \mathbb{F})$ -centraliser of G is the field extension $\mathbb{K} = \{x \in \Delta \mid xg = gx\}$ of degree m over \mathbb{F} (\mathbb{K} is the subfield of Δ invariant under the Galois automorphism induced by conjugation action of g). There is a field $\mathbb{K}_1 \cong \mathbb{K}$ and a \mathbb{K} -algebra isomorphism ϕ from $C_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ onto $\text{Mat}(2, \mathbb{K}_1)$ such that $\phi(C)$ is scalar and $\phi(G_2)$ is an absolutely irreducible subgroup of $\text{GL}(2, \mathbb{K}_1)$ (cf. Lemma 2.11). The map ϕ has a particularly simple description: each element g of G is a 2×2 block matrix over the field \mathbb{K}_1 ; moreover, as a 2×2 matrix over \mathbb{K}_1 , g is invertible; ϕ then merely identifies $g \in \text{GL}(m, \mathbb{F})$ with $g \in \text{GL}(2, \mathbb{K}_1)$.

The next suite of results comes from [8, Sections 3 and 4].

LEMMA 3.15. *If G is primitive, then $\phi(G_2)$ is primitive, m is odd, $\mathbb{K} = \langle C \rangle_{\mathbb{F}}$, and \mathbb{K}^\times does not contain an element of order 4. If $\phi(G_2)$ is primitive, then $C = \langle \text{diag}(x, x) \rangle$ up to conjugacy, where $C_1 := \langle x \rangle \leq \text{GL}(m, \mathbb{F})$ is irreducible.*

LEMMA 3.16. *Suppose that $\phi(G_2)$ is primitive. Define $d = \text{diag}(1_m, -1_m)$ and $d' = \begin{pmatrix} \alpha & \\ & -\beta \end{pmatrix}$ where $\alpha, \beta \in \langle C_1 \rangle_{\mathbb{F}}$, $\alpha^2 + \beta^2 = -1_m$. Then G is Δ^\times -conjugate either to $\langle A, d \rangle$ or to $\langle A, d' \rangle$, where A consists of matrices of the form $\begin{pmatrix} & \nu \\ -\mu & \end{pmatrix}$, $\mu, \nu \in \langle C_1 \rangle_{\mathbb{F}} = \mathbb{K}_1$.*

THEOREM 3.17. *G is primitive if and only if $C_1 \leq \text{GL}(m, \mathbb{F})$ and $\phi(G_2) \leq \text{GL}(2, \mathbb{K}_1)$ are primitive.*

Theorem 3.17 equates primitivity testing of G with a pair of much easier problems: testing primitivity of abelian linear groups (for which see Subsection 3.1), and testing primitivity of 2-dimensional linear groups. Suppose that G is imprimitive because $\phi(G_2)$ is imprimitive; for $|G_2| > 8$ this happens if and only if $\phi(A_2)$ is reducible. Since $\phi(G_2)$ is monomial, the one-dimensional components of a $\phi(G_2)$ -system of imprimitivity are m -dimensional \mathbb{F} -subspaces of V permuted by G . So we have a G -system of imprimitivity once we have a $\phi(G_2)$ -system of imprimitivity. Next we show how to construct an imprimitivity system for G from one for C_1 .

LEMMA 3.18. *Let $\phi(G_2)$ be primitive, and let $V = V_1 \oplus V_2$ where $C_{V_1} = C_{V_2} = C_1 = \langle x \rangle$ is an irreducible subgroup of $\text{GL}(m, \mathbb{F})$. Let $\{U_1, \dots, U_k\}$ be a system of imprimitivity for C_1 in V_1 , and $\{U'_1, \dots, U'_k\}$ be a corresponding system of imprimitivity for C_1 in V_2 . Define $W_i = U_i \oplus U'_i$ and $\mathcal{L} = \{W_1, \dots, W_k\}$. Then for some $h \in \text{GL}(n, \mathbb{F})$, \mathcal{L} is a hGh^{-1} -system of imprimitivity.*

Proof. We assume that G is of the form $\langle A, d \rangle$ or $\langle A, d' \rangle$, as in Lemma 3.16. In particular, $A = A_2 \times C$, $I_m \leq A_2$, and $A_2 \subset \Delta = \langle I_m \rangle_{\mathbb{K}}$, where $I_m = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m \end{pmatrix}$. Clearly, \mathcal{L} is a C -system of imprimitivity. We will show that G_2 stabilises each W_i , and hence that \mathcal{L} is a system of imprimitivity for G .

