

CLASSIFICATION OF NILPOTENT PRIMITIVE LINEAR GROUPS OVER FINITE FIELDS

A. S. DETINKO

Department of Applied Mathematics, Polotsk State University, Novopolotsk, Belarus
e-mail: detinko@yahoo.com

and D. L. FLANNERY

Department of Mathematics, National University of Ireland, Galway, Ireland
e-mail: dane.flannery@nuigalway.ie

(Received 28 November, 2003; accepted 22 January, 2004)

Abstract. We present a classification of the nilpotent primitive subgroups of $GL(n, q)$, up to conjugacy in $GL(n, q)$. Groups in the classification are specified explicitly by generating sets of matrices, where each generating set has size at most 2. Additionally we give an algorithm designed to provide electronic access to the classification for any n and q .

2000 *Mathematics Subject Classification.* 20H30.

1. Introduction. This paper is a successor to [2]; it generalises and strengthens results therein. Our aim here is to classify, up to conjugacy, the nilpotent primitive (irreducible) subgroups of $GL(n, \mathbb{F})$, where \mathbb{F} is a finite field of size q and characteristic p .

Nilpotent linear groups have been studied for a long time. The first systematic investigation of such groups was undertaken in the late 1940s by D. A. Suprunenko, who introduced basic techniques, particularly efficient for groups over an algebraically closed field \mathbb{E} (see [7, Chapter III]). In this case many structural results were obtained, as well as a complete classification of maximal locally nilpotent subgroups of $GL(n, \mathbb{E})$ (if the characteristic of \mathbb{E} does not divide n then such subgroups are unique up to conjugacy; otherwise, nilpotent irreducible subgroups of $GL(n, \mathbb{E})$ do not exist). Subsequent efforts by other authors were concentrated on extending Suprunenko's work to other fields. In [9, 10], methods from [7] were applied to the case of nilpotent irreducible groups over finite fields. But that approach turns out to be not very efficient. One reason for this is that if \mathbb{E} is algebraically closed then there are no nilpotent primitive subgroups of $GL(n, \mathbb{E})$: each nilpotent irreducible subgroup of $GL(n, \mathbb{E})$ is monomial (see [8, Lemma 2, p. 219]). The focus of study in [9, 10] is absolutely irreducible groups, and thus nilpotent primitive subgroups of $GL(n, \mathbb{F})$ are mostly ignored (nilpotent absolutely irreducible primitive linear groups over \mathbb{F} exist only in degree 2). So, although much was known about the structure of nilpotent linear groups, and there were some classification results known for maximal absolutely irreducible nilpotent subgroups of $GL(n, \mathbb{F})$, a complete classification of nilpotent irreducible – in particular, primitive – subgroups of $GL(n, \mathbb{F})$ was not derived.

Nilpotent linear groups over an arbitrary field \mathbb{E} are treated in several publications by V. S. Konyukh (see [4], where most of the relevant results are summarised). We

remark that, just as in [9, 10], classification results in [4] are concerned with *maximal* locally nilpotent subgroups of $\mathrm{GL}(n, \mathbb{E})$. To study a nilpotent absolutely irreducible primitive linear group G (of prime power degree), Konyukh considered factors of the series $G \geq Z \geq K \geq 1$ where $K = [G, G]$ and $Z = C_G(K)$. Since Z has nilpotency class at most 2, the problem is reduced to describing class 2 nilpotent irreducible linear groups. For nilpotent primitive groups G over \mathbb{F} this procedure is not really fruitful, because Z will be abelian except when the Sylow 2-subgroup of G is quaternion of order 8. In fact finite nilpotent primitive linear groups G have a very apparent structure: each odd order subgroup is cyclic, and the Sylow 2-subgroup of G has a cyclic subgroup of index 2, that is, G has a cyclic subgroup of index 2 (see [5, 12]). This information is the starting point for our classification. In the penultimate section of the paper we give an algorithm to compute, for any input n and q , a list of nilpotent primitive subgroups of $\mathrm{GL}(n, \mathbb{F})$ such that any group of that kind is $\mathrm{GL}(n, \mathbb{F})$ -conjugate to a single listed group. Each listed group is given by an explicit generating set of matrices, of size at most 2.

In the paper's last section we deal briefly with nilpotent imprimitive irreducible subgroups of $\mathrm{GL}(n, \mathbb{F})$. For some classes of subgroups (e.g. soluble, periodic) of $\mathrm{GL}(n, \mathbb{E})$, one may directly reduce study of the irreducible subgroups to study of the primitive subgroups. This is not a viable approach for nilpotent linear groups, partly because a wreath product $H \wr L \leq \mathrm{GL}(n, \mathbb{E})$ where $H \leq \mathrm{GL}(m, \mathbb{E})$, $L \leq \mathrm{Sym}(k)$ are nilpotent and $mk = n$, need not be nilpotent. Also note that there are several complications to be overcome in attempting a classification of nilpotent subgroups of $\mathrm{GL}(n, \mathbb{E})$ when \mathbb{E} is infinite. For example, $\mathrm{GL}(n, \mathbb{E})$ could contain nilpotent irreducible subgroups of every nilpotency class l (see the corollary on p. 73 of [7]). Moreover there may be infinitely many conjugacy classes of maximal locally nilpotent irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$, as shown in [4]. However, for finite fields the forecast is more optimistic, and our paper is a first step towards classifying nilpotent irreducible subgroups of $\mathrm{GL}(n, \mathbb{F})$.

2. Linear groups with an irreducible abelian normal subgroup. Recall that a Singer cycle in $\mathrm{GL}(n, \mathbb{F})$ is an irreducible maximal abelian subgroup. In this section we look at subgroups of the normaliser of a Singer cycle in $\mathrm{GL}(n, \mathbb{F})$, and conjugacy between elements of such normalisers. For basic theory of Singer cycles see e.g. Section 2 of [6].

