International Journal of Algebra and Computation
Vol. 15, No. 3 (2005) 467–502

LINEAR GROUPS OF SMALL DEGREE OVER FINITE FIELDS

D. L. FLANNERY

Department of Mathematics
National University of Ireland, Galway, Ireland
dane.flannery@nuigalway.ie

E. A. O'BRIEN

Department of Mathematics, University of Auckland
Private Bag 92019, Auckland, New Zealand
obrien@math.auckland.ac.nz

Received 21 December 2003
Revised 17 May 2004

Communicated by M. F. Newman

For $n = 2, 3$ and finite field $\mathbb{E}$ of characteristic greater than n, we provide a complete and irredundant list of soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$. The insoluble irreducible subgroups of $\mathrm{GL}(2, \mathbb{E})$ are similarly determined. Each group is given explicitly by a generating set of matrices. The lists are available electronically.

Keywords: Linear group; irreducible subgroups; $\mathrm{GL}(2, q)$; $\mathrm{GL}(3, q)$; soluble group.

Mathematics Subject Classification 2000: 20H30, 20G40

1. Introduction

In this paper we construct parametrized lists of soluble irreducible linear groups of degrees 2 and 3 over a finite field $\mathbb{E}$. That is, for $n = 2, 3$ and chosen $\mathbb{E}$ of characteristic greater than n, we provide a complete and irredundant list of soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$: any such subgroup is $\mathrm{GL}(n, \mathbb{E})$-conjugate to one and only one group in the list. A complementary list of the insoluble irreducible subgroups of $\mathrm{GL}(2, \mathbb{E})$ is also determined. Each group is given explicitly by a generating set of matrices. These lists are available electronically to use within computer algebra systems.

Although the abstract isomorphism types of subgroups of $\mathrm{PSL}(2, \mathbb{E})$ and $\mathrm{PSL}(3, \mathbb{E})$ have been known for some time (see, for example, [8, Secs. 8.4, 8.5] or Sec. 2 below), our work is a major advance beyond that knowledge. Most significantly, our lists furnish classifications by linear isomorphism in the general linear group, with groups given by explicit generating sets of matrices. Furthermore, this

is the first time such lists have been made available in electronic form, using methods that both avoid the natural permutation representation on the underlying set of vectors and are independent of computational machinery for soluble groups. Since field operations constitute the bulk of the computation, lists are constructed quickly.

This paper is a companion piece to [11], wherein the first author considered irreducible monomial linear groups of prime degree and degree 4 over finite fields. We were originally motivated by the problem of classifying soluble primitive permutation groups as in Short's monograph [22]. In particular, our results enable one to classify all primitive permutation groups with abelian socle in any degree that is the square or cube of a prime.

The books [23, 24] by Suprunenko contain much pioneering work on classification of soluble linear groups; for example, in [24, Sec. 21, pp. 162–168] generating sets are given for $\mathrm{GL}(n, \mathbb{E})$-conjugacy class representatives of the maximal soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E}), n$ prime. Building on Suprunenko's work (and with due credit given to Jordan), Short in [22] lists soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$ for $\mathbb{E}$ of prime order p with $p^n < 256$. His classification of soluble irreducible subgroups of $\mathrm{GL}(2, \mathbb{E})$ is incomplete: as first detected by Alexander Hulpke, two conjugacy classes of monomial subgroups are missing from [22, Theorem 3.5.2].

We draw on some of Short's essential work, but in degree 2 we employ an approach otherwise independent of his, which also applies to insoluble groups, and moreover may be applied successfully to list the soluble groups of degree 3 (indeed many of our methods are relevant in general prime degree).

Again motivated by classification of soluble primitive permutation groups, Eick and Höfling [7] have developed an algorithm to classify conjugacy classes of soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$. Following Aschbacher's classification [1] of the maximal subgroups of $\mathrm{GL}(n, \mathbb{E})$, their algorithm first writes down the maximal soluble irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$, then for each of those inductively constructs its maximal subgroups, deciding whether or not two irreducible elements in the resulting list are conjugate. The algorithm was used to classify the soluble primitive permutation groups of degree at most $3^8 - 1$; this has now been extended to degree 10000 by Höfling.

Comparisons between the two approaches are not very meaningful. The algorithm of Eick and Höfling requires explicit solutions to conjugacy problems, whose inherent complexity grows with the degree and size of field. Our approach assembles explicit generators and depends primarily only on the cost of computations in the finite field.

We have created a parametrized list of generating sets for the groups. The list is designed for Magma [4] but can be readily incorporated into other computer algebra systems. The construction of the list for a specified degree and finite field is very fast. While the generating set returned for a group may vary up to conjugacy, in all other respects the list (and its ordering) is completely determined. We report on this in more detail in Sec. 7.

Finally we comment on steps taken to ensure the accuracy of our list, and compare it with Suprunenko's classification [24, Theorem 6, p. 167] of the maximal irreducible soluble subgroups of $\mathrm{GL}(n,q)$, $n \leq 3$.

2. An Overview

We now recall well-known descriptions of the abstract isomorphism types of irreducible subgroups of $\mathrm{GL}(n,q)$ for $n = 2, 3$. These results guide our general approach in Secs. 4–6, and are consequences of Aschbacher's classification [1]; earlier treatments include [16, Chap. II, Sec. 8].

Theorem 2.1. *Suppose that G is an irreducible subgroup of $\mathrm{GL}(2,q)$ having center Z. Then one or more of the following holds*:

(1) *G is imprimitive and conjugate to a subgroup of the group of monomial matrices $\mathrm{GL}(1,q)$ wr S_2.*
(2) *G is conjugate to a subgroup of the normalizer of a Singer cycle in $\mathrm{GL}(2,q)$.*
(3) *G is conjugate to a subgroup of $\mathrm{GL}(2,r)Z$ where $\mathrm{GF}(r)$ is a proper subfield of $\mathrm{GF}(q)$.*
(4) *G/Z is isomorphic to one of A_4, S_4, or A_5.*
(5) *G contains $\mathrm{SL}(2,q)$.*

Theorem 2.2. *Suppose that G is a soluble irreducible subgroup of $\mathrm{GL}(3,q)$ having center Z. Then one or more of the following holds*:

(1) *G is imprimitive and conjugate to a subgroup of the group of monomial matrices $\mathrm{GL}(1,q)$ wr S_3.*
(2) *G is conjugate to a subgroup of the normalizer of a Singer cycle in $\mathrm{GL}(3,q)$.*
(3) *G is conjugate to a subgroup of $\mathrm{GL}(3,r)Z$ where $\mathrm{GF}(r)$ is a proper subfield of $\mathrm{GF}(q)$.*
(4) *G normalizes an extraspecial group of order 3^3 and so G/Z is isomorphic to a subgroup of the affine group $\mathrm{ASL}(2,3)$.*

3. Notation and Conventions

Throughout the paper, p is a prime and q is a power of p. The algebraic closure of $\mathrm{GF}(p)$ is denoted $\mathbb{F}_p$. Every finite field $\mathrm{GF}(q)$ is a subfield of $\mathbb{F}_p$.

We write a diagonal matrix as the ordered sequence consisting of its main diagonal entries, starting at position $(1,1)$. For a group of diagonal matrices M and set of primes ς, M_ς will denote the largest normal ς-subgroup $\mathsf{O}_\varsigma(M)$ of M. Hence M_ς is the direct product $\prod_{r\in\varsigma} M_r$.

Let $\mathbb{K}$ be a field. The group of all diagonal matrices in $\mathrm{GL}(n,\mathbb{K})$ is denoted $\mathrm{D}(n,\mathbb{K})$, and $\mathrm{M}(n,\mathbb{K}) = \mathrm{D}(n,\mathbb{K}) \rtimes S_n$ is the full monomial matrix subgroup of $\mathrm{GL}(n,\mathbb{K})$, where S_n is the group of all $n \times n$ permutation matrices (identified with the symmetric group of degree n). If $\mathbb{K}$ is finite of size k then "k" may replace "$\mathbb{K}$"

in this notation. The projection homomorphism $\mathrm{M}(n, \mathbb{K}) \to S_n$ defined by $ds \mapsto s$, $d \in \mathrm{D}(n, \mathbb{K})$, $s \in S_n$, will be denoted π.

A primitive linear group in this paper is always irreducible. If the field of definition of a linear group is not clear from the context, then it will be indicated by prefixing.

Another convention relates to our use of the word *list*, as in the Introduction; here we always mean a collection of linear groups all of a certain specified kind, that is complete and irredundant with respect to conjugacy in the ambient general linear group.

4. Preliminaries

In this section n is prime unless stated otherwise.

An irreducible subgroup G of $\mathrm{GL}(n, q)$ is completely reducible over $\mathbb{F}_p$, with $\mathbb{F}_p$-irreducible constituents all of the same degree. If G is not absolutely irreducible then that degree is 1, so G is abelian. As such, G is conjugate to a subgroup of a Singer cycle (a cyclic subgroup of $\mathrm{GL}(n, q)$ of order $q^n - 1$). The theory of Singer cycles in $\mathrm{GL}(n, q)$, and of their $\mathrm{GL}(n, q)$-normalizers, is well-understood (see, for example, [22, 2.32–2.35, p. 15]. Let $\mathcal{A}_{n,q}$ be a list of the irreducible subgroups of a Singer cycle in $\mathrm{GL}(n, q)$.

For nonabelian groups, we begin by solving the listing problem in $\mathrm{GL}(n, \mathbb{F}_p)$. The nonmodular (namely, of order not divisible by p) absolutely irreducible subgroups of $\mathrm{GL}(n, q)$ may then be obtained by determining groups in the list over $\mathbb{F}_p$ that have conjugates in $\mathrm{GL}(n, q)$ and rewriting those groups over $\mathrm{GF}(q)$.

Glasby and Howlett [14] present an algorithm which, given as input an absolutely irreducible matrix representation of degree d over a field $\mathbb{E}$, produces an equivalent representation in which all matrix entries lie in the smallest possible subfield $\mathbb{K}$ of $\mathbb{E}$. The complexity of this algorithm is $d^3|\mathbb{E}\colon \mathbb{K}|$. We use an implementation in Magma of this algorithm to perform rewriting.

An absolutely irreducible subgroup of $\mathrm{GL}(n, q)$ either is conjugate to a subgroup of $\mathrm{M}(n, \mathbb{F}_p)$, or is a primitive subgroup of $\mathrm{GL}(n, q)$. These two situations are not mutually exclusive. Thus we construct separately a list $\mathcal{M}_{n,q}$ of the absolutely irreducible subgroups of $\mathrm{M}(n, q)$, a list $\mathcal{PM}_{n,q}$ of the $\mathrm{GF}(q)$-primitive, $\mathbb{F}_p$-monomial absolutely irreducible subgroups of $\mathrm{GL}(n, q)$, and a list $\mathcal{P}_{n,q}$ of the $\mathbb{F}_p$-primitive absolutely irreducible subgroups of $\mathrm{GL}(n, q)$.

We will find $\mathcal{M}_{n,q}$ from a list of the irreducible subgroups of $\mathrm{M}(n, \mathbb{F}_p)$. Alternatively we could apply the "reduction mod p" theory of [11, Sec. 2] to the lists of finite irreducible subgroups of $\mathrm{M}(2, \mathbb{C})$ and $\mathrm{M}(3, \mathbb{C})$ in Bácskai's thesis [2]. In an attempt to keep the account here reasonably self-contained, we elect not to do that. While the constructions here and in [2] overlap to some extent, they differ in several key areas.

The simplest sort of monomial linear group in any degree n has cyclic projection in S_n. We use the next two results repeatedly when listing such monomial groups. Denote $(12 \cdots n) \in S_n$ by c.

Lemma 4.1 (cf. [2, Lemma 5.2]). *Let $\mathbb{K}$ be an algebraically closed field and $n > 1$ any integer. Suppose G is a subgroup of $\mathrm{M}(n, \mathbb{K})$ such that $\pi G = \langle c \rangle$. Choose $g \in G$ with $\pi g = c$, and let $\zeta \in \mathbb{K}$ be an nth root of $\det(c^{-1}g)$. Then there exists $w \in \mathrm{D}(n, \mathbb{K})$ such that $G^w = \langle \zeta c, \mathrm{D}(n, \mathbb{K}) \cap G \rangle$.*

Proof. Certainly $G = \langle g, \mathrm{D}(n, \mathbb{K}) \cap G \rangle$. The conjugation action of c on a diagonal matrix is to cycle forward its main diagonal entries, so that if $\zeta^{-1}c^{-1}g = (a_1, a_2, \ldots, a_n)$ and

$$w = (1, a_2, a_2a_3, a_2a_3a_4, \ldots, a_2a_3 \cdots a_n)^{-1}$$

then $g^w = \zeta c$ as desired. □

Lemma 4.2. *Suppose G is a finite subgroup of $\mathrm{M}(n, \mathbb{K})$ such that $\pi G = \langle c \rangle$, $\mathbb{K}$ an algebraically closed field of characteristic n. Then G is $\mathrm{D}(n, \mathbb{K})$-conjugate to the split extension $\langle c, \mathrm{D}(n, \mathbb{K}) \cap G \rangle$.*

Proof. By Lemma 4.1, G is conjugate to $\langle \zeta c, \mathrm{D}(n, \mathbb{K}) \cap G \rangle$, where ζ is a scalar whose nth power is in G. Since $|\zeta|$ is coprime to n, so $\zeta \in G$. □

By the next result, elements of $\mathcal{PM}_{n,q}$ for $n = 2$ or 3 normalize Singer cycles.

Theorem 4.3. *Let G be a primitive subgroup of $\mathrm{GL}(n, \mathbb{K})$ with normal subgroup N, $\mathbb{K}$ any field. Then N is either irreducible or scalar. Thus if N is finite abelian then N is cyclic.*

Proof. By Clifford's Theorem the $\mathbb{K}N$-module $\mathbb{K}^{(n)}$ has a single homogeneous component. Since n is prime, if this is reducible then it is a direct sum of isomorphic 1-dimensional submodules, and consequently N is scalar. □

Remark 4.4. If n is any integer and $G \leq \mathrm{GL}(n, \mathbb{K})$ is primitive, then an abelian normal subgroup N of G is a subgroup of the multiplicative group of a field, so that N is cyclic if it is finite.

The following variation on a well-known theme plays a fundamental part in our listing of the primitive subgroups of $\mathrm{GL}(2, q)$ and $\mathrm{GL}(3, q)$.

Theorem 4.5. *Let G be a subgroup of $\mathrm{GL}(n, q)$. Then there exists $\hat{G} \leq \mathrm{SL}(n, \mathbb{F}_p)$ such that $G/\mathsf{Z}(G) \cong \hat{G}/\mathsf{Z}(\hat{G})$. In fact, $\hat{G} \leq \mathrm{SL}(n, q^m)$, where*

(i) *m is a divisor of $n - 1$ if $n \neq p$ and n does not divide $q - 1$,*
(ii) *$m = n$ if $n \neq p$ and n divides $q - 1$,*
(iii) *$m = 1$ if $n = p$.*

Further, $\hat{G}$ has property P if and only if G has property P, where $\mathsf{P} \in \{$irreducible, absolutely irreducible, $\mathbb{K}$-primitive$\}$, $\mathbb{K}$ a subfield of $\mathbb{F}_p$ containing $\mathrm{GF}(q)$.