Set $|\mathbb{F}| = q$. The enveloping algebra $\tilde{\Delta} = \langle I_m \rangle_{\mathbb{F}}$ is a subfield of Δ , of size q^2 . Since Δ^\times is cyclic of order $q^{2m} - 1 = (q^m - 1)(q^m + 1)$, $q \equiv 3 \pmod{4}$, and m is odd, the Sylow 2-subgroup of Δ^\times is contained in $\tilde{\Delta}^\times$, so $A_2 \subset \tilde{\Delta}$. Then $\tilde{\Delta}W_i = W_i$ implies that \mathcal{L} is an A -system of imprimitivity.

Now $dW_i = W_i$ for all i , and we may choose α, β in the definition of d' to be elements of the ground field \mathbb{F}_{1_m} . Hence

$$d'W_i = \text{diag}(\alpha, \alpha)dW_i + \text{diag}(\beta, \beta) \begin{pmatrix} 0_m & 1_m \\ 1_m & 0_m \end{pmatrix} W_i \subseteq W_i,$$

completing the proof. \square

Finally, we propose an algorithm for irreducibility/primitivity testing of nilpotent metacyclic subgroups of $\text{GL}(n, \mathbb{F})$. Remember that if a subgroup H of $\text{GL}(n, \mathbb{F})$ has noncyclic abelian normal subgroups, then we conclude either that H is reducible with known H -submodules of V , or H is imprimitive with a known imprimitivity system and we continue irreducibility testing of H via Theorem 3.1.

Algorithm 6: IrredPrimMetacyclic(G)

Input: $G = \langle g, A \rangle \leq \text{GL}(n, \mathbb{F})$ nilpotent, A a maximal abelian normal subgroup of G , $\langle A \rangle_{\mathbb{F}}$ a field.

1. Calculate G_2 and $G_{2'}$.
 2. If $G_{2'}$ is nonabelian, then by Lemma 3.13 construct $\text{NoncyclicAbelian}(G) \leq G_{2'}$. Else go to the next step.
 3. Let $G_{2'}$ be abelian. By Lemma 3.13, if $\text{C}_{G_2}([G_2, G_2])$ is noncyclic and $G_2 \not\cong Q_8$, then construct $\text{NoncyclicAbelian}(G) \leq G_2$; else $|G : A| = 2$ and we go to the next step.
 4. Let $|G : A| = 2$, $G_{2'}$ cyclic. If A is reducible, then by Lemma 3.14 so too is G , and $\text{ModulesMetacyclic}(G)$ provides modules for G . Else go to the next step.
 5. Let A be irreducible. If $\phi(G_2)$ is imprimitive, where $\phi : G \rightarrow \text{GL}(2, \langle G_{2'} \rangle_{\mathbb{F}})$ is the injection described before Lemma 3.15, then G is irreducible imprimitive, and a $\phi(G_2)$ -system of imprimitivity is simultaneously a G -system of imprimitivity. Else go to the next step.
 6. Let $\phi(G_2)$ be primitive. If C_1 is imprimitive, then G is irreducible with explicit imprimitivity system per Lemma 3.18. Else the algorithm terminates, reporting that G is primitive, by Theorem 3.17.
-

At the termination of Algorithm 6, either we have found an imprimitivity system for irreducibility testing in a degree strictly dividing n , or we have found that G is reducible, or primitive, or irreducible imprimitive, with explicitly constructed modules or imprimitivity system.