Let $G = \langle A, g \rangle \leq \mathrm{GL}(n, \mathbb{F})$, where A is an irreducible maximal abelian normal subgroup of G , $|G : A| = r$. The \mathbb{F} -enveloping algebra $\Delta = \langle A \rangle_{\mathbb{F}}$ of A is a field extension of degree n over \mathbb{F}_1 . Since $G\Delta^\times$ normalises the Singer cycle Δ^\times , whose $\mathrm{GL}(n, \mathbb{F})$ -normaliser is the semidirect product of Δ^\times with a cyclic group of order n , and $G\Delta^\times / \Delta^\times \cong G/A$, it follows that r divides n . Set $n/r = m$. For some $d \in \mathrm{GL}(n, \mathbb{F})$ we have an \mathbb{F} -automorphism σ of Δ of order n defined by $\sigma : x \mapsto dx d^{-1}$, $x \in \Delta$. Let $\delta = \sigma^m$. Then $\delta : x \mapsto gxg^{-1}$, $x \in \Delta$, is an automorphism of Δ of order r . Denote by \mathbb{K} the δ -invariant subfield of Δ , so that $|\mathbb{K} : \mathbb{F}_1| = m$. It is not difficult to see that \mathbb{K} is the centraliser of G in $\mathrm{Mat}(n, \mathbb{F})$. Since \mathbb{K} is a field, the irreducible parts of \mathbb{K}^\times are pairwise equivalent, implying that there exists $y \in \mathrm{GL}(n, \mathbb{F})$ such that $(\mathbb{K}^\times)^y$ is generated by the block diagonal matrix $\mathrm{diag}(s, s, \dots, s)$, $\langle s \rangle$ a Singer cycle of $\mathrm{GL}(m, \mathbb{F})$. Therefore $\mathbb{K}_1 := \langle s \rangle_{\mathbb{F}} = \langle s \rangle \cup \{0\} \subseteq \mathrm{Mat}(m, \mathbb{F})$ is a field isomorphic to \mathbb{K} .

As explained in the proof of [11, Theorem 1.19, p. 12], there is a \mathbb{K} -algebra isomorphism ϕ of $\mathbf{C}_{\mathrm{Mat}(n, \mathbb{F})}(\mathbb{K})$ onto $\mathrm{Mat}(r, \mathbb{K})$ such that $\phi(G)$ is an absolutely irreducible subgroup of $\mathrm{GL}(r, \mathbb{K})$. We may view the action of ϕ more explicitly as follows. Let

$y \in \text{GL}(n, \mathbb{F})$ and $s \in \text{GL}(m, \mathbb{F})$ be as in the previous paragraph. If $c \in \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ then c^y as an $r \times r$ block matrix has $m \times m$ blocks that each commute with s , and are therefore either zero or invertible by Schur’s Lemma. If invertible, a block must be in $\langle s \rangle$, because the Singer cycle $\langle s \rangle$ is self-centralising in $\text{GL}(m, \mathbb{F})$. Thus we assume that G – or more generally any element of $\mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ – is in $r \times r$ block matrix form, with the blocks coming from a field $\mathbb{K}_1 \subseteq \text{Mat}(m, \mathbb{F})$ isomorphic to \mathbb{K} . The action of ϕ is then obvious. We reiterate that \mathbb{K} itself has block diagonal form, with constant entry on the main diagonal.

Let $h \in \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$. Denote by $\det_{\mathbb{K}/\mathbb{F}} h$ the determinant of $h \in \text{Mat}(r, \mathbb{K})$ over \mathbb{K} ; that is, $\det_{\mathbb{K}/\mathbb{F}} h = \det \phi(h)$. If $H \subseteq \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ then we define $\text{Det}_{\mathbb{K}/\mathbb{F}} H$ to be $\{\det_{\mathbb{K}/\mathbb{F}} h \mid h \in H\}$.

LEMMA 2.1. *Let $t_1 = db_1, t_2 = db_2, b_i \in \Delta^\times, i = 1, 2$. Suppose $\det b_1 = \det b_2$. Then there exists $h \in \Delta^\times$ such that $ht_1h^{-1} = t_2$.*

Proof. The norm of $x \in \Delta$ over $\mathbb{F}1_n$ is $(\det x)1_n$. Set $b = b_2b_1^{-1}$, so that $t_2 = t_1b$. Since $\det b = 1$, by Hilbert’s Theorem 90 [3, 23.13, p. 365] there exists $h \in \Delta^\times$ such that $b = \sigma^{-1}(h)h^{-1}$. Then $ht_1h^{-1} = ht_2b^{-1}h^{-1} = ht_2\sigma^{-1}(h^{-1})hh^{-1} = ht_2d^{-1}h^{-1}d = hdb_2d^{-1}h^{-1}d = db_2 = t_2$, because $b_2, d^{-1}h^{-1}d \in \Delta$ commute. \square

PROPOSITION 2.2. *Suppose $b_1, b_2 \in \Delta^\times$ and $\det_{\mathbb{K}/\mathbb{F}} b_1 = \det_{\mathbb{K}/\mathbb{F}} b_2$. Then gb_1, gb_2 are conjugate by an element of Δ^\times .*

Proof. The isomorphism ϕ is defined on $\Delta \subseteq \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$. Since $G \subseteq \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$, $\phi(g)$ is also defined, and (acting by conjugation) is a \mathbb{K} -automorphism of $\phi(\Delta)$ of order r . Now we apply Lemma 2.1 with n replaced by r , \mathbb{F} by \mathbb{K} , d by $\phi(g)$, and $x \in \Delta$ by $\phi(x)$, to conclude that there exists $\bar{h} \in \phi(\Delta)$ such that $\bar{h}\phi(gb_1)\bar{h}^{-1} = \phi(gb_2)$. Let $h_1 = \phi^{-1}(\bar{h}) \in \Delta$. Then $h_1gb_1h_1^{-1} = gb_2$. \square

COROLLARY 2.3. *Matrices gb_1, gb_2 , where $b_i \in \Delta^\times (i = 1, 2)$, are Δ^\times -conjugate if and only if $\det b_1 = \det b_2$ and $\det_{\mathbb{K}/\mathbb{F}} b_1 = \det_{\mathbb{K}/\mathbb{F}} b_2$.*