Proof. Suppose first that $n \neq p$. Let $\bar{m}$ be the order of q mod n. If n and $q - 1$ are coprime then n divides $(q^{\bar{m}} - 1)/(q - 1)$, and thus $\mathrm{GF}(q^{\bar{m}})$ contains nth roots of every element of $\mathrm{GF}(q)$. If $q \equiv 1 \bmod n$ then n divides $(q^n - 1)/(q - 1)$, so $\mathrm{GF}(q^n)$

contains all the nth roots. Of course the nth power of $\mathrm{GF}(q)^\times$ is $\mathrm{GF}(q)^\times$ if $n = p$. Then

$$\hat{G} = \{\omega g \mid g \in G,\, \omega \in \mathrm{GF}(q^m),\, \omega^{-n} = \det(g)\}$$

satisfies the stated conditions. □

The disjoint union $\mathcal{A}_{n,q} \cup \mathcal{M}_{n,q} \cup \mathcal{PM}_{n,q} \cup \mathcal{P}_{n,q}$ contains all irreducible subgroups of $\mathrm{GL}(n,q)$. If $n \leq 3$ then the first three components of this union consist entirely of soluble groups. We divide $\mathcal{P}_{n,q}$ into two sublists $\mathcal{P}^\circ_{n,q}$ and $\mathcal{P}^\bullet_{n,q}$ of soluble and insoluble groups, respectively. The structure of soluble quasiprimitive linear groups over algebraically closed fields has been thoroughly investigated by Suprunenko and others.

Theorem 4.6. *Let G be a soluble primitive subgroup of $\mathrm{GL}(n,\mathbb{F}_p)$. Then*

(i) $\mathrm{Fit}(G)$ *is irreducible*,
(ii) $\mathrm{Fit}(G)/\mathsf{Z}(G) \cong C_n \times C_n$,
(iii) $\mathrm{Fit}(G)/\mathsf{Z}(G)$ *is self-centralizing in* $G/\mathsf{Z}(G)$,
(iv) $G/\mathrm{Fit}(G)$ *is isomorphic to an irreducible subgroup of* $\mathrm{Sp}(2,n) \cong \mathrm{SL}(2,n)$,
(v) *a minimal normal subgroup of* $G/\mathrm{Fit}(G)$ *has order coprime to* n,
(vi) $p \neq n$.

Proof. Set $\mathrm{Fit}(G) = F$ and $\mathsf{Z}(G) = Z$. Note that $G \neq F$, for if G were equal to F then G would have a noncentral abelian normal subgroup, but every abelian normal subgroup of G is scalar.

The G-centralizer of F is $\mathsf{Z}(F)$, and, since G is nonabelian, $F \neq Z$. Thus (i) is a consequence of Theorem 4.3. For (ii)–(iv), see [24, Secs. 19, 20] or [6, pp. 71–74]. The representation implicit in (iv) arises from the conjugation action of G/Z on F/Z. It is an irreducible representation because otherwise there exists a normal subgroup L of G containing Z such that $L/Z \cong C_n$, so that L is an abelian normal subgroup of G. However Z is the maximal abelian normal subgroup of G.

A minimal normal subgroup of G/F is elementary abelian. It cannot have order n since $\mathsf{O}_n(G/F) = 1$ by (iv) and [18, 9.17, p. 159], so it has order dividing $|\mathrm{SL}(2,n)|/n = n^2 - 1$. Thus (v) holds.

To prove (vi), we define for each $h \in F$ a homomorphism $\theta_h\colon F/Z \to Z$ by $\theta_h\colon gZ \mapsto [g,h]$. If $p = n$ then θ_h is trivial, which yields the contradiction that F is abelian. □

Remark 4.7. In Theorem 4.5, $\mathrm{Fit}(G)/\mathsf{Z}(G)$ is the unique minimal normal subgroup of $G/\mathsf{Z}(G)$. Thus $G/\mathsf{Z}(G)$ has trivial center.

Theorem 4.8. *Let G be a finite soluble primitive subgroup of $\mathrm{GL}(n,\mathbb{F}_p)$.*

(i) $\mathrm{Fit}(G)$ *is conjugate to an irreducible subgroup of* $\mathrm{M}(n,\mathbb{F}_p)$ *with diagonal subgroup of index* n.

(ii) $|\mathsf{Z}(G)|$ *is divisible by* n.
(iii) $G/\mathsf{Z}(G)$ *splits over* $\mathrm{Fit}(G)/\mathsf{Z}(G)$, *and all complements of* $\mathrm{Fit}(G)/\mathsf{Z}(G)$ *in* $G/\mathsf{Z}(G)$ *are conjugate.*

Proof. We use Theorem 4.6 several times.

Since $F := \mathrm{Fit}(G)$ is a nilpotent p'-subgroup of $\mathrm{GL}(n, \mathbb{F}_p)$, it follows that F is monomial (see [16, 18.4, p. 580]). Let $\bar{F}$ be a conjugate of F in $\mathrm{M}(n, \mathbb{F}_p)$; then $Z := \mathsf{Z}(G) < \mathrm{D}(n, \mathbb{F}_p) \cap \bar{F}$ and so $1 < |\bar{F} : \mathrm{D}(n, \mathbb{F}_p) \cap \bar{F}| \leq n^2$. Since $\bar{F}$ is irreducible, so $\mathrm{D}(n, \mathbb{F}_p) \cap \bar{F} \neq Z$, for otherwise $C_n \times C_n$ is a transitive permutation group of degree n. Now (i) follows.

For (ii), note that if n does not divide $|Z|$ then $H^2(F/Z, Z) = 0$ by, for example, the Schur–Zassenhaus Theorem; so F splits over Z implying that F is abelian.

Let C/F be a minimal normal subgroup of G/F. We have $H^i(C/F, F/Z) = 0$, $i \geq 1$, and after factoring out trivial cohomology we get $H^i(G/F, F/Z) \cong H^i(G/C, (F/Z)^{C/F})$. If $(F/Z)^{C/F} \neq 0$ then $\mathsf{Z}(C/Z) \cap F/Z$ is a nontrivial normal subgroup of G/Z in F/Z, but F/Z is minimal normal and self-centralizing in G/Z. Hence $H^i(G/F, F/Z) = 0$ as required. □

Corollary 4.9. *If* G *is a finite soluble primitive subgroup of* $\mathrm{GL}(n, \mathbb{F}_p)$ *then* $G/\mathsf{Z}(G) \cong (C_n \times C_n) \rtimes H$ *for some irreducible subgroup* H *of* $\mathrm{SL}(2, n)$, *where the semidirect product is formed with respect to natural action of* H *on the underlying* 2*-dimensional* $\mathrm{GF}(n)$*-space.*

Soluble groups are our primary focus. We will not attempt construction of $\mathcal{P}^{\bullet}_{3,q}$, an arduous task as evidenced by [8, Theorem 8.4.2]. We include $\mathcal{P}^{\bullet}_{2,q}$ since its construction is not much extra work.

We adopt a simplifying restriction for $\mathcal{P}_{n,q}$, treating only the nonmodular case, which ensures that the characteristic p and characteristic zero representation theories coincide (see, for example, [18, 15.13, p. 268]). This is not a serious restriction in degrees 2 and 3, since it produces at most two exceptional values of p.

To end the section, we mention a fact used without further comment, a consequence of the Deuring–Noether Theorem [17, 1.22, p. 26]. Let $\mathbb{K}$ be a field, let n be any positive integer, and suppose G, H are finite subgroups of $\mathrm{GL}(n, \mathbb{K})$ which are conjugate in $\mathrm{GL}(n, \mathbb{L})$ for an extension field $\mathbb{L}$ of $\mathbb{K}$; then G and H are conjugate in $\mathrm{GL}(n, \mathbb{K})$.

5. Degree 2

Short [22, Chap. 3–5] describes how to list the soluble irreducible subgroups of $\mathrm{GL}(2, q)$. A partial implementation of his algorithm — providing such lists for $\mathrm{GL}(2, p)$ where $p^2 < 256$ — is available in GAP [13] and MAGMA [4]. In this section we list all irreducible subgroups of $\mathrm{GL}(2, q)$. Our methods are substantially different to Short's (especially for monomial and $\mathbb{F}_p$-primitive groups) and carry over to other prime degrees.

5.1. *The sublist* $\mathcal{A}_{2,q}$

Theorem 5.1. *Let* α *be a generator of* $\mathrm{GF}(q^2)^\times$, *and define*

$$b = \begin{pmatrix} 0 & 1 \\ -\alpha^{q+1} & \alpha + \alpha^q \end{pmatrix}.$$

Let r *be a divisor of* $q^2 - 1$ *but not* $q - 1$. *Then* $A(r) = \langle b^{(q^2-1)/r} \rangle$ *is an irreducible subgroup of* $\mathrm{GL}(2, q)$ *of order* r. *An irreducible abelian subgroup of* $\mathrm{GL}(2, q)$ *is conjugate to* $A(r)$ *for some* r.

Proof. This is standard; cf. [22, Sec. 2.3]. □

5.2. *The sublist* $\mathcal{M}_{2,q}$

This subsection covers the same ground as [22, Chap. 3] but avoids the error of [22, Theorem 3.5.2].

To list the absolutely irreducible subgroups of $\mathrm{M}(2, q)$ we apply results from [11]. We first assume that p is odd. Let a be the nontrivial 2×2 permutation matrix, and recall the definitions of the diagonal matrices z_i, w_i, and the monomial groups $H(i, j, k)$, made before [11, Theorem 5.1]. That is,

$$z_i = (\omega_i, \omega_i), \quad w_i = (\omega_i, \omega_i^{-1})$$

where $\omega_i \in \mathbb{F}_p$ has order 2^{i+1}, $\omega_i^2 = \omega_{i-1}$, and

$$H(i, j, 1) = \langle a,\, z_i,\, w_j \rangle, \quad H(i, j, 2) = \langle a z_{i+1},\, w_j \rangle, \quad H(i, j, 3) = \langle a,\, z_{i+1} w_{j+1},\, w_j \rangle.$$

Theorem 5.2. *Let* G *be an irreducible subgroup of* $\mathrm{M}(2, \mathbb{F}_p)$ *conjugate to a subgroup of* $\mathrm{M}(2, q)$. *Then* G *is conjugate to* $G_2 \ltimes G_{2'}$ *for some* 2*-subgroup* G_2 *of* $\mathrm{M}(2, q)$, *and odd order subgroup* $G_{2'}$ *of* $\mathrm{D}(2, q)$ *normal in* $\mathrm{M}(2, q)$.

(i) *Suppose* $q \equiv 1$ *mod* 4, *and let* α *be a generator of* $\mathsf{O}_2(\mathrm{GF}(q)^\times)$, $|\alpha| = 2^t$, $t \geq 2$. *Then* G_2 *is* $\mathrm{GL}(2, q)$*-conjugate to one of*

$H(i, j, 1)$	$0 \leq i \leq t-1$,	$1 \leq j \leq t-1$
$H(i, j, 2)$	$0 \leq i \leq t-2$,	$1 \leq j \leq t-1$
$\langle a(\alpha, 1),\, w_j \rangle$	$1 \leq j \leq t-1$	
$H(i, j, 3)$	$0 \leq i \leq t-2$,	$1 \leq j \leq t-2$
$H(t-1, t-1, 3)$		

if $G_{2'}$ *is scalar, and to one of*

$\langle a \rangle$		
$H(i, j, 1)$	$0 \leq i, j \leq t-1$	
$H(i, j, 2)$	$0 \leq i \leq t-2$,	$0 \leq j \leq t-1$
$\langle a(\alpha, 1),\, w_j \rangle$	$0 \leq j \leq t-1$	
$H(i, j, 3)$	$0 \leq i, j \leq t-2$	
$H(t-1, t-1, 3)$		

if $G_{2'}$ *is nonscalar.*

(ii) *Suppose* $q \equiv 3 \bmod 4$. *If* $G_{2'}$ *is scalar then* G_2 *is* $\mathrm{M}(2,q)$*-conjugate to*

$$\langle a,\ (1,-1)\rangle,$$

whereas if $G_{2'}$ *is nonscalar then* G_2 *is* $\mathrm{GL}(2,q)$*-conjugate to one of*

$$\langle a\rangle$$
$$\langle a,\ (-1,-1)\rangle$$
$$\langle a(1,-1)\rangle$$
$$\langle a,\ (1,-1)\rangle.$$

Distinct elements of the list consisting of all $G_2G_{2'}$ *with* G_2 *and* $G_{2'}$ *as prescribed in* (i), (ii) *are not* $\mathrm{GL}(2,q)$*-conjugate.*

Proof. By [11, Theorem 5.1], G is conjugate to $G_2G_{2'}$ where $G_{2'} \leq \mathrm{D}(2,\mathbb{F}_p)$ is an odd order normal subgroup of $\mathrm{M}(2,\mathbb{F}_p)$, and G_2 is $\langle a\rangle$ or some $H(i,j,k)$. Since $G_{2'}$ is conjugate to a subgroup of $\mathrm{D}(2,q)$, $G_{2'}$ must be in $\mathrm{D}(2,q)$.

(i) Suppose $G_2 = H(i,j,k)$. Then G has a scalar of order 2^{i+1}, so $i \leq t-1$, and $(\omega_j, \omega_j^{-1}) \in G_2$ implies $j \leq t-1$ by [11, Lemma 4.2].

The groups $H(i,j,1)$, $0 \leq i,\ j \leq t-1$, and $H(i,j,2)$, $0 \leq j \leq t-1$, $0 \leq i \leq t-2$, are contained in $\mathrm{M}(2,q)$. Although $H(t-1,j,2) \not\leq \mathrm{GL}(2,q)$, we have that $H(t-1,j,2)^{w_{t+1}} = \langle a(\omega_{t-1},1), w_j\rangle \leq \mathrm{M}(2,q)$.

Now suppose $G_2 = H(i,j,3)$. If $i,j \leq t-2$ or $i=j=t-1$ then $G_2 \leq \mathrm{M}(2,q)$. However, the hypotheses $\mathrm{tr}(G_2) \subseteq \mathrm{GF}(q)$ and (a) $i \leq t-2$, $j=t-1$, or (b) $i=t-1$, $1 \leq j \leq t-2$, lead to the contradiction $\omega_t \in \mathrm{GF}(q)$: in (a), by [11, Lemma 4.2], and in (b), because $\omega_{j+1} + \omega_{j+1}^{-1} \neq 0$. It remains to consider that $G_2 = H(t-1,0,3)$ and $G_{2'}$ is nonscalar. In that case the diagonal subgroup of $G_2G_{2'}$ is the unique subgroup of index 2, so is in $\mathrm{D}(2,q)$ if $G_2G_{2'}$ has a conjugate in $\mathrm{M}(2,q)$. But $H(t-1,0,3)$ has a diagonal element of order 2^{t+1}. Hence G_2 cannot be $H(t-1,0,3)$.

For all $H(i,j,k)$ we have $i \geq 0$, and the lower bound on j is determined by whether or not $G_{2'}$ is scalar, according to [11, Theorem 5.1]. Combining that information with the upper bounds on i,j derived earlier yields (i) in its entirety.