3.4. An algorithm testing irreducibility and primitivity of nilpotent linear groups

Let G be a nilpotent subgroup of $\text{GL}(n, \mathbb{F})$, generated by semisimple matrices. Our algorithm for irreducibility and primitivity testing of G is based on what are by now very familiar notions: repeatedly constructing noncyclic abelian normal subgroups of G (to decrease the dimension of subspaces under consideration), or constructing proper abelian normal overgroups in G of abelian normal subgroups of G (to decrease the size of the factor group in question). Eventually G must be reported imprimitive or reducible, or the process will encounter a metacyclic group, for which irreducibility and primitivity testing can be

carried out separately as in Subsection 3.3.

The next two fairly trivial lemmas underpin the operation of the entire algorithm (Lemma 3.20 recalls comments in the proof of Proposition 3.10).

LEMMA 3.19. *Let H be a nilpotent group. If $K \leq Z_2(H)$, then K^H has nilpotency class at most 2.*

LEMMA 3.20. *If $A = \langle a_1, \dots, a_s \rangle$ is a normal subgroup of H , where H is normal in G and $G = \langle g, H \rangle$, $|G : H| = k$, then*

$$A^G = \langle g^j a_i g^{-j} : 1 \leq i \leq s, 0 \leq j \leq k-1 \rangle.$$

Now we present the final irreducibility/primitivity testing algorithm.

Algorithm 7: IrredPrimNilpotent(G)

Input: $G = \langle g_1, \dots, g_r \rangle \leq \text{GL}(n, \mathbb{F})$ nilpotent, g_i semisimple.

Output: proper nonzero G -submodules of V , or a G -system of imprimitivity, or a report that G is primitive.

- (I) If G is abelian, then test irreducibility and primitivity as in Subsection 3.1. Else go to step (II).
- (II) Find a noncentral element $a_1 := \text{SecondCentralElement}(G, G)$ of G in $Z_2(G)$, and let $A_1 := \text{NoncentralAbelian}(G, a_1) = \langle a_1, E_{a_1} \rangle$ be the normal closure of $\langle a_1 \rangle$ in G , where $E_{a_1} = \langle [g_i, a_1] : 1 \leq i \leq r \rangle$.
 1. Construct a decomposition of V into a direct sum of simple A_1 -modules, via $\text{Cutting}(\langle A_1 \rangle_{\mathbb{F}})$. Since $A_1 \trianglelefteq G$, this is either a decomposition into G -modules, or a G -system of imprimitivity on which G acts transitively. If there is a single summand, then $\langle A_1 \rangle_{\mathbb{F}}$ is a field; otherwise we have proper nonzero G -submodules of V , or we have a G -system of imprimitivity, and then continue irreducibility testing of G using Theorem 3.1.
 2. Suppose that $\langle A_1 \rangle_{\mathbb{F}}$ is a field. Let $g_{a_1} := \text{GaloisGenerator}(G, A_1)$ and $C_G(A_1) := \text{Centraliser}(G, A_1)$, so $G = \langle g_{a_1}, C_G(A_1) \rangle$, and $|G : C_G(A_1)|$ divides n . If $A_1 = C_G(A_1)$ then invoke $\text{IrredPrimMetacyclic}(G)$. Else go to (III).
- (III) Set $C = C_G(A_1)$. Find $\text{SecondCentralElement}(G, C) = a_2 \in Z_2(C) \setminus Z(C)$ and determine the normal closure $\text{NoncentralAbelian}(C, a_2) = \langle a_2, E_{a_2} \rangle$ of $\langle a_2 \rangle$ in C . Then let \hat{A}_2 be the normal closure of $A_2 = \langle A_1, a_2, E_{a_2} \rangle$ in G (Lemma 3.20). By Lemma 3.19, \hat{A}_2 is either abelian or class-2 nilpotent.
 1. If \hat{A}_2 is abelian, then replace A_1 by \hat{A}_2 and go to (II) part (1). Note that $\langle \hat{A}_2 \rangle_{\mathbb{F}}$ properly contains $\langle A_1 \rangle_{\mathbb{F}}$, because $\hat{A}_2 \not\leq Z(C)$.
 2. Suppose that \hat{A}_2 is class-2 nilpotent. $\text{GoodAbelianNormal}(G)$ returns either: (a) a noncyclic abelian normal subgroup of G , or (b) an abelian normal subgroup B of G in C but not in $Z(C)$. In case (a), G is imprimitive and irreducibility testing of G goes down to a degree strictly dividing n . In case (b), we replace A_1 by the abelian normal subgroup $\langle B, A_1 \rangle$ of G , a proper overgroup of A_1 , and go to (II), part (1).