3. Nilpotent primitive linear groups. We retain notation from the previous section. Throughout G is nonabelian. We assume $G = \langle A, g \rangle = G_2 \times C$ where A is irreducible abelian, $|G : A| = 2$, G_2 denotes the Sylow 2-subgroup of G , and $C = \mathbf{O}_2(G)$ is cyclic. Thus $r = 2$ and $n = 2m, m = |\mathbb{K} : \mathbb{F}1_n|$, where \mathbb{K} is the subfield of $\Delta = \langle A \rangle_{\mathbb{F}}$ of δ -invariant elements, δ the order 2 element of $\text{Gal}(\Delta/\mathbb{F}1_n)$ defined by $\delta(x) = gxg^{-1}$. Further, if A_2 is the Sylow 2-subgroup of A then $A = C \times A_2$ and $G_2 = \langle g, A_2 \rangle$. All of these restrictions on the structure of G are realised if G is nilpotent and primitive; then G_2 is dihedral, semidihedral, or generalised quaternion – see [5, 12].

As shown in Section 2, each element of $\mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ – hence each element of Δ^\times and of G – can be written as a matrix over a field $\mathbb{K}_1 \subseteq \text{Mat}(m, \mathbb{F})$ isomorphic to \mathbb{K} , $|\mathbb{K}_1 : \mathbb{F}1_m| = m$, via a \mathbb{K} -algebra isomorphism ϕ of $\mathbf{C}_{\text{Mat}(n, \mathbb{F})}(\mathbb{K})$ onto $\text{Mat}(2, \mathbb{K}_1)$. In particular $C \subseteq \mathbb{K}$ implies $\phi(C)$ is scalar.

THEOREM 3.1. *Suppose G is primitive. Then*

- (i) $\phi(G_2) \leq \text{GL}(2, \mathbb{K}_1)$ is absolutely irreducible and primitive,
- (ii) $\phi(A_2)$ is irreducible,
- (iii) \mathbb{K}^\times does not contain an element of order 4,
- (iv) m is odd,
- (v) $\mathbb{K} = \langle C \rangle_{\mathbb{F}}$.

Proof. By [11, Theorem 1.19, p. 12], $\phi(G)$ is absolutely irreducible and primitive. Since $\phi(C)$ is scalar, (i) is now clear. As an index 2 subgroup of the primitive linear group $\phi(G_2)$, $\phi(A_2)$ is irreducible. By [12], if $\text{GL}(2, \mathbb{K})$ has nonabelian primitive 2-subgroups then $\sqrt{-1} \notin \mathbb{K}$. This gives (iii). For (iv), we observe that if m is even then 4 divides $q^m - 1$, which contradicts (iii).

Since $-1_n \in A_2$, and $\langle A_2 \rangle_{\mathbb{F}} \neq \mathbb{F}1_n$, so $\langle A_2 \rangle_{\mathbb{F}} = \mathbb{F}1_n(a)$ for some $a \in A_2$ of order divisible by 4. Thus $\langle A_2 \rangle_{\mathbb{F}} \cap \mathbb{K} = \mathbb{F}1_n$ by (i). Then from this fact, together with $\Delta = \langle A_2, C \rangle_{\mathbb{F}}$ and $\langle C \rangle_{\mathbb{F}} \subseteq \mathbb{K}$, we infer $|\langle C \rangle_{\mathbb{F}} : \mathbb{F}1_n| = m$; that is $\langle C \rangle_{\mathbb{F}} = \mathbb{K}$.

We assume henceforth that $\langle C \rangle_{\mathbb{F}} = \mathbb{K}$, $q \equiv 3 \pmod{4}$, and m is odd. (If $p = 2$ then a 2-subgroup of $\text{GL}(2, \mathbb{K})$ is abelian, so p will definitely be odd.) We then see that $C = \langle \text{diag}(x, x) \rangle$ for some $\langle x \rangle \leq \mathbb{K}_1^\times$, $\langle x \rangle_{\mathbb{F}} = \mathbb{K}_1$. Set $C_1 = \langle x \rangle$. Since $|\mathbb{K}_1^\times| = q^m - 1$, \mathbb{K}_1^\times is a Singer cycle of $\text{GL}(m, \mathbb{F})$, and thus C_1 is irreducible.

Denote the natural $\text{GL}(n, \mathbb{F})$ -module by V . We have $V = V_1 \oplus V_2$, $\dim_{\mathbb{F}} V_i = m$, $C|_{V_i} = C_1$, $1 \leq i \leq 2$. As C -modules, $V_1 \cong V_2$ and V_1 is irreducible. Indeed, if W is any irreducible C -submodule of V then $W \cong V_1$.

LEMMA 3.2. *Let T be a 2-subgroup of Δ^\times . Then $T \times C \leq \text{GL}(n, \mathbb{F})$ is irreducible if and only if $\phi(T) \leq \text{GL}(2, \mathbb{K}_1)$ is irreducible.*

Proof. Suppose $T^* = T \times C$ is irreducible. If $\phi(T)$ is reducible then by Maschke's Theorem it is generated (up to conjugacy) by a diagonal matrix with entries ± 1 ; but then each V_i is a T^* -module: contradiction.

Now suppose $\phi(T)$ is irreducible. An irreducible T^* -submodule of V contains an irreducible C -submodule, hence has dimension at least m , and so $\langle T^* \rangle_{\mathbb{F}} = \langle C \rangle_{\mathbb{F}}$ if T^* is reducible (by our assumption $\langle C \rangle_{\mathbb{F}} = \mathbb{K}$). But then $\phi(T)$ is scalar.

By Lemma 3.2, A irreducible implies $\phi(A_2)$ irreducible, and vice versa.

- LEMMA 3.3. (i) $|A_2|$ divides $q^2 - 1$.
 (ii) $|A_2|$ divides $2(q^r + 1)$ for all odd r .