(ii) Here $H(0,0,3) = \langle a,\ (1,-1)\rangle \cong D_8$ is a Sylow 2-subgroup of $\mathrm{M}(2,q)$. If $G_{2'}$ is scalar then G_2 is nonabelian, so must be conjugate to $H(0,0,3)$. If $G_{2'}$ is nonscalar then, as in (i), G has no diagonal elements of order greater than the exponent of $\mathrm{D}(2,q)$. After calculating orders we verify that the possibilities for G_2 are $H(0,0,k)$, $1 \leq k \leq 3$. Only $H(0,0,2)$ is not in $\mathrm{M}(2,q)$, and this group is $\mathrm{D}(2,\mathbb{F}_p)$-conjugate to $\langle a(1,-1)\rangle$.

A group $G_2G_{2'}$ here is conjugate to a group listed in [11, Theorem 5.1], so we have an irredundant list by [11, Theorem 5.3]. □

If $p \neq 2$ then $\mathcal{M}_{2,q}$ will be the list of all groups $G_2G_{2'}$ as specified in Theorem 5.2. The odd order normal subgroups N of $\mathrm{M}(2,q)$ contained in $\mathrm{D}(2,q)$ are easily found;

cf. [11, Remark 5.2]. For any prime p let Z denote the scalars of $\mathrm{D}(2,\mathbb{F}_p)$ and set $W = \mathrm{D}(2,\mathbb{F}_p) \cap \mathrm{SL}(2,\mathbb{F}_p)$. We have $|Z \cap W| = 2$ and $N \leq ZW$. Choose $zw \in N$ where $z \in Z$, $w \in W$ are of odd order. Since $(zw)^a = zw^{-1} \in N$, we see that z, $w \in N$. Thus $N \leq (Z \cap \mathrm{D}(2,q)) \times (W \cap \mathrm{D}(2,q))$. Let ω be a generator of $\mathrm{GF}(q)^\times$ and r be a prime divisor of $q-1$. Set $\omega_r = \omega^{(q-1)/r^s}$, where r^s is the largest r-power dividing $q-1$, and define $z_{i,r}$, $w_{i,r}$ to be the diagonal matrices $(\omega_r^{r^i}, \omega_r^{r^i})$, $(\omega_r^{r^i}, \omega_r^{-r^i})$ respectively. Then N_r is one of the r-subgroups of $\langle z_{i,r},\, w_{j,r}\rangle$ of $\mathrm{D}(2,q)$, $0 \leq i,\, j \leq s$.

If $p = 2$ then, by Lemma 4.2, groups in $\mathcal{M}_{2,q}$ are of the form $\langle a,\, N\rangle$ where N is a nonscalar odd order normal subgroup of $\mathrm{M}(2,q)$ in $\mathrm{D}(2,q)$. It is straightforward to prove that if $N \neq \bar{N}$ then $\langle a,\, N\rangle$ and $\langle a,\, \bar{N}\rangle$ are not $\mathrm{GL}(2,q)$-conjugate.

5.3. *The sublist $\mathcal{PM}_{2,q}$*

We could try to recognize $\mathcal{PM}_{2,q}$ within a list of the finite irreducible subgroups of $\mathrm{M}(2,\mathbb{F}_p)$, but will instead use Short's classification [22] of prime degree primitive metacyclic linear groups over finite fields.

Theorem 5.3. *Let α be a generator of $\mathrm{GF}(q)^\times$, and suppose $q-1 = 2^t l$, l odd. Denote the scalars of $\mathrm{GL}(2,q)$ by Z. Set*

$$c = \begin{pmatrix} 1 & 0 \\ \alpha + \alpha^q & -1 \end{pmatrix}$$

and let A be the Singer cycle generated by the matrix b of Theorem 5.1. *Then it is valid to define $\mathcal{PM}_{2,q}$ to be the list of all groups*

$$\langle c,\, \hat{A}\rangle, \quad \langle cb^{2^{t-k}l},\, \tilde{A}\rangle$$

where $\hat{A}$ ranges over the subgroups of A of order not dividing $2(q-1)$, $\tilde{A}$ ranges over the subgroups of A such that $\mathsf{O}_2(A) \not\leq \tilde{A}$, $|\tilde{A}|$ does not divide $q-1$, $\mathsf{O}_2(\tilde{A} \cap Z) \neq 1$, and k is defined by $\mathsf{O}_2(\tilde{A} \cap Z) = \langle b^{(q^2-1)/2^k}\rangle$.

Proof. This theorem paraphrases [22, Theorem 4.2.7]. As defined above, $\mathcal{PM}_{2,q}$ consists of pairwise nonconjugate primitive subgroups of $\mathrm{GL}(2,q)$. An element of this list is $\mathbb{F}_p$-monomial because it has a nonscalar abelian normal subgroup. By Theorem 4.3, an $\mathbb{F}_p$-monomial primitive subgroup of $\mathrm{GL}(2,q)$ normalizes an irreducible abelian subgroup of $\mathrm{GL}(2,q)$; hence it is conjugate to a subgroup of the normalizer of A and so to an element of the stated list. □

5.4. *The sublist $\mathcal{P}_{2,q}$*

Theorem 5.4. *Let G be an $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(2,q)$.*

(a) *Suppose p is odd. Then $G/\mathsf{Z}(G)$ is isomorphic to one of*

(i) A_4,
(ii) S_4,

(iii) A_5,
(iv) $\mathrm{PSL}(2,\bar{q})$,
(v) $\mathrm{PGL}(2,\bar{q})$,

where $\bar{q}$ *is a* p*-power such that* $\log_p \bar{q}$ *divides* $\log_p q$.

(b) *Suppose* $p = 2$. *Then* $G/\mathsf{Z}(G)$ *is isomorphic to one of*

(i) A_5 ($\log_2 q$ *even*),
(ii) $\mathrm{PSL}(2,\bar{q})$,
(iii) $\mathrm{PGL}(2,\tilde{q})$,

where $\bar{q}, \tilde{q} > 3$ *are* p*-powers such that* $\log_2 \bar{q}$ *divides* $\log_2 q$ *and* $2\log_2 \tilde{q}$ *divides* $\log_2 q$.

Proof. By Theorem 4.5 there is an $\mathbb{F}_p$-primitive subgroup $\hat{G}$ of $\mathrm{SL}(2,q^2)$ with central quotient $G^* \cong G/\mathsf{Z}(G)$. If $p = 2$ then $\hat{G} \leq \mathrm{SL}(2,q)$, and by Theorem 4.6 (vi), G^* is insoluble. Then by work of Dickson (see [16, 8.27, p. 213]), G^* is a group as in the statement of the theorem, or p is odd and $G^* \cong \mathrm{PSL}(2,\tilde{q})$ and $\log_p \tilde{q}$ divides $2\log_p q$, or G has a nontrivial cyclic normal subgroup, or G has a nontrivial normal elementary abelian p-subgroup. It is easy to prove that neither of the two latter cases is possible: the preimage of a cyclic normal subgroup of G^* in G is abelian and normal, hence central; and if G^* had a normal elementary abelian p-subgroup then its preimage in G would be in $\mathrm{Fit}(G)$, but p does not divide $|\mathrm{Fit}(G)|$ by Theorem 4.6.

We now show that $\log_p \tilde{q}$ divides $\log_p q$ when p is odd, $G^* \cong \mathrm{PSL}(2,\tilde{q})$, and $\log_p \tilde{q}$ divides $2\log_p q$. Suppose $\tilde{q} = p^r$, $r = 2l$, and $s = \log_p q = ml$. As G^* is isomorphic to a subgroup of $\mathrm{PGL}(2,q)$, we get that $s \geq r$ and $(p^r+1)(p^r-1)$ divides $2p^{s-r}(p^s+1)(p^s-1)$. If m is even then we are done, so let $m = 2k+1$. Certainly p^r+1 is not a power of 2, so we can choose an odd prime divisor t of p^r+1. Then t divides p^s+1 or p^s-1, so it divides $p^s+1+\sigma$ or $p^s-1+\sigma$, where $\sigma = (p^{2l}+1)\left(\sum_{i=1}^{k} p^{(2k-2i+1)l}(-1)^i\right)$. Since

$$\begin{aligned}\sigma &= \sum_{i=1}^{k} p^{(2k-2i+3)l}(-1)^i + \sum_{i=1}^{k} p^{(2k-2i+1)l}(-1)^i \\ &= -\sum_{i=0}^{k-1}(-1)^i p^{(2k-2i+1)l} + \sum_{i=1}^{k} p^{(2k-2i+1)l}(-1)^i \\ &= p^l(-1)^k - p^s,\end{aligned}$$

t divides either p^l+1 or p^l-1. In both cases, t divides p^r-1, so $t \leq 2$, a contradiction. □

To list p'-subgroups of $\mathrm{GL}(2,q)$ as in (a)(i)–(a)(iii) and (b)(i) of Theorem 5.4 we use some very old results, due to Jordan and Klein, which amount to a classification of the finite subgroups of $\mathrm{SL}(2,\mathbb{C})$ (see Blichfeldt [3, Chap. 3]). The classification

rests on an isomorphism $\iota : \mathrm{PSU}(2) \to \mathrm{SO}(3)$, coming from conjugation action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$, where the former is identified with the unit quaternions and the latter with the unit quaternions having zero real part. This much is very familiar from Lie group theory. Similarly, the finite subgroups of $\mathrm{SO}(3)$ are known: up to conjugacy, there are two infinite families, one of cyclic groups and one of dihedral groups, and three groups isomorphic to A_4, S_4, and A_5. (The latter three isomorphism types can be determined purely algebraically. The noncyclic subgroups of $\mathrm{SO}(3)$ are permutation groups of finite degree such that each nontrivial element has precisely two fixed points, and each point stabilizer is a maximal cyclic subgroup. Such a group is the union of its maximal cyclic subgroups, which are the point stabilizers. Different point stabilizers intersect trivially.) Given that all homomorphisms involved are explicit, and that one may get explicit generating rotations for the finite subgroups of $\mathrm{SO}(3)$, it is possible to write down generators for corresponding inverse images in $\mathrm{SU}(2)$ of those groups under the composite of the natural homomorphism $\mathrm{SU}(2) \to \mathrm{PSU}(2)$ and ι. (For our purposes this is the vital point. Analogs of the elements S, U, V, and W_1 of $\mathrm{SL}(2,\mathbb{C})$ given in [3, Secs. 57, 58, pp. 70–73] will be chosen as generators for the $\mathbb{F}_p$-primitive subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ defined in Secs. 5.5 and 5.6.) Moreover, it is clear that a finite subgroup of $\mathrm{SU}(2)$, and thus a finite subgroup of $\mathrm{SL}(2,\mathbb{C})$, is $\mathrm{SL}(2,\mathbb{C})$-conjugate to one of these inverse images or to a splitting subgroup of index 2 in one of them. However, leaving aside the cyclic case, no inverse image splits over its center, the full group of scalars. Those with dihedral central quotient are dicyclic, irreducible and monomial. Those with central quotient A_4, S_4, or A_5 in $\mathrm{PSU}(2)$ are Schur double covers of A_4, S_4, or A_5, respectively; they are all primitive. (A dicyclic group is a double cover if and only if it has order divisible by 8.) The covers of the alternating groups are unique, whereas S_4 has two covers, and the one in $\mathrm{SL}(2,\mathbb{C})$ is the binary octahedral group.

5.5. *The sublist* $\mathcal{P}^{\circ}_{2,q}$

If the prime power r is greater than 3 then $\mathrm{PSL}(2,r)$ and $\mathrm{PGL}(2,r)$ are insoluble. Thus, by Theorem 4.6(vi) and Theorem 5.4, there exists a soluble $\mathbb{F}_p$-primitive subgroup G of $\mathrm{GL}(2,q)$ only if p is odd, and G has central quotient $A_4 \cong \mathrm{PSL}(2,3)$ or $S_4 \cong \mathrm{PGL}(2,3)$. Note that these isomorphism types may be inferred from Corollary 4.9: $\mathrm{SL}(2,2) \cong S_3$ has irreducible subgroups C_3 and S_3 acting on the underlying $\mathrm{GF}(2)$-space $\mathrm{Fit}(G)/\mathsf{Z}(G) \cong C_2 \times C_2$; further $(C_2 \times C_2) \rtimes C_3$, $(C_2 \times C_2) \rtimes S_3$ are isomorphic to A_4, S_4 respectively.

Theorem 5.5. *Suppose $p \geq 5$. Let $\omega \in \mathrm{GF}(p^2)$ be a primitive fourth root of unity, and define*

$$s = \frac{1}{2}\begin{pmatrix} \omega - 1 & \omega - 1 \\ \omega + 1 & -(\omega + 1) \end{pmatrix}.$$

Let E be the set of even order scalars in $\mathrm{GL}(2,q)$. If $q \equiv 1 \bmod 3$, for each $z \in E$ select a scalar $\nu_z \in \mathrm{GL}(2,q^3)$ such that $\nu_z^3 = z$, yet $\nu_z \notin \langle z \rangle$. Define $\mathcal{P}^1_{2,q}$ to be the

following list of subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$:

$$\begin{array}{ll} \langle s,\,(\omega,-\omega),\,z\rangle & \\ \langle \nu_z s,\,(\omega,-\omega)\rangle & q\equiv 1 \bmod 3 \quad \textit{and} \quad \nu_z\in \mathrm{GF}(q) \textit{ only} \end{array}$$

as z *ranges over* E.

(i) *An* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(2,q)$ *with central quotient* A_4 *has center of even order, and is conjugate to a group in* $\mathcal{P}^1_{2,q}$.
(ii) *Each group in* $\mathcal{P}^1_{2,q}$ *is conjugate to an* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(2,q)$ *with central quotient* A_4.
(iii) *Distinct groups in* $\mathcal{P}^1_{2,q}$ *are not* $\mathrm{GL}(2,\mathbb{F}_p)$*-conjugate.*

Proof. This is an application of [11, Theorem 5.4]. The conditions on ν_z ensure $|\nu_z| = 3|z|$. An element of $\mathbb{F}_p$ of order divisible by 3 lies in $\mathrm{GF}(q)$ only if $q \equiv 1 \bmod 3$, and as $\det(s) = 1$, the necessity of the condition $\nu_z \in \mathrm{GF}(q)$ is apparent. Let $G = \langle s, (\omega, -\omega)\rangle$. The conjugacy classes of $G/H \cong A_4$ have representatives gH, $g \in \{1, (\omega,-\omega), s, s^2\}$, and therefore $\mathrm{tr}(G) = \{0, \pm 1, \pm 2\} \subseteq \mathrm{GF}(q)$. Similarly, $\mathrm{tr}(\langle \nu_z s,\,(\omega,-\omega)\rangle) \subseteq \langle \nu_z\rangle \mathrm{GF}(q)$. Hence an element of $\mathcal{P}^1_{2,q}$ has trace values in $\mathrm{GF}(q)$, so it is conjugate to a subgroup of $\mathrm{GL}(2,q)$ by [18, 9.14, p. 150]. □

Remark 5.6. If $q \equiv 3 \bmod 4$ then no element of $\mathcal{P}^1_{2,q}$ is in $\mathrm{GL}(2,q)$, but all groups may be rewritten over $\mathrm{GF}(q)$ using the algorithm of [14].

Remark 5.7. Let $\langle\alpha\rangle$ be the scalar subgroup of $\mathrm{GL}(2,q^3)$. In Theorem 5.5, $z = \alpha^{(q^3-1)/r}$ for some (even) r dividing $q-1$, and if $q \equiv 1 \bmod 3$ then we can take $\nu_z = \alpha^{(q^3-1)/3r}$.