Algorithm 7 terminates in no more than n loops back to (II) part (1) from (III), since each recursion necessitates adding to a tower of fields in $\text{Mat}(n, \mathbb{F})$, each properly containing the other (cf. Lemma 2.20).

Reduction to smaller dimensions for irreducibility testing possibly occurs in (II) part (1) and (III) part (2) of Algorithm 7, as well as in (II) part (2), when Algorithm 6 (`IrredPrimMetacyclic`) may be called. This reduction can occur no more than $\log_2 n$ times over the course of the entire algorithm.

Algorithm 7 shares many of its basic computational ingredients with the nilpotency testing algorithm `IsNilpotent` of Subsection 2.4 (Algorithm 3). Just as in `IsNilpotent`, the construction of abelian normal subgroups is based on computing sets of elements whose sizes depend polynomially on n , $|\mathbb{F}|$, and nilpotency class of input. The procedure `GoodAbelianNormal` (Algorithm 4) involves a recursion that terminates in no more than n^2 rounds, but otherwise consists of linear algebra and pre-ordained group operations. (The longest chain of operations occurs when calculating D in the proof of Proposition 3.10: in this calculation there are one inversion and $O(sn^2)$ multiplications, where s is the size of a generating set for C ; see after Proposition 2.22 for remarks about polynomial growth in the size of such generating sets.) Also note that in part (2) of step (II), the field arithmetic in `GaloisGenerator` (see the end of Subsection 2.2) replaces the more complicated method of finding a transversal for the cosets of $C_G(A_1)$ outlined after Corollary 2.18. Other functions have been analysed earlier as part of `IsNilpotent` (Algorithm 3).

In steps (5) and (6) of `IrredPrimMetacyclic` (Algorithm 6) we should perform primitivity testing on linear groups that are abelian or of degree 2. In fact, as indicated after Theorem 3.17, the degree-2 case is also concerned mainly with testing abelian groups, which by Subsection 2.3 amounts to manipulations with the cutting procedure and cyclic groups of known order. Algorithm 5 (`NoncyclicAbelian`), at the point of its application within (II) part (2) of Algorithm 7, is just group operations, the number of which is no worse than $O(n^2)$.

In some parts of Algorithm 7, algorithms for permutation groups are needed, such as algorithms to calculate orbits and point stabilisers. Those algorithms are available in [24], and are polynomial-time in the permutation degree (always a divisor of n) and input size; see [24, pp. 48–49].

4. Permutation representation of nilpotent matrix groups

This very brief final section is about the link between nilpotent linear groups and permutation groups, which can yield permutation representations of nilpotent linear groups of much smaller degree than the exponential-degree representations arising from action on the underlying space.

Let G be nilpotent and completely reducible. It is a consequence of [27, §27, Lemma 6] that G is monomial over the algebraic closure of \mathbb{F} , and thus over some finite extension of \mathbb{F} . In the irreducible case we have a familiar bound on the degree of the extension.

PROPOSITION 4.1. *If the nilpotent subgroup G of $\text{GL}(n, \mathbb{F})$ is irreducible, then G is monomial over an extension \mathbb{E} of \mathbb{F} such that $|\mathbb{E} : \mathbb{F}|$ divides n .*

Proof. First suppose that G is absolutely irreducible, and hence nonabelian. If G is primitive, then $n = 2$ and G has an irreducible abelian normal subgroup of index 2, which can be diagonalised over the degree-2 extension of \mathbb{F} . But then G is monomial over that extension.