Proof. Certainly $|A_2|$ divides $|\Delta^\times| = q^{2m} - 1$. We have

$$q^{2m} - 1 = (q^2 - 1)(q^{2(m-1)} + q^{2(m-2)} + \dots + q^2 + 1)$$

and since m is odd, the second factor on the right hand side above is odd. Hence $|A_2|$ divides $q^2 - 1$. Since $q \equiv 3 \pmod{4}$, $|A_2|/2$ divides $q + 1$. Then

$$q^r + 1 = (q + 1)(q^{r-1} - q^{r-2} + q^{r-3} - \dots + q^2 - q + 1)$$

yields (ii).

We rely heavily on the criterion stated in [6, 2.6]: an irreducible abelian linear group of degree d over a finite field of size f is imprimitive if and only if its order divides $r(f^{d/r} - 1)$ for some prime divisor r of d . To illuminate one direction of this equivalence, note that if the group has an imprimitivity system of prime size r then the group's order divides $r(f^{d/r} - 1)$.

LEMMA 3.4. *Suppose $C_1 \leq \text{GL}(m, \mathbb{F})$ is primitive. If A is imprimitive then every imprimitivity system for A has size 2.*

Proof. If k is a prime dividing the size l of an imprimitivity system for A then A has an imprimitivity system of size k . Suppose k is odd. Then $|A_2||C_1|$ divides

$k(q^{m/k} - 1)(q^{m/k} + 1)$. Some prime divisor of $|C_1|$ must divide $q^{m/k} + 1$, hence divides $q^m + 1$ – cf. the proof of Lemma 3.3. As $|C_1|$ divides $q^m - 1$ we get a contradiction. Thus l is a 2-power dividing $2m$, so that $l = 2$.

THEOREM 3.5. *A is primitive if and only if $C_1 \leq \text{GL}(m, \mathbb{F})$ and $\phi(A_2) \leq \text{GL}(2, \mathbb{K}_1)$ are primitive.*

Proof. Let A be primitive. Suppose C_1 is imprimitive, so $m > 1$ and $|C_1|$ divides $r(q^{m/r} - 1)$ for some prime divisor r of m . But then by Lemma 3.3 (ii), $|A| = |A_2||C_1|$ divides $r(q^{2m/r} - 1)$, contradicting primitivity of A . If $\phi(A_2)$ were imprimitive then it would have to be monomial, but an abelian monomial 2-subgroup of $\text{GL}(2, \mathbb{K}_1)$ has order at most 4, whereas $|A_2||C_1|$ does not divide $2(q^m - 1)$.

Now suppose C_1 and $\phi(A_2)$ are primitive. If A is imprimitive then by Lemma 3.4, $|A|$ divides $2(q^m - 1)$. But then $\phi(A_2)$, of order less than 8, cannot be primitive.

THEOREM 3.6. *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.*

Proof. Let G be primitive, so $\phi(G_2)$ is primitive by Theorem 3.1. If A is primitive then C_1 is primitive by Theorem 3.5. Suppose A is imprimitive. As a consequence of Lemma 3.4 and the fact that the V_i are the unique (up to isomorphism) m -dimensional C -submodules of V , we may then consider that $\{V_1, V_2\}$ is an A -system of imprimitivity. Let A' denote the kernel of the permutation action of A on this system. Each V_i is a faithful A' -module, and is primitive by Lemma 3.4. Since $|A'|$ divides $q^m - 1$ we have $|A' \cap A_2| = 2$ i.e. $A'|_{V_i} = \langle -1_m, C_1 \rangle$, so C_1 is primitive.

Now let C_1 and $\phi(G_2)$ be primitive. Then $\phi(A_2)$ is irreducible. If $\phi(A_2)$ is primitive then G is primitive by Theorem 3.5. Suppose that $\phi(A_2)$ is imprimitive. By the usual order criterion this means that $|\phi(A_2)| = 4$ and thus $G_2 \cong Q_8$, so $G_2 = \langle a_2, g \rangle$ where $a_2^2 = g^2 = [a_2, g] = -1_n$ and $\langle a_2 \rangle = A_2$.

Suppose G is imprimitive. An imprimitivity system \mathcal{I} for G is an imprimitivity system for A , and by Lemma 3.4, \mathcal{I} has size 2. Again we may assume $\mathcal{I} = \{V_1, V_2\}$. Since $\phi(A_2)$ is irreducible, a_2 interchanges V_1 and V_2 , so a_2 has form $l = \begin{pmatrix} 0_m & \alpha \\ -\alpha^{-1} & 0_m \end{pmatrix}$ where $\alpha \in \text{GL}(m, \mathbb{F})$ (here we have also used the relation $a_2^2 = -1_n$). In fact $\alpha \in \langle C_1 \rangle_{\mathbb{F}}$ because α centralises C_1 . The $\text{GL}(n, \mathbb{F})$ -normaliser of the Singer cycle Δ^\times is $\langle \text{diag}(1_m, -1_m), \Delta^\times \rangle$, and therefore $g = \text{diag}(1_m, -1_m)\beta$ for some $\beta \in \Delta^\times$.

Recalling that $\{V_1, V_2\}$ is a G -system of imprimitivity, we see that either g fixes the V_i , and then $\beta = \text{diag}(\beta_1, \beta_1) \in \langle C \rangle_{\mathbb{F}}$, or g interchanges the V_i . In the first case $g^2 = -1_n$ forces $\beta_1^2 = -1_m$, which we know cannot be true. $\langle C \rangle_{\mathbb{F}} = \mathbb{K}$ is an odd degree extension of a field of size congruent to 3 (mod 4). In the second case we get the same contradiction that $\langle C \rangle_{\mathbb{F}}$ contains an element of order 4.

4. The classification. In this section we present a full classification of nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$; that is, we give a list of such groups that is complete and irredundant with respect to conjugacy in $\text{GL}(n, \mathbb{F})$. We also outline an algorithm for constructing the list, given any input degree n and field size q . Every listed group is metacyclic, and so can be specified by at most two (explicit) generating matrices.