The techniques used to prove [11, Theorem 5.4] are also important in proving the next result.

Theorem 5.8. *Suppose* $p \geq 5$. *Let* $\omega \in \mathrm{GF}(p^2)$ *be a primitive fourth root of unity and* $\alpha \in \mathrm{GF}(p^2)$ *be a square root of* 2. *Define* s *as in Theorem* 5.5, *and*

$$u = \frac{1}{\alpha}\begin{pmatrix} 1+\omega & 0 \\ 0 & 1-\omega \end{pmatrix}.$$

For each scalar $z \in \mathrm{GL}(2,q)$ *of even order choose a scalar* $\mu_z \in \mathrm{GL}(2,q^2)$ *such that* $\mu_z^2 = z$, *and denote the set of all pairs* (z,μ_z) *by* E. *If* $p \equiv \pm 1$ *mod* 8 *or* $\log_p q$ *is even then define* $\mathcal{P}^2_{2,q}$ *to be the list of groups*

$$\begin{array}{ll} \langle s,\,u,\,z\rangle & \\ \langle s,\,\mu_z u,\,z\rangle & \mu_z \in \mathrm{GF}(q) \textit{ only,} \end{array}$$

(z,μ_z) *ranging over* E; *otherwise* $\mathcal{P}^2_{2,q}$ *is the list of all* $\langle s,\,\mu_z u,\,z\rangle$ *such that* $\mu_z\alpha \in \mathrm{GF}(q)$.

(i) *An* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(2,q)$ *with central quotient* S_4 *has center of even order, and is conjugate to a group in* $\mathcal{P}^2_{2,q}$.

(ii) *Each group in* $\mathcal{P}^2_{2,q}$ *is conjugate to an* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(2,q)$ *with central quotient* S_4.
(iii) *Distinct groups in* $\mathcal{P}^2_{2,q}$ *are not* $\mathrm{GL}(2,\mathbb{F}_p)$*-conjugate.*

Proof. Suppose G is an $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(2,q)$ with center $Z = \langle z \rangle$ such that $G/Z \cong S_4$. By Theorem 4.8(ii), $|Z|$ is even. By the Universal Coefficient Theorem,

$$H^2(G/Z, Z) = \mathrm{Ext}(S_4/S_4', Z) \times \mathrm{Hom}(H_2(S_4), Z) \cong \mathrm{Ext}(C_2, Z) \times \mathrm{Hom}(C_2, Z).$$

Say the extension-equivalence class of G corresponds to $[\xi] \in H^2(G/Z, Z)$. We cannot have $[\xi] \in \mathrm{Ext}(S_4/S_4', Z)$, as ξ is trivial on the normal fours group in S_4, so gives rise to an S_4-extension of Z with a noncyclic abelian normal subgroup (cf. Theorem 4.3). Thus there are only two possible isomorphism types for G. Each type of group contains a copy of $\mathrm{SL}(2,3)$, the unique Schur cover of A_4. The one for which the Ext component of $[\xi]$ is nontrivial has a noncentral element squaring to z, and does not contain a Schur cover of S_4 if $|Z| \geq 4$.

Since G splits over its group of odd order scalars, we may assume Z is a 2-group. If $|Z| = 2$ then G is isomorphic to one of the two Schur covers of S_4: namely $\mathrm{GL}(2,3)$, or the binary octahedral group, call it B. Now $\mathrm{GL}(2,3)$ has two faithful irreducible ordinary representations of degree 2, but these are related in the usual way (cf. [11, Proposition 2.12]) by the nontrivial outer automorphism of $\mathrm{GL}(2,3)$, so there is a single conjugacy class of irreducible subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ isomorphic to the p'-group $\mathrm{GL}(2,3)$. Similarly there is a single conjugacy class of irreducible subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ isomorphic to B. Let $K_1 = \langle s, u \rangle$ and $K_2 = \langle s, \omega u \rangle$ where $\omega \in \mathrm{GF}(p^2)$ is a square root of -1. Using $s^3 = (usu)^3 = 1$ and $(sus)^2 = u^4 = (-1,-1)$, it is not difficult to check that $K_1 \cong B$ and $K_2 \cong \mathrm{GL}(2,3)$. Note that K_1 but not K_2 is in $\mathrm{SL}(2,\mathbb{F}_p)$, so K_1 and K_2 are not conjugate. Both K_1 and K_2 are nonabelian and hence absolutely irreducible, and they are primitive because neither has an abelian subgroup of index 2 (since $\mathrm{SL}(2,3)$ is the unique subgroup of index 2 in a Schur cover of S_4).

If $|Z| = 2$ then we have seen that G is conjugate to precisely one of K_1 or K_2. Assume $|Z| \geq 4$. If G contains K_1 (up to conjugacy) then it contains K_2, and vice versa, and G is conjugate to $K_1Z = K_2Z = \langle s, u, z \rangle$. Suppose now that G does not have a subgroup isomorphic to K_1 or K_2, so that $g^2 = z$ for some $g \in G \setminus Z$. Let $\mu_z \in \mathrm{GL}(2,q^2)$ be a scalar such that $\mu_z^2 = z$, so $\langle G, \mu_z \rangle$ has a subgroup K conjugate to K_2, generated by the noncentral involution $\mu_z^{-1}g$ and a copy of $\mathrm{SL}(2,3)$; say $K^x = K_2$, $x \in \mathrm{GL}(2,\mathbb{F}_p)$. Then $G^x/Z \cong S_4$ is a subgroup of $H = \langle K_2Z, \mu_z \rangle / Z \cong S_4 \times C_2$. Now H has only two subgroups isomorphic to S_4, namely K_2Z/Z and $\langle s, \mu_z u, z \rangle / Z$. We can discard K_2Z/Z as a possibility for G^x/Z, so G^x must be $\langle s, \mu_z u, z \rangle$.

It has been demonstrated that G is conjugate in $\mathrm{GL}(2,\mathbb{F}_p)$ to $G_1 = \langle s, u, z \rangle$ or $G_2 = \langle s, \mu_z u, z \rangle$, and $G_1 \ncong G_2$. Since $G_1X = G_2X = K_1X$, where X denotes the scalars of $\mathrm{GL}(2,\mathbb{F}_p)$, it follows that G_1 and G_2 are $\mathbb{F}_p$-primitive, and both have

central quotient S_4. Let $H = \langle s,\, (\omega, -\omega),\, z\rangle$. We have $H \le G_1 \cap G_2$ and $|G_1 : H| = |G_2 : H| = 2$, and, as noted in the proof of Theorem 5.5, $\mathrm{tr}(H) \subseteq \mathrm{GF}(q)$. If $h \in H$ then $\mathrm{tr}(uh) = \alpha^{-1}(\mathrm{tr}(h) + \mathrm{tr}((\omega, -\omega)h)) \in \alpha\mathrm{GF}(q)$. Thus $\mathrm{tr}(G_1) \subseteq \langle\alpha\rangle\mathrm{GF}(q)$. Similarly $\mathrm{tr}(G_2) \subseteq \langle\mu_z\alpha\rangle\mathrm{GF}(q)$. Since $\alpha = \mathrm{tr}(u) \in \mathrm{tr}(G_1)$, G_1 is conjugate to a subgroup of $\mathrm{GL}(2,p)$ if and only if 2 is a quadratic residue mod p, that is, $p \equiv \pm 1$ mod 8. Alternatively, if $\log_p q$ is even then $\alpha \in \mathrm{GF}(p^2) \subseteq \mathrm{GF}(q)$. In either case G_1 should be in our list, and G_2 should be there too, as long as $\mu_z \in \mathrm{GF}(q)$. However, if $\log_p q$ is odd and $p \equiv \pm 3$ mod 8 then $\alpha \in \mathrm{GF}(p^2) \setminus \mathrm{GF}(p)$, but $\mathrm{GF}(q) \cap \mathrm{GF}(p^2) = \mathrm{GF}(p)$, so only G_2 can have a conjugate in $\mathrm{GL}(2,q)$. The test for this is simply whether or not $\mathrm{tr}(\mu_z u) = \mu_z\alpha \in \mathrm{GF}(q)$. □

Remark 5.9. If $q \equiv 3$ mod 4, then no element of $\mathcal{P}^2_{2,q}$ is in $\mathrm{GL}(2,q)$, but all groups may be rewritten over $\mathrm{GF}(q)$ using the algorithm of [14].

Theorem 5.10. *Suppose $p \ge 5$. After all necessary rewriting, $\mathcal{P}^\circ_{2,q} = \mathcal{P}^1_{2,q} \cup \mathcal{P}^2_{2,q}$ is a list of the soluble $\mathbb{F}_p$-primitive subgroups of* $\mathrm{GL}(2,q)$.

5.6. *The sublist $\mathcal{P}^\bullet_{2,q}$*

Theorem 5.11. *Suppose $p > 5$. Let $\omega \in \mathrm{GF}(p^2)$ be a primitive fourth root of unity and let $\beta \in \mathrm{GF}(p^2)$ be a square root of* 5. *Define s as in Theorem* 5.5, *and*

$$v = \frac{1}{2}\begin{pmatrix} \omega & \frac{1-\beta}{2} - \omega(\frac{1+\beta}{2}) \\ \frac{-1+\beta}{2} - \omega(\frac{1+\beta}{2}) & -\omega \end{pmatrix}.$$

(i) *There is an $\mathbb{F}_p$-primitive subgroup of* $\mathrm{GL}(2,q)$ *with central quotient A_5 if and only if $q \equiv \pm 1$ mod* 5.

(ii) *Suppose $q \equiv \pm 1$ mod* 5. *Let $\mathcal{P}^3_{2,q}$ be the list of all groups*

$$\langle s,\, (\omega, -\omega),\, v,\, z\rangle$$

as z ranges over the even order scalars in $\mathrm{GL}(2,q)$. *Every element of $\mathcal{P}^3_{2,q}$ is $\mathbb{F}_p$-primitive and has central quotient A_5. Conversely, such a subgroup of* $\mathrm{GL}(2,q)$ *is conjugate to a single group in $\mathcal{P}^3_{2,q}$.*

Proof. Let G be an $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(2,q)$ with center Z such that $G/Z \cong A_5$. If $|Z|$ is even then $H^2(G/Z, Z) \cong C_2$, otherwise $H^2(G/Z, Z) = 1$. From the ordinary character table of A_5 it can be seen that G does not split over Z. Therefore $|Z|$ is even and G contains the unique Schur cover of A_5, namely $\mathrm{SL}(2,5)$. The two faithful irreducible degree 2 representations of $\mathrm{SL}(2,5)$ in characteristic $p > 5$ are related by the nontrivial outer automorphism of $\mathrm{SL}(2,5)$, so there is a single conjugacy class of irreducible subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ isomorphic to $\mathrm{SL}(2,5)$.

Let $H = \langle s,\, (\omega, -\omega),\, v\rangle$ and

$$K = \langle x_1,\, x_2,\, x_3 \mid x_1^3 = x_2^2 = x_3^2 = (x_1x_2)^3 = (x_2x_3)^3 = (x_1x_3)^2 = 1\rangle.$$

It is easy to deduce that $K \cong A_5$. Since $s^3 = 1$, $(\omega, -\omega)^2 = v^2 = (-1, -1)$, $(s(\omega, -\omega))^3 = ((\omega, -\omega)v)^3 = 1$, and $(sv)^2 = (-1, -1)$, we see that $H/\langle(-1, -1)\rangle$ is a homomorphic image of K, hence must be all of K. As H has an element of order 4, unlike $A_5 \times C_2$, H cannot split over its center. Therefore $H \cong \mathrm{SL}(2, 5)$, and G is conjugate to HZ. Clearly $\mathcal{P}^3_{2,q}$ is irredundant (it contains a single group of each order $60z$).

A set of representatives for the conjugacy classes of K is $\{1, x_1, x_2, x_1x_2x_3, x_3x_2x_1\}$. Using the epimorphism of H onto K defined by $s \mapsto x_1$, $(\omega, -\omega) \mapsto x_2$, $v \mapsto x_3$, we can then calculate that, up to multiplication by -1, the elements of H have trace in $\{\, 0, 1, 2, (1 + \beta)/2, (1 - \beta)/2 \,\}$. Thus $\beta \in \mathrm{GF}(q)$, which is equivalent to $q \equiv \pm 1 \bmod 5$, by quadratic reciprocity. □

Theorem 5.12. *Let $p = 5$. The list $\mathcal{P}^4_{2,q}$ consisting of all groups $\langle \mathrm{SL}(2, 5), z\rangle$, z an even order scalar in $\mathrm{GL}(2, q)$, is a list of the $\mathbb{F}_p$-primitive subgroups of $\mathrm{GL}(2, q)$ with central quotient A_5.*

The next few results are needed to list the insoluble absolutely irreducible subgroups of $\mathrm{GL}(2, q)$ with central quotient other than A_5.

Lemma 5.13. *If p is odd then $\mathrm{PSL}(2, q)$ does not have a faithful representation of degree 2 over $\mathrm{GF}(q)$.*

Lemma 5.14. *$A_5 \cong \mathrm{PSL}(2, q)$ if and only if $q = 5$; $A_5 \cong \mathrm{PGL}(2, q)$ if and only if $q = 4$.*

Lemma 5.15. *Let $\mathbb{K}$ be an algebraically closed field and $\mathbb{L}$ a subfield of $\mathbb{K}$. Suppose G is a subgroup of $\mathrm{GL}(n, \mathbb{L})$ that is irreducible over $\mathbb{K}$. Then, modulo scalars, $\mathsf{N}_{\mathrm{GL}(n,\mathbb{K})}(G) \leq \mathrm{GL}(n, \mathbb{L})$.*

Proof. If $x \in \mathsf{N}_{\mathrm{GL}(n,\mathbb{K})}(G)$ then $xy \in \mathsf{C}_{\mathrm{GL}(n,\mathbb{K})}(G)$ for some $y \in \mathrm{GL}(n, \mathbb{L})$, by the Deuring–Noether Theorem. By the hypotheses about $\mathbb{K}$ and G, $\mathsf{C}_{\mathrm{GL}(n,\mathbb{K})}(G)$ is scalar. □

Theorem 5.16. *Suppose $n \geq 3$, or $n = 2$ and $q > 3$. Let $\mathbb{E}$ be any extension of $\mathrm{GF}(q)$. If G is a subgroup of $\mathrm{GL}(n, \mathbb{E})$ isomorphic to $\mathrm{SL}(n, q)$ then G is irreducible over $\mathbb{E}$, and is conjugate to $\mathrm{SL}(n, q)$.*

Proof. Some ideas in this proof were suggested to us by L. G. Kovács.

It is known that $\mathrm{GF}(q)$, hence $\mathbb{E}$, is a splitting field for $\mathrm{SL}(n, q)$; see the main theorem of [20]. Thus the image of any irreducible $\mathbb{E}$-representation of $\mathrm{SL}(n, q)$ is conjugate to a group over $\mathrm{GF}(q)$ (see, for example, [18, 9.8, p. 148]). The result will follow once we show that G is irreducible, because $\mathrm{SL}(n, q)$ is the unique subgroup of $\mathrm{GL}(n, q)$ isomorphic to $\mathrm{SL}(n, q)$.