Suppose now that G is imprimitive. If n is odd, then G is monomial over \mathbb{F} by [8, Theorem 5.3]; otherwise, by [27, §15, Theorem 4], G is conjugate to a subgroup of a wreath product $H \wr T$ where $H \leq \text{GL}(2, \mathbb{F})$ is nilpotent absolutely irreducible primitive and T is a nilpotent transitive subgroup of $\text{Sym}(n/2)$. Since H is monomial over the degree-2 extension of \mathbb{F} , the proposition is proved in this case.

Now let G be irreducible but not absolutely irreducible. For some extension \mathbb{E} of \mathbb{F} of degree m dividing n , G is $\text{GL}(n, \mathbb{E})$ -conjugate to a group of block-diagonal matrices, where each block is absolutely irreducible in $\text{GL}(n/m, \mathbb{E})$ (see, for example, [10, Theorem 2.10B, pp. 41–42]). Now we get the result from the previous paragraph. \square

We can attempt to find a monomial representation of nonabelian G as follows.

1. Find $a = \text{SecondCentralElement}(G, G)$.
2. Let $A = \text{NoncentralAbelian}(G, a)$.
3. If $\langle A \rangle_{\mathbb{F}}$ is a field, then find $x^{-1}Ax = \langle \text{diag}(a_1, \dots, a_n) \rangle$; otherwise construct simple $\langle A \rangle_{\mathbb{F}}$ -modules.

If in step (3) the a_i are distinct (as happens when A is irreducible), then $x^{-1}Gx$ is monomial over the smallest field containing the a_i s (which is the degree- n extension of \mathbb{F} when A is irreducible).

If we apply the above procedure to any subgroup G of $\text{GL}(n, \mathbb{F})$, then either we obtain a monomial representation of G — and hence a permutation representation $\tau : G \rightarrow \text{Sym}(n)$ with abelian kernel — or we discover that G is not nilpotent. In the former case we can test nilpotency of $\tau(G)$ using well-established algorithms for permutation groups. If $\tau(G)$ is nilpotent, then, knowing the primary decompositions of $\ker \tau$ and $\tau(G)$, we can test nilpotency of G as in Lemma 2.23.

Acknowledgment This publication has emanated from research conducted with the financial support of Science Foundation Ireland.

References

1. LÁSZLÓ BABAI, ROBERT BEALS, JIN YI CAI, GÁBOR IVANYOS and EUGENE M. LUKS, ‘Multiplicative equations over commuting matrices’, *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, Atlanta, GA, 1996 (ACM, New York, 1996) 498–507. 108
2. R. BEALS, ‘Towards polynomial time algorithms for matrix groups’, *DIMACS II*, Series in Discrete Mathematics and Theoretical Computer Science 28 (Amer. Math. Soc., Providence, RI, 1997) 31–54. 104
3. R. BEALS, ‘Algorithms for matrix groups and the Tits alternative’, *J. Comput. System Sci.* 58 (1999) 260–279. 104
4. T. R. BERGER, L. G. KOVÁCS and M. F. NEWMAN, ‘Groups of prime power order with cyclic Frattini subgroup’, *Nederl. Akad. Wetensch. Indag. Math.* 42 (1980) 13–18. 122, 125
5. A. BIALOSTOCKI, ‘The nilpotency class of the p -Sylow subgroups of $\text{GL}(n, q)$ where $(p, q) = 1$ ’, *Canadian Math. Bull.* 29 (1986) 218–223. 110
6. F. CELLER and C. R. LEEDHAM-GREEN, ‘Calculating the order of an invertible matrix’, *DIMACS II*, Series in Discrete Mathematics and Theoretical Computer Science 28 (Amer. Math. Soc., Providence, RI, 1997) 55–60. 108, 118