Let $\mathcal{A}_{n,q}$ be a list of all the primitive subgroups of the Singer cycle Δ^\times of $\text{GL}(n, \mathbb{F})$. The elements of $\mathcal{A}_{n,q}$ are precisely those subgroups of Δ^\times whose orders do not divide $r(q^{n/r} - 1)$ for any prime divisor r of n . If either $q \not\equiv 3 \pmod{4}$, or n is not twice an odd integer, then $\mathcal{P}_{n,q} = \mathcal{A}_{n,q}$.

To proceed further we need a couple of auxiliary results.

LEMMA 4.1. *Let \mathbb{E} be a finite field of characteristic p and size e , $e \equiv 3 \pmod{4}$. The Sylow 2-subgroup S of a Singer cycle in $\text{GL}(2, \mathbb{E})$ is primitive, and $\text{Det} S = \{-1, 1\}$. If $p \equiv 3 \pmod{8}$ then S is the unique (up to conjugacy) abelian primitive 2-subgroup of $\text{GL}(2, \mathbb{E})$, and $|S| = 8$. If $p \equiv 7 \pmod{8}$ then $|S| > 8$, there exist abelian primitive 2-subgroups B of $\text{GL}(2, \mathbb{E})$ other than S , and $\text{Det} B = \{1\}$ for each such B .*

Proof. Obviously p is odd and not congruent to 1 or 5 (mod 8). Let 2^t be the largest power of 2 dividing $e + 1$, and define

$$x = \begin{pmatrix} 0 & 1 \\ -\omega^{e+1} & \omega + \omega^e \end{pmatrix}^{(e^2-1)/2^{t+1}}$$

where ω is a primitive element of the degree 2 Galois extension of \mathbb{E} . Then $x \in \text{GL}(2, \mathbb{E})$ and $|x| = 2^{t+1}$, which is the largest power of 2 dividing $e^2 - 1$; that is, $\langle x \rangle$ can serve as S . The usual order criterion ensures S is primitive. We calculate that $(\det x)^2 = 1$ and $\det x = 1$ implies $\omega^{(e^2-1)/2} = 1$, so $\det x = -1$. Every proper subgroup of S , and so every abelian primitive 2-subgroup of $\text{GL}(2, \mathbb{E})$ other than S , must therefore lie in $\text{SL}(2, \mathbb{E})$.

The subgroup of $\text{GL}(2, \mathbb{E})$ generated by $l = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is irreducible of order 4 (because \mathbb{E}^\times does not have an element of order 4). Thus any abelian irreducible 2-subgroup of $\text{GL}(2, \mathbb{E})$ of order less than 8 is monomial, so $\text{GL}(2, \mathbb{E})$ has abelian primitive 2-subgroups if and only if there exists $h \in \text{GL}(2, \mathbb{E})$ such that $h^2 = l$.

Suppose $p \equiv 3 \pmod{8}$. By quadratic reciprocity, $-2 \in \mathbb{E}^2$, and $\frac{\sqrt{-2}}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ has determinant -1 and squares to l . Hence $|S| = 8$.

Suppose $p \equiv 7 \pmod{8}$. Then $e \equiv 7 \pmod{8}$, $t > 2$, and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in \text{GL}(2, \mathbb{E})$ squares to l .

We continue with the notation and assumptions of Section 3. Suppose $\phi(A_2)$ is irreducible (as happens when G is primitive). Then, up to conjugacy in $\text{GL}(2, \mathbb{K}_1)$, $\phi(A_2)$ contains the irreducible group of order 4 generated by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since $\phi(C)$ is scalar, we can assume A contains $l_m := \begin{pmatrix} 0_m & 1_m \\ -1_m & 0_m \end{pmatrix}$. Then $\Delta = \langle l_m \rangle_{\mathbb{K}}$, because $|\Delta: \mathbb{K}| = 2$. The $\text{GL}(2, \mathbb{K}_1)$ -normaliser of $\phi(\Delta^\times)$ is generated by $\phi(\Delta^\times)$ and $\phi(d)$, where $d = \text{diag}(1_m, -1_m)$, so $g = db$ for some $b \in \Delta^\times$. Let $d' = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$, $\alpha, \beta \in \mathbb{K}_1$, $\alpha^2 + \beta^2 = -1_m$ (\mathbb{K}_1 is finite, so such α, β always exist).

PROPOSITION 4.2. *Suppose G is primitive. If $-1 \in \text{Det}_{\mathbb{K}/\mathbb{F}} G$ then G is Δ^\times -conjugate to $\langle A, d \rangle$. Otherwise G is Δ^\times -conjugate to $\langle A, d' \rangle$.*

Proof. Since $\text{Det}_{\mathbb{K}/\mathbb{F}} G_2 \subseteq \{-1, 1\}$ and $\det_{\mathbb{K}/\mathbb{F}} d = -1$, we have $\det_{\mathbb{K}/\mathbb{F}} b = \pm 1$.

Suppose $-1 \in \text{Det}_{\mathbb{K}/\mathbb{F}} G$. If $-1 \notin \text{Det}_{\mathbb{K}/\mathbb{F}} A$ then $\det_{\mathbb{K}/\mathbb{F}}(dba) = -1$ for some $a \in A$, i.e. $\det_{\mathbb{K}/\mathbb{F}}(bc) = 1$ for some $c \in C$, yielding $\det_{\mathbb{K}/\mathbb{F}} b = 1$. By Proposition 2.2, G is then Δ^\times -conjugate to $\langle A, d \rangle$. If $\det_{\mathbb{K}/\mathbb{F}} e = -1$ for some $e \in A$ then either $\det_{\mathbb{K}/\mathbb{F}} b = 1$ or $\det_{\mathbb{K}/\mathbb{F}}(be) = 1$; therefore $G = \langle A, dh \rangle$ for some $h \in \Delta^\times$, $\det_{\mathbb{K}/\mathbb{F}} h = 1$. Again the desired conclusion follows by Proposition 2.2.

Suppose $-1 \notin \text{Det}_{\mathbb{K}/\mathbb{F}} G$, so that $\det_{\mathbb{K}/\mathbb{F}} b = -1$. Since $d' = db'$ where $b' = \text{diag}(\alpha, \alpha)1_n + \text{diag}(\beta, \beta)l_m \in \langle l_m \rangle_{\mathbb{K}} = \Delta$ and $\det_{\mathbb{K}/\mathbb{F}} b' = -1$, we are done by Proposition 2.2.