Suppose the $\mathbb{E}G$-module $\mathbb{E}^{(n)}$ has a composition series factor of dimension $m < n$, so there is an irreducible representation $G \to \mathrm{GL}(m, q)$. If $m \neq 1$ then this

further implies that $\mathrm{GL}(m,q)$ has a subgroup with quotient $\mathrm{PSL}(n,q)$ (if $m=1$ then the representation is trivial). But $q^{n(n-1)/2}$ divides $|\mathrm{PSL}(n,q)|$, whereas the highest power of p dividing $|\mathrm{GL}(m,q)|$ is $q^{m(m-1)/2}$. Therefore all $\mathbb{E}G$-composition factors of $\mathbb{E}^{(n)}$ are 1-dimensional, and a conjugate of G is unitriangular. But then G is a p-group. □

Theorem 5.17. *Suppose p is odd and $q>5$. Let α be a generator of $\mathrm{GF}(q)^\times$ and let $\bar{q}$ be a power of p such that $\log_p \bar{q}$ divides $\log_p q$ and $\bar{q}>3$ if $p=3$. Set $r=(q-1)/(\bar{q}-1)$. For each $\bar{q}$ define a list $\mathcal{L}_{q,\bar{q}}$ of subgroups of $\mathrm{GL}(2,q)$ as follows*:

$\langle(\alpha^s,\alpha^s),\ \mathrm{SL}(2,\bar{q})\rangle$ — *only if $p\neq 5$, or $p=5$ and $\bar{q}>5$*

$\langle(\alpha^{r/2},\alpha^{-r/2}),\ (\alpha^s,\alpha^s),\ \mathrm{SL}(2,\bar{q})\rangle$ — *r even*

$\langle(\alpha^{(s+r)/2},\alpha^{(s-r)/2}),\ (\alpha^s,\alpha^s),\ \mathrm{SL}(2,\bar{q})\rangle$ — *s, r both odd or both even,*

where $s\geq 1$ ranges over the divisors of $q-1$ such that $(q-1)/s$ is even. Then define

$$\mathcal{P}^5_{2,q}=\bigcup_{\bar{q}}\mathcal{L}_{q,\bar{q}}\,.$$

(i) *Every group in $\mathcal{P}^5_{2,q}$ is absolutely irreducible and has central quotient $\mathrm{PSL}(2,\bar{q})$ or $\mathrm{PGL}(2,\bar{q})$ for some $\bar{q}$, and no group has central quotient A_5.*

(ii) *An absolutely irreducible insoluble subgroup G of $\mathrm{GL}(2,q)$ with central quotient other than A_5 is conjugate to a group in $\mathcal{P}^5_{2,q}$.*

(iii) *Distinct groups in $\mathcal{P}^5_{2,q}$ are not conjugate.*

Proof. (i) $\mathrm{SL}(2,\bar{q})$ is an insoluble absolutely irreducible subgroup of $\mathrm{GL}(2,q)$, and hence so too is every group in $\mathcal{P}^5_{2,q}$. By Lemma 5.14, and because $(\alpha^{r/2},\alpha^{-r/2})\equiv(\alpha^r,1)$ mod scalars and $\mathrm{GL}(2,\bar{q})=\langle(\alpha^r,1),\ \mathrm{SL}(2,\bar{q})\rangle$, every group has central quotient as described.

(ii) Denote the scalars of $\mathrm{GL}(2,q)$ by Z and set $\mathsf{Z}(G)=X=\langle(\alpha^s,\alpha^s)\rangle$, where s divides $q-1$. By Theorem 5.4(i), G/X is isomorphic to $\mathrm{PSL}(2,\bar{q})$ or $\mathrm{PGL}(2,\bar{q})$ for some $\bar{q}$ such that $\log_p\bar{q}$ divides $\log_p q$. Thus G has a subgroup H of index at most 2 with $\mathsf{Z}(H)=X$ and such that $H/X\cong\mathrm{PSL}(2,\bar{q})$. By [19, Theorem 9.1, p. 189] (which cites R. Steinberg), the multiplier of $\mathrm{PSL}(2,\bar{q})$ has order 2 unless $\bar{q}=9$, in which case the multiplier has order 6. Hence there are just two possible isomorphism types for H. One of these, the direct product, is irrelevant by Lemma 5.13. Therefore $|X|=(q-1)/s$ is even and there is a subgroup K of H isomorphic to the unique Schur cover of $\mathrm{PSL}(2,\bar{q})$, viz. $\mathrm{SL}(2,\bar{q})$. The only normal subgroup of $H=KX$ isomorphic to K and containing the scalar of order 2 is K, so K is characteristic in H and therefore normal in G.

By Theorem 5.16, K is absolutely irreducible and conjugate to $\mathrm{SL}(2,\bar{q})$. We can therefore assume that $\mathrm{SL}(2,\bar{q})$ is a normal subgroup of G, and so $|G:\mathrm{SL}(2,\bar{q})X|\leq 2$. If this index is 1 then the structure of G is transparent: G is generated by $\mathrm{SL}(2,\bar{q})$ and (α^s,α^s). Consequently, from now on let the index be

2, that is, $G/X \cong \mathrm{PGL}(2,\bar{q})$. Lemma 5.15 tells us that $G \leq \mathrm{GL}(2,\bar{q})Z$, and so $GZ = \mathrm{GL}(2,\bar{q})Z$. Thus

$$\mathrm{GL}(2,\bar{q})Z/\mathrm{SL}(2,\bar{q})X = G/\mathrm{SL}(2,\bar{q})X \times \mathrm{SL}(2,\bar{q})Z/\mathrm{SL}(2,\bar{q})X \cong C_2 \times C_s. \qquad (1)$$

If s is odd then there is a single possibility for G in $\mathrm{GL}(2,\bar{q})Z$, and if s is even then there are two possibilities (remember $G \not\leq \mathrm{SL}(2,\bar{q})Z$). To obtain generators for these, we seek an involution of $\mathrm{GL}(2,\bar{q})Z/\mathrm{SL}(2,\bar{q})X$ not in $\mathrm{SL}(2,\bar{q})Z/\mathrm{SL}(2,\bar{q})X$. A preimage g of this involution in $\mathrm{GL}(2,\bar{q})Z$ may be expressed as $(\alpha^r,1)z$, some $z \in Z$. For the square of $(\alpha^r,1)z$ to be in $\mathrm{SL}(2,\bar{q})X$ it is necessary that $\alpha^r z^2 \in X$; in other words, there is some $(\delta,\delta) \in X$ such that δ/α^r has a square root in $\mathrm{GF}(q)$. This occurs if and only if either $\mathrm{GF}(\bar{q})^\times \leq (\mathrm{GF}(q)^\times)^2$, or $\mathrm{GF}(\bar{q})^\times \not\leq (\mathrm{GF}(q)^\times)^2$ and $X \not\leq (\mathrm{GF}(q)^\times)^2$, which in turn is equivalent to r being even, or r and s both being odd. If r is even then we take $g = (\alpha^{r/2}, \alpha^{-r/2})$, and G is generated by $\mathrm{SL}(2,\bar{q})X$ and either g when s is odd, or $g(\alpha^{s/2}, \alpha^{s/2})$ when s is even. If r,s are odd then we take $g = (\alpha^{(s+r)/2}, \alpha^{(s-r)/2})$. This now accounts for all groups in $\mathcal{L}_{q,\bar{q}}$.

(iii) Since the set $\{\mathrm{PSL}(2,\bar{q}),\ \mathrm{PSL}(2,\tilde{q}),\ \mathrm{PGL}(2,\bar{q}),\ \mathrm{PGL}(2,\tilde{q})\}$ for a power $\tilde{q}$ of p contains an isomorphic pair only if $\bar{q} = \tilde{q}$, there is no overlap between the different $\mathcal{L}_{q,\bar{q}}$. For the same reason, a group of the type listed first in $\mathcal{L}_{q,\bar{q}}$, which has central quotient $\mathrm{PSL}(2,\bar{q})$, is not conjugate to a group of the second or third type. If groups of the second and third type were conjugate, by $x \in \mathrm{GL}(2,q)$ say, then $x \in \mathrm{GL}(2,\bar{q})Z$; but after passing to quotients in (1), x would have trivial conjugation action. □

Theorem 5.18. (i) *After rewriting over* $\mathrm{GF}(q)$, $\mathcal{P}^3_{2,q} \cup \mathcal{P}^5_{2,q}$ $(p > 5)$ *or* $\mathcal{P}^4_{2,q} \cup \mathcal{P}^5_{2,q}$ $(q > p = 5)$ *is a list* $\mathcal{P}^\bullet_{2,q}$ *of the insoluble* $\mathbb{F}_p$*-primitive subgroups of* $\mathrm{GL}(2,q)$.
(ii) *If* $q = 5$ *then* $\mathcal{P}^\bullet_{2,5} = \{\mathrm{SL}(2,5), \langle \mathrm{SL}(2,5), (4,1)\rangle, \mathrm{GL}(2,5)\}$ *is a list of the insoluble irreducible subgroups of* $\mathrm{GL}(2,5)$.

This completes the listing of the irreducible subgroups of $\mathrm{GL}(2,q)$ for all $p \geq 5$.

6. Degree 3

6.1. *The sublist* $\mathcal{A}_{3,q}$

Theorem 6.1. *Let* α *be a generator of* $\mathrm{GF}(q^3)^\times$, *and define*

$$b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix}$$

where $\alpha_1 = \alpha^{q^2+q+1}$, $\alpha_2 = -(\alpha^{q+1} + \alpha^{q+q^2} + \alpha^{q^2+1})$, *and* $\alpha_3 = \alpha + \alpha^q + \alpha^{q^2}$. *Let* r *be a divisor of* $q^3 - 1$ *but not* $q - 1$ *nor* $q^2 - 1$. *Then* $A(r) = \langle b^{(q^3-1)/r} \rangle$ *is an irreducible subgroup of* $\mathrm{GL}(3,q)$ *of order* r. *An irreducible abelian subgroup of* $\mathrm{GL}(3,q)$ *is conjugate to* $A(r)$ *for some* r.

Proof. Cf. [22, Sec. 2.3]. □

6.2. *The sublist* $\mathcal{M}_{3,q}$

Following earlier practice, we construct a list of the finite irreducible subgroups of $\mathrm{M}(3,\mathbb{F}_p)$ and then rewrite the relevant part of that list in $\mathrm{GL}(3,q)$.

Denote by c and d the 3×3 permutation matrices obtained from the identity by permuting its columns as (123) and (12), respectively. The transitive subgroups of S_3 are $S_3 = \langle c, d\rangle$ and $C = \langle c\rangle$. Observe that c acts by conjugation on a diagonal matrix to cycle forward the main diagonal entries; d swaps the first two diagonal entries.

Theorem 6.2. *Let $\mathbb{K}$ be an algebraically closed field and G be a finite subgroup of $\mathrm{M}(3,\mathbb{K})$. Set $M = \mathrm{D}(3,\mathbb{K}) \cap G$.*

(i) *If $\pi G = C$ then G is $\mathrm{D}(3,\mathbb{K})$-conjugate to $\langle cz, M_3\rangle \ltimes M_{3'}$, where z is a scalar of 3-power order such that $z^3 \in M_3$.*
(ii) *If $\pi G = S_3$ then G is $\mathrm{D}(3,\mathbb{K})$-conjugate to $\langle c, dz, M_2\rangle \ltimes M_{2'}$, where z is a scalar of 2-power order such that $z^2 \in M_2$.*

Proof. (i) is clear by Lemma 4.1 and the fact that $H^2(G/M_{3'}, M_{3'}) = 1$.

(ii) Certainly G splits over $M_{\{2,3\}'}$, and by (i), G is $\mathrm{D}(3,\mathbb{K})$-conjugate to $HM_{\{2,3\}'}$ where $H = \langle cz_c, dm, M_2, M_3\rangle$, z_c a scalar of 3-power order, $z_c^3 \in M_3$, and $m \in \mathrm{D}(3,\mathbb{K})$. We may write m as the product of a scalar z_d and a diagonal matrix $(\tilde{\omega}, \tilde{\omega}^{-1}\omega, \omega^{-1})$ in $\mathrm{SL}(3,\mathbb{F}_p)$. The relations $c^{-d} = c$ and $d^2 = 1$ in S_3 imply that $(\tilde{\omega}, \tilde{\omega}^{-1}, 1) \equiv z_c^2(1, \tilde{\omega}, \tilde{\omega}^{-1})(\omega, \omega, \omega^{-2})^{-1}$ and $(\omega, \omega, \omega^{-2}) \equiv z_d^{-2} \bmod M_2M_3$, from which we conclude that in H (and relabeling as necessary), m may be chosen as $z_d(1, \omega, \omega^{-1})$. Then $(\omega^{-2}, \omega, \omega)$ and $(\omega, \omega^{-2}, \omega)$ are in the C-module M_2M_3, up to multiplication by scalars. Therefore

$$\begin{aligned} H^{(1,\omega,\omega^2)} &= \langle cz_c(\omega^{-2}, \omega, \omega),\ dz_d(\omega^{-1}, \omega^2, \omega^{-1}),\ M_2,\ M_3\rangle \\ &= \langle cz_c,\ dz_d,\ M_2,\ M_3\rangle \end{aligned}$$

after relabeling. Since $z_d^2 \in M_2M_3$, if we express z_d as the product of its 2-part, 3-part, and $\{2,3\}'$-part, then it is evident that z_d is a 2-element, at least mod M_2M_3. Similarly we can assume z_c is a 3-element. But $(cz_c)^d \equiv (cz_c)^{-1} \bmod M_2M_3$, which implies $z_c^2 \in M_3$ and hence $z_c \in M_3$. □

Remark 6.3. For a generalization of the claim in Theorem 6.2(ii) that G has a (monomial) conjugate containing πG up to scalars, see [2, Theorem 6.10].

Lemma 6.4. *A group as in Theorem* 6.2(i) *is not isomorphic to a group as in Theorem* 6.2(ii).

Until further notice, in this subsection $p \geq 5$.

Theorem 6.5 (cf. [2, Theorem 5.4]). *Let G be a finite subgroup of $\mathrm{M}(3,\mathbb{F}_p)$. Then G is irreducible if and only if $\pi G = C$ or S_3 and $M := \mathrm{D}(3,\mathbb{F}_p) \cap G$ is nonscalar.*

Proof. Suppose G is irreducible; then πG is transitive and hence is S_3 or C. If M is scalar then the 1-dimensional $\mathbb{F}_p$-space spanned by the all 1s vector is invariant under G, by Theorem 6.2; that is, G is reducible.

Suppose M is nonscalar and $\pi G = C$ or S_3, so that G has a nonabelian subgroup H with $\pi H = C$ and $H \cap \mathrm{D}(3, \mathbb{F}_p) = M$. The p'-group H is isomorphic to a subgroup of $\mathrm{GL}(3, \mathbb{C})$, and if the latter were reducible then all of its irreducible characters would have degree 1, by Ito's theorem [18, 6.15, p. 84]. But then H would be abelian. Hence H and thus G is irreducible. □

We now determine the finite C-submodules and S_3-submodules of $\mathrm{D}(3, \mathbb{F}_p)$. Bácskai does this in [2, Chaps. 3 and 4]. Much of what we present for submodules of 3-power order can be extracted from Conlon [5], although he does not always give explicit matrix generators for groups.