7. G. COOPERMAN and L. FINKELSTEIN, 'Combinatorial tools for computational group theory', *DIMACS II*, Series in Discrete Mathematics and Theoretical Computer Science 11 (Amer. Math. Soc., Providence, RI, 1993) 31–54. 104
8. A. S. DETINKO and D. L. FLANNERY, 'Classification of nilpotent primitive linear groups over finite fields', *Glasgow Math. J.* 46 (2004) 585–594. 105, 118, 128, 132
9. A. S. DETINKO and D. L. FLANNERY, 'Nilpotent primitive linear groups over finite fields', *Comm. Algebra* 33 (2005) 1–9. 105, 118, 121
10. JOHN D. DIXON, *The structure of linear groups* (Van Nostrand Reinhold, London, 1971). 132
11. B. EICK and G. OSTHEIMER, 'On the orbit-stabilizer problem for integral matrix actions of polycyclic groups', *Math. Comp.* 72 (2003) 1511–1529. 105
12. DEREK F. HOLT, BETTINA EICK and EAMONN A. O'BRIEN, *Handbook of computational group theory* (Chapman & Hall/CRC Press, Boca Raton/London/New York/Washington, 2005). 105, 112, 116, 118
13. D. HOLT, C. R. LEEDHAM-GREEN, E. A. O'BRIEN and S. REES, 'Computing matrix group decompositions with respect to a normal subgroup', *J. Algebra* 184 (1996) 818–838. 105
14. D. HOLT, C. R. LEEDHAM-GREEN, E. A. O'BRIEN and S. REES, 'Testing matrix groups for primitivity', *J. Algebra* 184 (1996) 795–817. 105
15. D. HOLT and S. REES, 'Testing modules for irreducibility', *J. Austral. Math. Soc. Ser. A* 57 (1994) 1–16. 105
16. B. HUPPERT, *Endliche gruppen I* (Springer, Berlin, 1967). 122, 123
17. E. LO, 'Finding intersections and normalisers in finitely generated nilpotent groups', *J. Symbolic Comput.* 25 (1998) 45–59. 105
18. E. LUKS, 'Computing in solvable matrix groups', *Proc. 33rd IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Washington, DC, 1992) 111–120. 104, 109, 110, 112, 115, 117, 118
19. G. OSTHEIMER, 'Practical algorithms for polycyclic matrix groups', *J. Symbolic Comput.* 28 (1999) 361–379. 105
20. DEREK J. S. ROBINSON, *A course in the theory of groups*, Graduate Texts in Mathematics 80 (Springer, New York, 1996). 107, 119, 122, 124, 125, 127
21. L. RÓNYAI, *Computations in associative algebras*, DIMACS Series in Discrete Mathematics 11 (Amer. Math. Soc., Providence, RI, 1993) 221–243. 105, 111, 112, 118
22. D. SEGAL, *Polycyclic groups* (Cambridge University Press, Cambridge, 1983). 108
23. Á. SERESS, 'An introduction to computational group theory', *Notices Amer. Math. Soc.* 44 (1997) 671–679. 104, 111, 113
24. Á. SERESS, *Permutation group algorithms* (Cambridge University Press, Cambridge, 2003). 131
25. C. C. SIMS, *Computation with finitely presented groups*, Encyclopedia of Math. Appl. 48 (Cambridge University Press, New York, 1994). 105, 116
26. D. A. SUPRUNENKO, *Soluble and nilpotent linear groups*, Transl. Math. Monogr. 9 (Amer. Math. Soc., Providence, RI, 1963). 105, 111, 124

27. D. A. SUPRUNENKO, *Matrix groups*, Transl. Math. Monogr. 45 (Amer. Math. Soc., Providence, RI, 1976). 105, 108, 109, 121, 131, 132
28. B. A. F. WEHRFRITZ, *Infinite linear groups* (Springer, Berlin/Heidelberg/New York, 1973). 110

A. S. Detinko alla.detinko@nuigalway.ie

D. L. Flannery dane.flannery@nuigalway.ie

Department of Mathematics
National University of Ireland, Galway
Ireland