Let $\Delta_2 = \langle a_2 \rangle$ be the Sylow 2-subgroup of Δ^\times , $|a_2| = 2^t$; note that $t > 2$. For each $T \leq \Delta_2$ such that $4 \leq |T| \leq 2^t$, $\phi(T)$ is a subgroup of the Singer cycle $\phi(\Delta^\times)$ of $\text{GL}(2, \mathbb{K}_1)$, and has order not dividing $|\mathbb{K}_1| - 1$. Hence $\phi(T)$ is irreducible. Also, $\phi(T)$ is primitive if (and only if) $|T| \geq 8$.

Let $\mathcal{C}_{n,q} = \{ \langle \text{diag}(x, x) \rangle \mid \langle x \rangle \leq \mathbb{K}_1^\times 1_m \leq \text{GL}(m, \mathbb{F}) \text{ odd order primitive} \}$. Denote $|\mathcal{C}_{n,q}|$ by $\tau_{n,q}$. If $n = 2$ then $\mathcal{C}_{n,q}$ is the list of all odd order subgroups of $\mathbb{F}^\times 1_2$.

Define $\mathcal{B}_{n,q}^1 = \{ \langle a_2^{2^{t-2}} \rangle \times C \mid C \in \mathcal{C}_{n,q} \}$. Further define

$$\begin{aligned} \mathcal{B}_{n,q}^2 &= \{ \langle a_2 \rangle \times C \mid C \in \mathcal{C}_{n,q} \}, \\ \mathcal{B}_{n,q}^3 &= \{ \langle a_2^{2^k} \rangle \times C \mid C \in \mathcal{C}_{n,q}, 1 \leq k \leq t-3 \} \end{aligned}$$

and

$$\begin{aligned} \mathcal{N}_{n,q}^1 &= \{ \langle A, d' \rangle \mid A \in \mathcal{B}_{n,q}^1 \}, \\ \mathcal{N}_{n,q}^2 &= \{ \langle A, d \rangle \mid A \in \mathcal{B}_{n,q}^2 \}, \\ \mathcal{N}_{n,q}^3 &= \{ \langle A, d \rangle, \langle A, d' \rangle \mid A \in \mathcal{B}_{n,q}^3 \}. \end{aligned}$$

Note that $|\mathcal{B}_{n,q}^1| = |\mathcal{B}_{n,q}^2| = |\mathcal{N}_{n,q}^1| = |\mathcal{N}_{n,q}^2| = \tau_{n,q}$, $|\mathcal{B}_{n,q}^3| = (t-3)\tau_{n,q}$, and $|\mathcal{N}_{n,q}^3| = 2(t-3)\tau_{n,q}$. Every element of $\mathcal{B}_{n,q}^1 \cup \mathcal{B}_{n,q}^2 \cup \mathcal{B}_{n,q}^3$ is irreducible by Lemma 3.2. By Theorem 3.5, every element of $\mathcal{B}_{n,q}^2 \cup \mathcal{B}_{n,q}^3$ is primitive, and $\mathcal{B}_{n,q}^1$ contains only imprimitive groups. If $p \equiv 3 \pmod{8}$ then $\mathcal{B}_{n,q}^3$ and consequently $\mathcal{N}_{n,q}^3$ are empty by Lemma 4.1. If $p \equiv 7 \pmod{8}$ then $t \geq 4$ and $\mathcal{N}_{n,q}^3$ is nonempty. Let $\mathcal{N}_{n,q} = \mathcal{N}_{n,q}^1 \cup \mathcal{N}_{n,q}^2 \cup \mathcal{N}_{n,q}^3$.

THEOREM 4.3. $\mathcal{P}_{n,q} = \mathcal{A}_{n,q} \cup \mathcal{N}_{n,q}$ consists entirely of nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$, pairwise non-conjugate in $\text{GL}(n, \mathbb{F})$. Conversely, a nilpotent primitive subgroup of $\text{GL}(n, \mathbb{F})$ is conjugate to some element of $\mathcal{P}_{n,q}$.

Proof. Let $G = \langle A, g \rangle \in \mathcal{N}_{n,q}$. Clearly G is nilpotent. If $G \in \mathcal{N}_{n,q}^2 \cup \mathcal{N}_{n,q}^3$ then G is primitive because A is primitive. If $G \in \mathcal{N}_{n,q}^1$ then $\phi(G_2) \cong Q_8$ is primitive (the full monomial 2-subgroup of $\text{GL}(2, \mathbb{K}_1)$ is dihedral of order 8) so G is primitive by Theorem 3.6.

Suppose H is a nonabelian nilpotent primitive subgroup of $\text{GL}(n, \mathbb{F})$, $H = \langle h, B \rangle$ where B is abelian irreducible, $|H : B| = 2$. Certainly B is conjugate to an element $T \times C$ of $\mathcal{B}_{n,q}^1 \cup \mathcal{B}_{n,q}^2 \cup \mathcal{B}_{n,q}^3$. Suppose $|B| > 4$. By Proposition 4.2, if $-1 \in \text{Det}_{\mathbb{K}/\mathbb{F}} T$ then H is conjugate to an element of $\mathcal{N}_{n,q}^2$, whereas H is conjugate to an element of $\mathcal{N}_{n,q}^3$ otherwise. Suppose $|B| = 4$, so the Sylow 2-subgroup of H is Q_8 , and as $\langle l_m, d \rangle$ is dihedral, H is conjugate to an element of $\mathcal{N}_{n,q}^1$ by Proposition 4.2.

It remains to prove $\mathcal{P}_{n,q}$ is irredundant. Suppose $G, \tilde{G} \in \mathcal{N}_{n,q}$ are distinct and conjugate. From the definitions we see that G and \tilde{G} must both be in $\mathcal{N}_{n,q}^3$, say $G = \langle A, d \rangle, \tilde{G} = \langle A, d' \rangle$. Since $\det(d'a) = \det(a) \in (\mathbb{F}^\times)^2$ for all $a \in A$, $-1 \notin \text{Det} \tilde{G}$. However $-1 = \det d \in \text{Det} G$.