Let Z be the scalars of $\mathrm{GL}(3, \mathbb{F}_p)$, U be the subgroup of $\mathrm{D}(3, \mathbb{F}_p)$ consisting of all diagonal matrices $(\omega, \omega^{-1}, 1)$, and set $W = U^c$. Neither U nor W is a C-module, but $U \times W = \mathrm{D}(3, \mathbb{F}_p) \cap \mathrm{SL}(3, \mathbb{F}_p)$ is. Also $\mathrm{D}(3, \mathbb{F}_p) = ZUW$, and $|Z \cap UW| = 3$.

Let $r \neq p$ be a prime, and for $i \geq 0$ inductively select primitive r^ith roots of unity $\omega_{i,r} \in \mathbb{F}_p$ such that $\omega_{i+1,r}^r = \omega_{i,r}$. Define

$$z_{i,r} = (\omega_{i,r}, \omega_{i,r}, \omega_{i,r}), \quad u_{i,r} = (\omega_{i,r}, \omega_{i,r}^{-1}, 1), \quad w_{i,r} = u_{i,r}^c = (1, \omega_{i,r}, \omega_{i,r}^{-1}).$$

Note that $w_{i,r}^c = u_{i,r}^{-1} w_{i,r}^{-1}$, $u_{i,r}^d = u_{i,r}^{-1}$, and $w_{i,r}^d = u_{i,r} w_{i,r}$. A finite subgroup of $(UW)_r = U_r \times W_r \cong C_{r^\infty} \times C_{r^\infty}$ is one of

$$\langle u_{i,r},\, w_{j,r} \rangle \quad \langle u_{i+k,r}^l w_{j+k,r},\, u_{i,r},\, w_{j,r} \rangle$$

for some $i, j \geq 0$, $k \geq 1$, and $1 \leq l \leq r^k - 1$ such that l is coprime to r: this may be deduced from the Goursat–Remak Theorem (see [21, 1.6.1, p. 35]), which will be used again later. For one of these subgroups to be a C-module, i must equal j. Certainly $\langle u_{i,r},\, w_{i,r} \rangle$ is a C-module. Suppose $M = \langle u_{i+k,r}^l w_{i+k,r},\, u_{i,r},\, w_{i,r} \rangle$ is a C-module. Then

$$w_{i+k,r}^{l^2-l+1} = (u_{i+k,r}^{l^2} w_{i+k,r}^l)^c u_{i+k,r}^l w_{i+k,r} \in M \cap W = \langle w_{i,r} \rangle$$

so that $l^2 - l + 1 \equiv 0 \bmod r^k$. Conversely, if $l^2 - l + 1 \equiv 0 \bmod r^k$ then M is a C-module; furthermore r is odd and (completing the square) -3 is a quadratic residue mod r. If $r \neq 3$ then $\left(\frac{r}{3}\right) = 1$ by quadratic reciprocity. Hence $r \equiv 1 \bmod 3$. Summing up: if $r \equiv 2 \bmod 3$ then the C-submodules of $(UW)_r$ are

$$\langle u_{i,r},\, w_{i,r} \rangle, \quad i \geq 0$$

and these are also precisely the S_3-submodules of $(UW)_r$. If $r \equiv 1 \bmod 3$ then there are additionally the C-submodules

$$\langle u_{i+k,r}^l w_{i+k,r},\, u_{i,r},\, w_{i,r} \rangle, \quad i \geq 0, \quad k \geq 1, \quad l^2 - l + 1 \equiv 0 \mod r^k,$$

which are not, however, S_3-modules. The two distinct solutions of $l^2 - l + 1 \equiv 0 \bmod r^k$ may be found recursively in the manner explained before [10, Theorem 2.3.3].

Now suppose $r = 3$. There is a solution of $l^2 - l + 1 \equiv 0 \bmod 3^k$ only if $k = 1$. The finite C-submodules of $(UW)_3$ are then

$$\langle u_{i,3},\, w_{i,3}\rangle, \quad \langle u_{i+1,3}^2 w_{i+1,3},\, u_{i,3},\, w_{i,3}\rangle, \quad i \geq 0,$$

with order 3^{2i} in the first instance and 3^{2i+1} in the second. All C-submodules of $(UW)_3$ are S_3-modules too.

Theorem 6.6. *Let r be a prime, $r \neq p$.*

(i) *A finite C-submodule of $\mathrm{D}(3, \mathbb{F}_p)$ of r-power order is one of*

$$\langle z_{i,r},\, u_{j,r},\, w_{j,r}\rangle$$
$$\langle z_{i,r},\, u_{j+k,r}^l w_{j+k,r},\, u_{j,r},\, w_{j,r}\rangle \quad r \equiv 1 \text{ mod } 3 \text{ only}$$

if $r \neq 3$, where $i,\, j \geq 0$, $k \geq 1$, $l^2 - l + 1 \equiv 0$ mod r^k, or one of

$$\langle z_{i,3},\, u_{j,3},\, w_{j,3}\rangle \qquad i, j \geq 1 \quad \text{or} \quad i = j = 0$$
$$\langle z_{i,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle \qquad i \geq 1,\ j \geq 0$$
$$\left.\begin{array}{l}\langle z_{i+1,3} u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle \\ \langle z_{i+1,3}^2 u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle\end{array}\right\} \quad i, j \geq 1$$
$$\left.\begin{array}{l}\langle z_{i+1,3} u_{j+1,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle \\ \langle z_{i+1,3}^2 u_{j+1,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle\end{array}\right\} \quad i \geq 1,\ j \geq 0$$

if $r = 3$.

(ii) *A finite S_3-submodule of $\mathrm{D}(3, \mathbb{F}_p)$ of r-power order is one of*

$$\langle z_{i,r},\, u_{j,r},\, w_{j,r}\rangle$$

$i, j \geq 0$, if $r \neq 3$, or one of

$$\langle z_{i,3},\, u_{j,3},\, w_{j,3}\rangle \qquad i, j \geq 1 \quad \text{or} \quad i = j = 0$$
$$\langle z_{i,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle \qquad i \geq 1,\ j \geq 0$$
$$\left.\begin{array}{l}\langle z_{i+1,3} u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle \\ \langle z_{i+1,3}^2 u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle\end{array}\right\} \quad i, j \geq 1$$

if $r = 3$.

Proof (cf. [9, Sec. 3.1] and [2, Chap. 3]). Since a section of $(UW)_r$ is annihilated by $1 + c + c^2$, only sections of order 3 can be C-isomorphic to sections of Z. Thus when $r \neq 3$ only "Cartesian" C-submodules arise in the direct product $Z_r \times (UW)_r$. On the other hand, the order 3 sections of $(UW)_3$, a uniserial C-module (see [5, Lemma 1.5] or [2, Lemma 3.8]), are

$$\langle u_{j+1,3}^2 w_{j+1,3}, u_{j,3}, w_{j,3}\rangle / \langle u_{j,3}, w_{j,3}\rangle, \quad \langle u_{j+1,3}, w_{j+1,3}\rangle / \langle u_{j+1,3}^2 w_{j+1,3}, u_{j,3}, w_{j,3}\rangle,$$

$j \geq 0$, and the first but not the second of these is S_3-trivial, whereas both are C-trivial. Every nonidentity finite C-submodule of $(ZUW)_3$ contains the scalar $z_{1,3}$, and once this is factored out (set $j \geq 1$ for the first kind of order 3 section

of $(UW)_3$ stated above) we have a direct product on which the Goursat–Remak Theorem may be brought to bear. Non-Cartesian C-modules are obtained for each of the two C-isomorphisms from one length 3 section of $Z_3/\langle z_{1,3}\rangle$ onto a length 3 section of $(UW)_3/\langle z_{1,3}\rangle$. The S_3-submodules of $(ZUW)_3$ can be picked out from the C-submodules, or by construction, as the S_3-trivial sections of $(UW)_3$ are known. □

The next theorem resolves S_3-conjugacy among C-submodules of $\mathrm{D}(3,q)$ of $3'$-order.

Theorem 6.7. *Let R be the set of all primes not equal to 3 dividing $q-1$, with R_1 the subset of primes congruent to 1 mod 3. For each $r \in R$, denote by r^{e_r} the largest r-power dividing $q-1$, and define*

$$\mathcal{C}_{1,r} = \{\langle z_{i,r},\, u_{j,r},\, w_{j,r}\rangle \mid 0 \le i,j \le e_r\}.$$

For each $k \ge 1$ and $r \in R_1$, choose a single solution $l_{r,k}$ of $l^2 - l + 1 \equiv 0$ mod r^k, and define

$$\begin{aligned}\mathcal{C}_{2,r} &= \{\langle z_{i,r},\, u_{j+k,r}^{l_{r,k}} w_{j+k,r},\, u_{j,r},\, w_{j,r}\rangle \mid 0 \le i,\, j \le e_r,\, k \le e_r - j\},\\ \mathcal{C}_{3,r} &= \{\langle z_{i,r},\, u_{j+k,r}^{l_{r,k}} w_{j+k,r},\, u_{j,r},\, w_{j,r}\rangle,\\ &\qquad \langle z_{i,r},\, u_{j+k,r}^{1-l_{r,k}} w_{j+k,r},\, u_{j,r},\, w_{j,r}\rangle \mid 0 \le i,\, j \le e_r,\, k \le e_r - j\}.\end{aligned}$$

Then let $\mathcal{C}$ be the list consisting of all $M = \prod_{r\in R} M_r$ where either $M_r \in \mathcal{C}_{1,r}$ for all r, or for some $\bar r \in R_1$, $M_{\bar r} \in \mathcal{C}_{2,\bar r}$ and $M_r \in \mathcal{C}_{1,r}$ if $r < \bar r$, $M_r \in \mathcal{C}_{1,r} \cup \mathcal{C}_{3,r}$ if $r > \bar r$. A C-submodule of $\mathrm{D}(3,q)$ of $3'$-order is S_3-conjugate to an element of $\mathcal{C}$, and no two distinct elements of $\mathcal{C}$ are S_3-conjugate.

Define

$$\begin{aligned}
C(i,j,1,\varepsilon) &= \langle cz_{i+1,3}^{\varepsilon},\, z_{i,3},\, u_{j,3},\, w_{j,3}\rangle, && \varepsilon \in \{0,1\},\ i,j \ge 1\\
C(i,j,2,\varepsilon) &= \langle cz_{i+1,3}^{\varepsilon},\, z_{i,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle, && \varepsilon \in \{0,1\},\ i \ge 1,\ j \ge 0\\
C(i,j,3) &= \langle c,\, z_{i+1,3}u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle, && i,j \ge 1\\
C(i,j,4) &= \langle c,\, z_{i+1,3}^2 u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle, && i,j \ge 1\\
C(i,j,5) &= \langle c,\, z_{i+1,3}u_{j+1,3},\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle, && i \ge 1,\ j \ge 0.
\end{aligned}$$

All these groups bar the $C(i,0,2,\varepsilon)$ are nonabelian. Aided by the order formulas $|C(i,j,1,\varepsilon)| = 3^{i+2j}$, $|C(i,j,2,\varepsilon)| = |C(i,j,3)| = |C(i,j,4)| = 3^{i+2j+1}$, $|C(i,j,5)| = 3^{i+2j+2}$, it is easy to see that the $C(i,j,k,\varepsilon)$ and $C(i,j,k)$ are distinct for distinct values of the parameters i,j,k,ε.

Theorem 6.8. *Let G be a finite irreducible subgroup of $\mathrm{M}(3,\mathbb{F}_p)$ with $\pi G = C$. Then G is $\mathrm{GL}(3,\mathbb{F}_p)$-conjugate to $G_3 \ltimes G_{3'}$ where $G_{3'} := \mathsf{O}_{3'}(G) \le \mathrm{D}(3,\mathbb{F}_p)$, and if $G_{3'}$ is scalar then G_3 is one of $C(i,j,1,\varepsilon)$, $C(i,j,2,\varepsilon)$, $C(i,j,3)$, $C(i,j,4)$, $C(i,j,5)$, $i,\ j \ge 1$ and $\varepsilon \in \{0,1\}$, whereas if $G_{3'}$ is nonscalar then G_3 is C, one of the aforementioned 3-groups, or some $C(i,0,2,\varepsilon)$ or $C(i,0,5)$.*

Proof. Let M be the diagonal subgroup of G. By Theorem 6.2(i), G is $\mathrm{D}(3,\mathbb{F}_p)$-conjugate to $\langle cz,\ M_3\rangle M_{3'}$, where $z \in Z_3$ and $z^3 \in M_3$. Referring to Theorem 6.6(i), we discover that either $z \in \mathrm{SL}(3,\mathbb{F}_p)$ mod M_3 and then G is $\mathrm{D}(3,\mathbb{F}_p)$-conjugate to $\langle c,\ M_3\rangle M_{3'}$ by Lemma 4.1, or M_3 is an S_3-module and $z = z_{i+1,3}^{\eta}$ mod M_3, $\eta \in \{0,1,2\}$, where 3^i is the order of the scalar subgroup of M_3. Now $(\langle cz_{i+1,3}^2,\ M_3\rangle M_{3'})^d = \langle cz_{i+1,3},\ M_3^d\rangle M_{3'}^d$, so η can be restricted to $\{0,1\}$. Similarly, note that

$$\langle c,\ z_{i+1,3}^2 u_{j+1,3},\ u_{j+1,3}^2 w_{j+1,3},\ u_{j,3},\ w_{j,3}\rangle^d = C(i,j,5), \quad i \geq 1,\ j \geq 0.$$

At this stage we can see that G is $\mathrm{M}(3,\mathbb{F}_p)$-conjugate to $G_3 M_{3'}$, where G_3 is one of the choices stated for nonscalar $M_{3'} = G_{3'}$ (every nondiagonal subgroup of $\mathrm{M}(3,\mathbb{F}_p)$ of order 3 is conjugate to C). Further, if $M_{3'}$ is indeed nonscalar then $G_3 M_{3'}$ is irreducible by Theorem 6.5.

Assume now that $M_{3'}$ is scalar. Let

$$m = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_{1,3} & \omega_{1,3}^2 \\ 1 & \omega_{1,3}^2 & \omega_{1,3} \end{pmatrix}.$$

Then $c^m = w_{1,3}$, $u_{1,3}^m = c^{-1} z_{1,3}$, and $w_{1,3}^m = c^{-1}$, so $C(i,1,1,1)^m = C(i,0,5)$. Hence we include $C(i,j,5)M_{3'}$ only for $j \geq 1$. By Theorem 6.5, G is irreducible if and only if G_3 is nonabelian. We ensure this by taking j greater than 0 when $G_3 = C(i,j,2,\varepsilon)$. □

Lemma 6.9. *Every group listed in Theorem* 6.8, *apart from the* $C(i,1,1,\varepsilon)G_{3'}$ *with* $G_{3'}$ *scalar, has a unique abelian normal subgroup of index* 3.

Proof. If $G_3 G_{3'}$ has more than one abelian normal subgroup of index 3 then its diagonal subgroup has scalar subgroup of index 3, containing $G_{3'}$. By Theorem 6.8 and the order formulas before the theorem, we see that this can happen only if $G_3 = C(i,1,1,\varepsilon)$. □

Lemma 6.10. *Let* G *and* H *be isomorphic finite irreducible subgroups of* $\mathrm{M}(3,\mathbb{F}_p)$.

(i) $\pi G = \pi H = C$ *or* $\pi G = \pi H = S_3$.
(ii) *If* $\pi G = S_3$ *then* $\mathsf{O}_{\{2,3\}'}(G) = \mathsf{O}_{\{2,3\}'}(H)$.

Proof. (i) is just Theorem 6.5 and Lemma 6.4. For (ii) we use the fact that the groups of diagonal matrices $\mathsf{O}_{\{2,3\}'}(G)$ and $\mathsf{O}_{\{2,3\}'}(H)$ have the same scalar subgroup and order, and hence must be equal, since those two parameters completely determine an S_3-submodule of $(ZUW)_{3'}$; see Theorem 6.6(ii). □

Theorem 6.11. *Let* G, H *be finite subgroups of* $\mathrm{M}(3,\mathbb{F}_p)$ *such that* $\pi G = \pi H = C$. *If* $G^m = H$ *and* $M^m = N$ *for some* $m \in \mathrm{GL}(3,\mathbb{F}_p)$ *and nonscalar subgroups* M *of* $\mathrm{D}(3,\mathbb{F}_p) \cap G$, N *of* $\mathrm{D}(3,\mathbb{F}_p) \cap H$, *then* $m \in \mathrm{M}(3,\mathbb{F}_p)$.

Proof. Bácskai [2, (2.14)] proved a version of this result for subgroups of $\mathrm{M}(n, \mathbb{C})$, n prime, and his proof is valid for groups over $\mathbb{F}_p$. □

Theorem 6.12. *Let $\mathcal{T}$ be the list of all G_3 appearing in the semidirect products $G_3 G_{3'}$ of Theorem* 6.8, *with $G_{3'}$ nonscalar. Distinct groups in $\mathcal{T}$ are not isomorphic, except that $C(i,1,1,1) \cong C(i,0,5), i \geq 1$.*

Proof. We reconcile our notation for 3-subgroups of $\mathrm{M}(3, \mathbb{F}_p)$ with the notation $P_{kl0}, P_{kl1}, P_{kl2}, P_{kl3}$ of [5, Sec. 2]. If k is even then $P_{kl0} = C(l, \frac{k}{2}, 1, 0), P_{kl3} = C(l, \frac{k}{2}, 1, 1), P_{kl1} = C(l, \frac{k}{2} - 1, 5)$, and $P_{kl2} = C(l, \frac{k}{2} - 1, 5)^d$. If k is odd then $P_{kl0} = C(l, \frac{k-1}{2}, 2, 0), P_{kl3} = C(l, \frac{k-1}{2}, 2, 1), P_{kl1} = C(l, \frac{k-1}{2}, 3)$, and $P_{kl2} = C(l, \frac{k-1}{2}, 4)$. Therefore

$$\{C(i,j,1,\varepsilon), C(i,j,2,\varepsilon), C(i,j,3), C(i,j,4), C(i,j,5), C(i,0,5) \mid \varepsilon \in \{0,1\}, i,j \geq 1\}$$

is a sublist of the list consisting of all P_{kl0}, P_{kl3}, P_{kl1}, P_{kl2} for $k \geq 2, l \geq 1$. According to [5, Proposition 3.3], the only isomorphism between two distinct groups in the latter list is $P_{kl1} \cong P_{kl2}$, k even, which translates to $C(l, \frac{k}{2} - 1, 5) \cong C(l, \frac{k}{2} - 1, 5)^d$. However $C(l, \frac{k}{2} - 1, 5)^d \notin \mathcal{T}$.

Suppose $G, H \in \mathcal{T}$ are isomorphic. There is a single element of $\mathcal{T}$ of order 3, so by the preceding paragraph G or H is in $\{C(i,0,2,\varepsilon),\ C(i,0,5) \mid \varepsilon \in \{0,1\}, i \geq 1\}$. The only abelian groups in $\mathcal{T}$ are the $C(i,0,2,\varepsilon)$, and $C(i,0,2,0) \ncong C(i,0,2,1)$, leaving us with the possibility that $G, H \in \{C(i,0,5),\ C(i,1,1,\varepsilon)\}$. We saw in the proof of Theorem 6.8 that $C(i,0,5)$ and $C(i,1,1,1)$ are conjugate. Since $C(i,0,5)$ but not $C(i,1,1,0)$ has a cyclic normal subgroup of index 3, the proof is complete. □

Define $\{2,3\}$-subgroups $S(i,j,k,l,m,\eta)$ of $\mathrm{M}(3, \mathbb{F}_p)$, $1 \leq m \leq 4$, as follows:

$$S(i,j,k,l,m,\eta) = \langle T(i,j,m),\ dz_{k+1,2}^{\eta},\ z_{k,2},\ u_{l,2},\ w_{l,2} \rangle, \quad k,l \geq 0,\ \eta \in \{0,1\},$$

where

$$\begin{aligned} T(i,j,1) &= \begin{cases} C(i,j,1,0) & i,j \geq 1 \\ C & i = j = 0 \end{cases} \\ T(i,j,2) &= C(i,j,2,0) \qquad i \geq 1,\ \ j \geq 0 \\ T(i,j,m) &= C(i,j,m) \qquad 3 \leq m \leq 4,\ \ i,j \geq 1. \end{aligned}$$

The $S(i,j,k,l,m,\eta)$ are distinct for distinct values of the parameters $i, \ldots, \eta$.

Lemma 6.13. *Let G be a finite subgroup of $\mathrm{M}(3, \mathbb{K})$, $\mathbb{K}$ any field, such that $\pi G = S_3$. Then G has a unique subgroup H of index 2 such that $|H\colon A| = 3$ for some abelian normal subgroup A of H.*

Proof. We claim that H is the subgroup of G containing $A = \mathrm{D}(3, \mathbb{K}) \cap G$ and such that $\pi H = C$. Suppose $K \neq H$ is another subgroup of the same kind, with abelian normal subgroup B of index 3. Since $\pi K \trianglelefteq S_3$ and K is not diagonal

nor does it contain a subgroup of diagonal matrices of index 3, it follows that $\pi K = S_3$. Denote $A \cap K$ by A^*. We cannot have $A^*B = B$ because S_3 has no normal subgroup of index 3. Thus $A^*B = K$. But then S_3 is isomorphic to the abelian group $B/(B \cap A^*)$. □

Theorem 6.14. *A finite irreducible subgroup G of $\mathrm{M}(3, \mathbb{F}_p)$ such that $\pi G = S_3$ is $\mathrm{GL}(3, \mathbb{F}_p)$-conjugate to one and only one group $S(i, j, k, l, m, \eta)M$ where M is a finite S_3-submodule of $\mathrm{D}(3, \mathbb{F}_p)$ of $\{2, 3\}'$-order, and either M is nonscalar, or M is scalar and $l \geq 1$ or $j \geq 1$.*

Proof. By Theorem 6.2, G is $\mathrm{D}(3, \mathbb{F}_p)$-conjugate to $\langle c,\, dz,\, N_{\{2,3\}} \rangle N_{\{2,3\}'}$ where $N := \mathrm{D}(3, \mathbb{F}_p) \cap G$ and $z \in Z_2$, $z^2 \in N_2$. The choices for N_2 and $N_{\{2,3\}'}$ are given in Theorem 6.6(ii), and $\langle c,\, N_3 \rangle$ is one of the $T(i, j, m)$ appearing in the definitions of the $S(i, j, k, l, m, \eta)$. We ensure N is nonscalar, as required by Theorem 6.5, by stipulating that N_2, N_3, or $M = N_{\{2,3\}'}$ is nonscalar.

Suppose $(S(i, j, k, l, m, \eta)M)^x = S(i', j', k', l', m', \eta')M'$ for some $x \in \mathrm{GL}(3, \mathbb{F}_p)$. Then $M = M'$ by Lemma 6.10, and the equalities $i = i'$, $j = j'$, $k = k'$, $l = l'$, and $m = m'$ follow from Lemma 6.13, Theorem 6.5, and Theorem 6.12. By [11, Theorem 8.10(i)], x is monomial — the sole situation in which conceivably $x \notin \mathrm{M}(3, \mathbb{F}_p)$ involves conjugacy between $\langle C(i, 1, 1, 0),\, d,\, z_{k,2} \rangle$ and $\langle C(i, 1, 1, 0),\, dz_{k+1,2} \rangle$, groups which have more than one abelian normal subgroup with quotient S_3 (here $l = 0$ and M is scalar). But a Sylow 2-subgroup of the second group is $\langle dz_{k+1,2} \rangle$, whereas a Sylow 2-subgroup of the first group is noncyclic. So we are left to consider $\eta = 0$ and $\eta' = 1$, in which case

$$\langle d,\, z_{k,2},\, u_{l,2},\, w_{l,2} \rangle^x = \langle dz_{k+1,2},\, u_{l,2},\, w_{l,2} \rangle$$

for some $x \in \mathrm{M}(3, \mathbb{F}_p)$. Therefore $x^{1-d} \equiv z_{k+1,2} \bmod \langle z_{k,2},\, u_{l,2},\, w_{l,2} \rangle$, further implying that $\langle z_{k+1,2} \rangle \subseteq \mathrm{SL}(3, \mathbb{F}_p)$. This is absurd. Hence $\eta = \eta'$. □

At last we can list the absolutely irreducible subgroups of $\mathrm{M}(3, q)$.

Theorem 6.15. *Let G be an irreducible subgroup of $\mathrm{M}(3, \mathbb{F}_p)$ conjugate to a subgroup of $\mathrm{M}(3, q)$. Let α be a generator of $\mathsf{O}_3(\mathrm{GF}(q)^\times)$, $|\alpha| = 3^t$, and set $|\mathsf{O}_2(\mathrm{GF}(q)^\times)| = 2^s$.*

(i) *Suppose $\pi G = C$. Let $\mathcal{C}$ be as in Theorem 6.7. Then G is conjugate to a group in $\mathcal{M}'_{3,q}$, defined for $t \geq 1$ to be the list of all subgroups $G_3 G_{3'}$ of $\mathrm{M}(3, q)$, $G_{3'}$ a C-submodule of $\mathrm{D}(3, q)$ of order not divisible by 3, and G_3 one of*

$$\left.\begin{array}{ll} C, & G_{3'} \text{ nonscalar only} \\ C(i, j, 1, 0) & 1 \leq i \leq t \\ C(i, j, 1, 1) & 1 \leq i \leq t-1 \\ \langle c(\alpha, 1, 1),\, u_{j,3},\, w_{j,3} \rangle & \end{array}\right\} \; 1 \leq j \leq t$$

$$\left.\begin{array}{ll} C(i,j,2,0) & 1 \le i \le t \\ C(i,j,2,1) & 1 \le i \le t-1 \\ \langle c(\alpha,1,1),\, u_{j+1,3}^2 w_{j+1,3},\, u_{j,3},\, w_{j,3}\rangle & \end{array}\right\} \quad \begin{array}{l} 0 \le j \le t-1, \\ \textit{but } j \ge 1 \textit{ when} \\ G_{3'} \textit{ is scalar} \end{array}$$

$$\begin{array}{ll} C(i,j,3) & 1 \le i,j \le t-1 \textit{ or } i=j=t \\ C(i,j,4) & 1 \le i,j \le t-1 \\ C(i,j,5) & 1 \le i \le t-1,\ 0 \le j \le t-1, \textit{ but } j \ge 1 \textit{ when } G_{3'} \textit{ is scalar,} \end{array}$$

where $G_{3'} \in \mathcal{C}$ *when* G_3 *is* C, $C(i,j,1,0), C(i,j,2,0), C(i,j,3)$, *or* $C(i,j,4)$, *and* $G_{3'}$ *is unrestricted otherwise. If* $t = 0$ *then* $\mathcal{M}'_{3,q}$ *consists of the* $CG_{3'}$ *with* $G_{3'} \in \mathcal{C}$ *nonscalar.*

(ii) *Suppose* $\pi G = S_3$. *Then* G *is conjugate to a group in* $\mathcal{M}''_{3,q}$, *defined to be the list of all subgroups* $S(i,j,k,l,m,\eta)M$ *of* $\mathrm{M}(3,q)$, *where* M *is an* S_3*-submodule of* $\mathrm{D}(3,q)$ *of* $\{2,3\}'$*-order, and* $S(i,j,k,l,m,\eta)$ *is as defined before Lemma* 6.13, *with* $0 \le k,l \le s, \eta \in \{0,1\}, \eta = 0$ *if* $k = s$, *and the other parameters range as follows*:

$$\begin{array}{ll} m=1, & 1 \le i,j \le t \\ m=1, & i=j=0,\ M \textit{ nonscalar or } l \ge 1 \textit{ only} \\ m=2, & 1 \le i \le t,\ 0 \le j \le t-1, \textit{ but } j \ge 1 \textit{ if } M \textit{ is scalar and } l=0 \\ m=3, & 1 \le i,j \le t-1 \textit{ or } i=j=t \ge 1 \\ m=4, & 1 \le i,j \le t-1. \end{array}$$

(iii) $\mathcal{M}_{3,q} := \mathcal{M}'_{3,q} \cup \mathcal{M}''_{3,q}$ *consists of absolutely irreducible subgroups of* $\mathrm{M}(3,q)$.

(iv) *Distinct groups in* $\mathcal{M}_{3,q}$ *are not conjugate.*

Proof. (i) It suffices to assume $G = G_3 G_{3'}$ is in the list of Theorem 6.8. Clearly $G_{3'} \le \mathrm{D}(3,q)$, and if G_3 is normalized by S_3 then by Theorem 6.7 we may take $G_{3'} \in \mathcal{C}$. For some $i,j \ge 0$, $\langle z_{i,3},\, u_{j,3},\, w_{j,3}\rangle \le G$, and $i \le t$. Since a conjugate of G_3 lies in a Sylow 3-subgroup of $\mathrm{M}(3,q)$, and the latter has exponent 3^{t+1}, we have $|u_{j,3}| \le 3^{t+1}$, so $j \le t+1$. If $j = t+1$ then $u_{j,3}$ is conjugate to cm for some $m \in \mathrm{D}(3,q)$. But $\mathrm{tr}(cm) = 0$, and if $\omega_{j,3} + \omega_{j,3}^{-1} + 1 = 0$ then $j = 1$. Thus if $t \ge 1$ then $j \le t$. If $\mathrm{GF}(q)^\times$ has trivial Sylow 3-subgroup then $G_3 = C$ and $G_{3'}$ is nonscalar. From now on, $t \ge 1$.

If $G_3 = C(i,j,1,\varepsilon)$, $1 \le j \le t$, and $1 \le i \le t$ or $1 \le i \le t-1$ according as $\varepsilon = 0$ or $\varepsilon = 1$, respectively, then $G \le \mathrm{M}(3,q)$. However $C(t,j,1,1) \not\le \mathrm{M}(3,q)$. By Lemma 6.9, the diagonal subgroup of every other G is conjugate to a subgroup of $\mathrm{D}(3,q)$, so must also be in $\mathrm{D}(3,q)$. Since $C(i,t,2,\varepsilon)$ has an element $(\omega^2, \omega^{-1}, \omega^{-1})$, $\omega^3 = \alpha$, not in $\mathrm{D}(3,q)$, we insist $j < t$ if $G_3 = C(i,j,2,\varepsilon)$. For the same reason, if G_3 is $C(i,j,3)$ or $C(i,j,4)$ and $i \le t-1$, then $j \le t-1$, although $i = j = t$ is allowed for $G_3 = C(i,j,3)$. Suppose $G_3 = C(i,j,5)$, so that G_3 contains the diagonal subgroup of $C(i,j,2,\varepsilon)$. Therefore j cannot be t, and $i \le t-1$ too.