COROLLARY 4.4. Let $\eta_{n,q}$ be the number of conjugacy classes of nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$, and let $\gamma_{n,q}$ be the number of primitive subgroups of a Singer cycle in $\text{GL}(n, \mathbb{F})$. If either $q \not\equiv 3 \pmod{4}$ or n is not twice an odd integer then $\eta_{n,q} = \gamma_{n,q}$; otherwise $\eta_{n,q} = \gamma_{n,q} + 2\tau_{n,q}$ if $p \equiv 3 \pmod{8}$, and $\eta_{n,q} = \gamma_{n,q} + (2t-4)\tau_{n,q}$ if $p \equiv 7 \pmod{8}$.

We can use Theorem 4.3 to derive a result on isomorphism between the nilpotent primitive subgroups of $\text{GL}(n, \mathbb{F})$, and to determine the maximal such subgroups.

PROPOSITION 4.5. *Nilpotent primitive subgroups of $GL(n, \mathbb{F})$ are conjugate if and only if they are isomorphic.*

Proof. (Cf. [2, Theorem 5.11].) Suppose $G, H \in \mathcal{P}_{n,q}$ are isomorphic, $G \neq H$. Since $|G| = |H|$, necessarily $G, H \in \mathcal{N}_{n,q}^3$. But then one of G_2, H_2 is dihedral and the other is generalised quaternion.

PROPOSITION 4.6. *A maximal nilpotent primitive subgroup of $GL(n, \mathbb{F})$ is conjugate either to Δ^\times , or to $\widehat{G} = \langle a_2, d, \widehat{C} \rangle$ where \widehat{C} has maximal order in $C_{n,q}$.*

(i) *If $p = 2$, or $q \equiv 1 \pmod{4}$, or n is not twice an odd integer, then there is a single conjugacy class of maximal nilpotent primitive subgroups of $GL(n, \mathbb{F})$, namely the class containing Δ^\times .*

(ii) *Suppose $q \equiv 3 \pmod{4}$ and $n = 2m$, m odd. If $n = 2$ and $q = 2^{t-1} - 1$ then Δ^\times is conjugate to a subgroup of \widehat{G} , and there is precisely one conjugacy class of maximal nilpotent primitive subgroups of $GL(n, \mathbb{F})$; otherwise there are precisely two conjugacy classes.*

Proof. Only (ii) requires proof. We have $\widehat{G} = \langle A, d \rangle$ where $|\widehat{G} : A| = 2$ and $|A| = 2^{t-1}(q^m - 1)$. Suppose there is a single conjugacy class of maximal nilpotent primitive subgroups of $GL(n, \mathbb{F})$. Then, up to conjugacy, $\Delta^\times \leq \widehat{G}$, i.e. $|\Delta^\times| = |A|$. Thus $q^m + 1 = 2^{t-1}$. By Lemma 3.3 (i), $2^t = |a_2|$ divides $q^2 - 1$, say $2^t l = q^2 - 1$. If $m > 1$ then it follows that $2l(q^{m-1} - q^{m-2} + q^{m-3} - \dots - q + 1) = q - 1$, which is impossible.

REMARK. The normaliser of a Singer cycle is not usually nilpotent. Proposition 4.6 shows that the normaliser of Δ^\times is nilpotent if and only if $n = 2$ and $q = 2^{t-1} - 1$. In particular a Singer cycle normaliser in $GL(2, p)$ is nilpotent if and only if p is a Mersenne prime.

As is evident from the foregoing, classifying nilpotent primitive linear groups over \mathbb{F} boils down to listing primitive subgroups of a Singer cycle. These are found explicitly by taking known powers of a standard generator. It is enough to construct an element of $GL(n, \mathbb{F})$ of order $q^n - 1$, and this can be done e.g. by methods discussed in [1, Section 2].

We now outline an algorithm for listing the nilpotent primitive subgroups of $GL(n, \mathbb{F})$. Let **SingerCycle**(n, q) be a function that returns a (generator of) a Singer cycle of $GL(n, \mathbb{F})$. We can then define functions **AbelianPrimitive**(n, q) and **OddAbelianPrimitive**(n, q) which return lists of all the abelian primitive subgroups of $GL(n, \mathbb{F})$, and the subgroups of odd order amongst those. Two other functions are implicit below. One calculates the 2-part g_2 of a given element g of $GL(n, \mathbb{F})$, i.e. $g = g_2 g_2'$ where $g_2, g_2' \in \langle g \rangle$ have 2-power order and odd order, respectively; this calculation depends on factoring **Order**(g). The other function finds an intertwining matrix (by basic linear algebra).

Input: n, q
 $m := n/2$
 $a := \mathbf{SingerCycle}(n, q)$
 $\mathcal{A}_{n,q} := \mathbf{AbelianPrimitive}(n, q)$

```

 $\mathcal{P}_{n,q} := \mathcal{A}_{n,q}$ 
if  $p = 2$  or  $n$  is odd or  $m$  is an even integer or  $4$  divides
 $q - 1$ 
    return  $\mathcal{P}_{n,q}$ 
else find  $a_2$ 
 $t := \log_2(\text{Order}(a_2))$ 
 $\mathcal{C}_{n,q} := \text{OddAbelianPrimitive}(m, q)$ 
if  $\mathcal{C}_{n,q} = \emptyset$ 
    return  $\mathcal{P}_{n,q}$ 
else find  $h \in \text{GL}(n, \mathbb{F})$  such that  $ha_2^{2^{t-2}}h^{-1} = \begin{pmatrix} 0_m & 1_m \\ -1_m & 0_m \end{pmatrix}$ 
 $a_2 := ha_2h^{-1}$ 
 $d := \begin{pmatrix} 1_m & 0_m \\ 0_m & -1_m \end{pmatrix}$ 
 $d' := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}, \alpha^2 + \beta^2 = -1_m \in \mathbb{K}_1$ 
 $\mathcal{N}_{n,q}^1 := \{ \langle a_2^{2^{t-2}}, C, d' \rangle \mid C \in \mathcal{C}_{n,q} \}$ 
 $\mathcal{N}_{n,q}^2 := \{ \langle a_2, C, d \rangle \mid C \in \mathcal{C}_{n,q} \}$ 
 $\mathcal{P}_{n,q} := \mathcal{P}_{n,q} \cup \mathcal{N}_{n,q}^1 \cup \mathcal{N}_{n,q}^2$ 
if  $p \equiv 3 \pmod{8}$ 
    return  $\mathcal{P}_{n,q}$ 
else  $\mathcal{N}_{n,q}^3 := \{ \langle a_2^{2^i}, C, d \rangle, \langle a_2^{2^i}, C, d' \rangle \mid C \in \mathcal{C}_{n,q}, 1 \leq i \leq t - 3 \}$ 
 $\mathcal{P}_{n,q} := \mathcal{P}_{n,q} \cup \mathcal{N}_{n,q}^3$ 
return  $\mathcal{P}_{n,q}$ 

```

A nonabelian group returned by the algorithm is generated by two elements: d or d' , and the generator $\bar{a}\bar{c}$ of a cyclic subgroup of index 2, where $\bar{a} \in \langle a_2 \rangle$ and \bar{c} is a generator of some $C \in \mathcal{C}_{n,q}$.

5. Nilpotent linear groups. We can use our knowledge of nilpotent primitive linear groups to say something about nilpotent imprimitive (irreducible) linear groups.

THEOREM 5.1. *There exist nonabelian nilpotent absolutely irreducible primitive subgroups of $\text{GL}(n, \mathbb{F})$ if and only if $n = 2$.*

Proof. Suppose $G \leq \text{GL}(n, \mathbb{F})$ is nonabelian nilpotent primitive. Then $n = 2m$, $G = G_2 \times C$, and $\mathbb{K} = \langle C \rangle_{\mathbb{F}}$ is a field extension of \mathbb{F}_1 of degree m . If G is absolutely irreducible then $\mathbb{K} = \mathbf{C}_{\text{Mat}(n, \mathbb{F})}(G) \subseteq \mathbb{F}_1$, so $m = 1$.

COROLLARY 5.2. *If G is a nilpotent absolutely irreducible imprimitive subgroup of $\text{GL}(n, \mathbb{F})$ then every component of an unrefinable system of imprimitivity for G is at most 2-dimensional.*

THEOREM 5.3. *Let G be a nilpotent absolutely irreducible subgroup of $\text{GL}(n, \mathbb{F})$. If any of the following hold then G is monomial.*

- (i) $|G|$ is odd.
- (ii) n is odd.
- (iii) $q \equiv 1 \pmod{4}$.

Proof. If G is primitive then $G \leq \text{GL}(2, \mathbb{F})$ has nontrivial Sylow 2-subgroup and $q \equiv 3 \pmod{4}$, so none of (i), (ii), or (iii) can occur. Suppose G is imprimitive. By [8, Theorem 4, p. 109], for some n_1, n_2 such that $n = n_1 n_2$, G is conjugate to a subgroup of $G_1 \wr T$ where G_1 is a nilpotent absolutely irreducible primitive subgroup of $\text{GL}(n_1, \mathbb{F})$ and $T \leq \text{Sym}(n_2)$ is nilpotent transitive. Furthermore G_1 and T are π -groups, where π is the set of primes dividing $|G|$. Therefore if $|G|$ is odd then G_1 is abelian i.e. $n_1 = 1$ and G_1 is scalar. We already know that if n (hence n_1) is odd or $q \equiv 1 \pmod{4}$ then G_1 is abelian.

REMARK. In [10] it is proved that if $G \leq \text{GL}(n, \mathbb{F})$ is maximal irreducible nilpotent, n is odd, and the $\text{GL}(n, \mathbb{F})$ -centraliser of G is $\mathbb{F}^\times 1_n$, then G is monomial. Theorem 5.3 is a generalisation of that result.

ACKNOWLEDGEMENT. A. S. Detinko received support from the Enterprise Ireland International Collaboration Programme, grants IC/2002/009 and IC/2003/24.

REFERENCES

1. A. S. Detinko, A new GAP group library for irreducible maximal solvable subgroups of prime degree classical groups, *J. Math. Sci.* **108** (2002), 942–950.
2. A. S. Detinko and D. L. Flannery, Nilpotent primitive linear groups over finite fields, *Comm. Algebra*, to appear.
3. I. Martin Isaacs, *Algebra: a graduate course* (Brooks/Cole, Pacific Grove, 1994).
4. V. S. Konyukh, Irreducible locally nilpotent linear groups, *Fundam. Prikl. Mat.* **4** (1998), 1345–1364 (Russian).
5. Peter Roquette, Realisierung von darstellungen endlicher nilpotenter Gruppen, *Arch. Math.* **9** (1958), 241–250.
6. Hyo-Seob Sim, Metacyclic primitive linear groups, *Comm. Algebra* **22** (1994), 269–278.
7. D. A. Suprunenko, *Soluble and nilpotent linear groups*, (Transl. Math. Monographs No. 9. American Mathematical Society, Providence, RI, 1963).
8. D. A. Suprunenko, *Matrix groups*, Transl. Math. Monographs No. 45. (American Mathematical Society, Providence, RI, 1976).
9. D. A. Suprunenko and R. F. Apatenok, Nilpotent irreducible matrix groups over a finite field, *Dokl. Akad. Nauk. BSSR* **3** (1959), 475–478 (Russian).
10. D. A. Suprunenko and R. F. Apatenok, Nilpotent irreducible matrix groups over a finite field, *Dokl. Akad. Nauk. BSSR* **5** (1961), 535–537 (Russian).
11. B. A. F. Wehrfritz, *Infinite linear groups* (Springer-Verlag, 1973).
12. A. E. Zaleskii, Supersolvable and nilpotent subgroups of simple algebras, *Dokl. Akad. Nauk. BSSR* **7** (1963), 800–802 (Russian).