With parameter ranges as indicated, all groups are visibly in $\mathrm{M}(3,q)$ except for the $C(t,j,1,1)G_{3'}$ and $C(t,j,2,1)G_{3'}$. In each case here we conjugate by

$(1, \omega^{-1}, \omega^{-2})$ to get a group in $\mathrm{M}(3, q)$, generated by the same diagonal subgroup and $c(\alpha, 1, 1)$.

(ii) By Theorem 6.14, G is the product of some $S(i, j, k, l, m, \eta)$ and an S_3-submodule of $\mathrm{D}(3, \mathbb{F}_p)$ of $\{2, 3\}'$-order. It follows from Lemma 6.13 that the diagonal subgroup of G is in $\mathrm{D}(3, q)$, and thus $0 \leq k, l \leq s$. Now if $k = s$ and $\eta = 1$ then G contains the element $dz_{s+1,2}$ which has trace outside $\mathrm{GF}(q)$, so we exclude that pair of parameter values. The restrictions on i and j come from (i).

(iii) We reiterate that groups in $\mathcal{M}_{3,q}$ are irreducible over $\mathbb{F}_p$ by Theorem 6.5.

(iv) We appeal to Lemma 6.4 and Theorem 6.14 to discount conjugacy between different groups in $\mathcal{M}''_{3,q}$, or between a group in $\mathcal{M}''_{3,q}$ and one in $\mathcal{M}'_{3,q}$. Suppose $G, H \in \mathcal{M}'_{3,q}$ are conjugate. By Theorem 6.12, either $G_3 = H_3$, or $G_3, H_3 \in \{C(i, 1, 1, 1), C(i, 0, 5)\}$ and $G_{3'}, H_{3'}$ are nonscalar. Since $C(i, 1, 1, 1)$, $C(i, 0, 5)$ are certainly not $\mathrm{M}(3, \mathbb{F}_p)$-conjugate, by Lemma 6.9 and Theorem 6.11 we have $G_3^{\tilde{m}} = H_3 = G_3$ and $G_{3'}^{m} = H_{3'}$ for some $\tilde{m}, m \in \mathrm{M}(3, \mathbb{F}_p)$, $\pi\tilde{m} = \pi m$. If $\pi m \in C$ then $G_{3'} = H_{3'}$. If $\pi m \notin C$ then G_3^d is $\mathrm{D}(3, \mathbb{F}_p)$-conjugate to G_3, and so the diagonal subgroup of G_3 is an S_3-module. From the definitions it may then be seen that $G_3^d = G_3$. But in this case $G_{3'}, H_{3'} \in \mathcal{C}$, and distinct elements of $\mathcal{C}$ are not S_3-conjugate. □

Remark 6.16. The list of S_3-submodules of $\mathrm{D}(3, q)$ of $\{2, 3\}'$-order may be easily written down from Theorem 6.7.

We leave as an exercise the formulation of an equivalent to Theorem 6.15 for fields of characteristic 3, by employing Lemma 4.2 for projection C.

6.3. *The sublist* $\mathcal{PM}_{3,q}$

Theorem 6.17. *Let G be an absolutely irreducible* $\mathrm{GF}(q)$*-primitive* $\mathbb{F}_p$*-monomial subgroup of* $\mathrm{GL}(3, q)$*. Then G has an irreducible abelian normal subgroup.*

Proof. We invoke Theorem 4.3 several times. Observe that G has an abelian normal subgroup A where G/A is isomorphic to C or S_3. Suppose $G/A \cong C$. If A is scalar then G is abelian; but G is absolutely irreducible and so A is irreducible. Suppose $G/A \cong S_3$. If A is reducible then G has an abelian subgroup of index 2 containing A, which is not scalar; so A must be irreducible. □

Theorem 6.18. *Let α be a generator of* $\mathrm{GF}(q)^\times$*, and write $q - 1 = 3^t l, l$ coprime to 3. Denote the scalars of* $\mathrm{GL}(3, q)$ *by Z. Let A be the Singer cycle generated by b as in Theorem* 6.1*, and let a be the matrix whose ith row is the first row of $b^{(i-1)q}, 1 \leq i \leq 3$. Then it is valid to define $\mathcal{PM}_{3,q}$ to be the list of all groups*

$$\langle a, \hat{A} \rangle, \quad \langle a b^{3^{t-k} l}, \tilde{A} \rangle$$

where $\hat{A}$ ranges over the subgroups of A of order not dividing $3(q-1)$, $\tilde{A}$ ranges over the subgroups of A such that $\mathsf{O}_3(A) \not\leq \tilde{A}, |\tilde{A}|$ does not divide $q - 1, \mathsf{O}_3(\tilde{A} \cap Z) \neq 1$, and k is defined by $\mathsf{O}_3(\tilde{A} \cap Z) = \langle b^{(q^3-1)/3^k} \rangle$.

Proof. Heeding Theorem 6.17, we follow Short's prescription [22, Theorem 4.2.7] as in Theorem 5.3. □

6.4. *The sublist* $\mathcal{P}^\circ_{3,q}$

By Theorem 4.8(ii), $\mathcal{P}^\circ_{3,q}$ is nonempty only if $q \equiv 1 \bmod 3$, implying $p \neq 3$ and if $p = 2$ then $\log_2 q$ is even. Henceforth $p \geq 5$.

Corollary 4.9 tells us that a soluble primitive subgroup of $\mathrm{GL}(3, \mathbb{F}_p)$ has central quotient $T_L := (C_3 \times C_3) \rtimes L$ where L is an irreducible subgroup of $\mathrm{SL}(2,3)$, and the conjugation action of L on $C_3 \times C_3$ is the natural action of a subgroup of $\mathrm{SL}(2,3)$ on its underlying vector space. The possible isomorphism types for L are C_4, Q_8, and $\mathrm{SL}(2,3)$. Since, for each isomorphism type, there is a single conjugacy class of subgroups of $\mathrm{SL}(2,3)$ of that type, each choice of L determines a single isomorphism type of T_L. An easy exercise establishes that $T_{\mathrm{SL}(2,3)}$ has the following power-conjugate presentation:

$$\begin{aligned}\langle x_1, x_2, x_3, x_4, x_5, x_6 \mid\ & x_1^3 = 1,\ x_2^2 = x_3^2 = x_4,\ x_4^2 = x_5^3 = x_6^3 = 1,\\ & x_2^{x_1} = x_2x_3x_4,\ x_3^{x_1} = x_2,\ x_3^{x_2} = x_3x_4,\\ & x_5^{x_1} = x_5x_6^2,\ x_5^{x_2} = x_5x_6,\ x_5^{x_3} = x_6^2,\ x_5^{x_4} = x_5^2,\\ & x_6^{x_2} = x_5x_6^2,\ x_6^{x_3} = x_5,\ x_6^{x_4} = x_6^2\rangle\end{aligned}$$

with the usual convention that trivial conjugate relations are omitted (for example, $x_6^{x_1} = x_6$). We have $\langle x_2, x_3\rangle \cong Q_8$, $\langle x_2, x_3\rangle \rtimes \langle x_1\rangle \cong \mathrm{SL}(2,3)$, and $\langle x_5, x_6\rangle \cong C_3 \times C_3$ is the underlying GF(3)-space.

For each L, we determine first all isomorphism types of extensions of a scalar group Z by T_L; then, for each isomorphism type G (apart from those with a non-cyclic abelian normal subgroup), from its character table and knowledge of its automorphism group, we find the number of $\mathrm{GL}(3, \mathbb{F}_p)$-conjugacy classes of irreducible primitive subgroups of $\mathrm{GL}(3, \mathbb{F}_p)$ isomorphic to G. Finally we demonstrate explicitly the required number of linear groups in each case. We can assume the only primes dividing $|Z|$ are 2 or 3.

Note that $\mathrm{Aut}(Z) \times \mathrm{Aut}(T_L)$-action accounts for all possible isomorphisms between extensions of Z by T_L, because such an extension has center precisely Z (T_L has trivial center).

In the sequel we use the results of routine computations in Magma: Holt's algorithm [15] to determine Schur multipliers of permutation groups and the authors' package [12] to construct cocycles for central extensions of soluble groups.

First let $L = \langle x_2\rangle \cong C_4$. The derived subgroup of T_{C_4} is $C_3 \times C_3$ and its Schur multiplier has order 3. Suppose Z is a (nontrivial) 3-group. An extension of Z by T_{C_4} contains the (unique) Schur cover S of T_{C_4}: this can be seen in the usual fashion. By the Universal Coefficient Theorem, $H^2(T_{C_4}, Z) = \mathrm{Hom}(H_2(T_{C_4}), Z) = \mathrm{Hom}(C_3, Z) \cong C_3$. Denote the elements of $\mathrm{Hom}(H_2(T_{C_4}), Z)$ as $[\chi_i]$, $1 \leq i \leq 3$, $[\chi_1]$

trivial. We may write χ_i as $\mu_i\phi$ where ϕ is a 2-cocycle $T_{C_4}\times T_{C_4}\to H_2(T_{C_4})$ and $\mu_i\in \mathrm{Hom}(H_2(T_{C_4}),Z)$. Further, if θ is the inversion automorphism of Z then $\theta\mu_2=\mu_3$, so $[\chi_2]^\theta=[\chi_2^\theta]=[\theta\mu_2\phi]=[\chi_3]$. Consequently $[\chi_2]$, $[\chi_3]$ give rise to isomorphic extensions. The split extension of Z by T_{C_4} is forbidden here (by primitivity), and since χ_2 maps into the minimal subgroup of Z, an extension arising from $[\chi_2]$ contains a subgroup isomorphic to S, as claimed. A power-conjugate presentation for S is

$$\begin{aligned}\langle y_1,\, y_2,\, y_3,\, y_4,\, y_5 \mid\ & y_1^2=y_2,\ y_2^2=y_3^3=y_4^3=y_5^3=1,\\ & y_3^{y_1}=y_3y_4,\ y_3^{y_2}=y_3^2,\\ & y_4^{y_1}=y_3y_4^2y_5,\ y_4^{y_2}=y_4^2y_5^2,\ y_4^{y_3}=y_4y_5^2\rangle.\end{aligned}\tag{2}$$

Lemma 6.19. *The subgroups of* $\mathrm{GL}(3,\mathbb{F}_p)$ *isomorphic to* S *fall into three conjugacy classes.*

Proof. The automorphism group of S has three orbits in the set of faithful irreducible ordinary characters of S of degree 3. □

Let $\omega\in\mathbb{F}_p$ be a fixed primitive cube root of unity, and let c, $z:=z_{1,3}=(\omega,\omega,\omega)$, $w:=w_{1,3}=(1,\omega,\omega^{-1})$, $u:=u_{1,3}=(\omega,\omega^{-1},1)$ be as in Sec. 6.2. Define

$$v=\frac{1}{\omega-\omega^2}\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\1&\omega^2&\omega\end{pmatrix}.$$

Observe that $v\in\mathrm{SL}(3,\mathbb{F}_p)$ and $|v|=4$. (In the proof of Theorem 6.8, $(\omega-\omega^2)v$ was called m. The choice of v and other generators is suggested to us by [3, pp. 108–109].) We have the following relations involving c,w,u,z, and v:

$$z=uw^{-1},\quad u^c=w,\quad w^c=u^{-1}w^{-1},\quad c^v=w,\quad u^v=c^{-1}z,\quad w^v=c^{-1}.$$

Fix a square root $\iota\in\mathbb{F}_p$ of -1. Consider the three subgroups

$$S_1=\langle v,\, c,\, z,\, u,\, w\rangle,\quad S_2=\langle -v,\, c,\, z,\, u,\, w\rangle,\quad S_3=\langle \iota v,\, c,\, z,\, u,\, w\rangle$$

of $\mathrm{GL}(3,\mathbb{F}_p)$. Each of these groups is a split extension of $C(1,1,1,0)=\langle c,\, z,\, u,\, w\rangle$ (notation defined before Theorem 6.8) by a cycle of order 4. Thus $|S_i|=108$ for all i.

Remark 6.20. If H is a soluble absolutely irreducible $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(3,q)$ then by Theorem 4.8, $\mathrm{Fit}(H)$ is conjugate to a subgroup of $\mathrm{M}(3,\mathbb{F}_p)$. Indeed, if $|\mathsf{Z}(H)|=3^i$ then a Sylow 3-subgroup of $\mathrm{Fit}(H)$ is conjugate to $C(i,1,1,0)$.

Lemma 6.21. $S_1\cong S_2\cong S_3\cong S$.

Proof. Let $y_3=w$, $y_4=c^2u^2$, $y_5=z$, and $y_1=v$. It is readily checked that all relations in the power-conjugate presentation (2) for S hold in S_1. Since

$S_1 = \langle v, c^2u^2, z, w\rangle$ and $|S_1| = 108 = |S|$, we deduce that $S_1 \cong S$. The other two isomorphisms follow after replacing $y_1 = v$ by $y_1 = -v$ and $y_1 = \iota v$ respectively. □

Theorem 6.22. *Let $q \equiv 1$ mod 3. Let $\mathcal{L}$ be the list consisting of all groups*

$$\langle S_1,\, x\rangle, \quad \langle S_2,\, x\rangle,$$

and

$$\langle S_3,\, x\rangle \quad q \equiv 1 \text{ mod } 4 \text{ only},$$

as $\langle x\rangle$ runs over the set of distinct odd order scalar subgroups of $\mathrm{GL}(3,q)$ *such that the 3-part of $|x|$ is not 3. Every group in $\mathcal{L}$ is a soluble $\mathbb{F}_p$-primitive subgroup of* $\mathrm{GL}(3,q)$*, and distinct groups in $\mathcal{L}$ are not conjugate. An $\mathbb{F}_p$-primitive subgroup of* $\mathrm{GL}(3,q)$ *with central quotient T_{C_4} and odd order center is conjugate to a group in $\mathcal{L}$.*

Proof. $\mathrm{Fit}(S_i) = C(1,1,1,0)$ is absolutely irreducible, and each S_i is $\mathbb{F}_p$-primitive because its central quotient does not have a normal subgroup of index 3 or 6. Therefore each group in $\mathcal{L}$ is $\mathbb{F}_p$-primitive. Suppose $\langle S_i,\, x\rangle$ and $\langle S_j,\, x'\rangle$ are conjugate. Both groups have the same center $Z = \langle z,\, x\rangle = \langle z,\, x'\rangle$, and S_iZ_3 and S_jZ_3 are conjugate. By Theorem 4.8(iii), if $K, \tilde{K}$ are complements of $\mathrm{Fit}(S_iZ_3)$ in S_iZ_3 of order 4 then $KZ_3, \tilde{K}Z_3$ are conjugate; since $v \in \mathrm{SL}(3,\mathbb{F}_p)$ and $\det(\iota v) = -\iota$ and $\det(-v) = -1$, it follows that $i = j$.

If the 3-part of $|x|$ is 3 then $\langle S_i,\, x\rangle = \langle S_i,\, x'\rangle \in \mathcal{L}$, where x' is scalar of odd order whose 3-part is not 3. The restrictions on $|x|$ also mean that groups $\langle S_i,\, x\rangle$ in $\mathcal{L}$ are distinct for different values of i, x.

A subgroup of $\mathrm{GL}(3,\mathbb{F}_p)$ isomorphic to S_1 is conjugate to one and only one of S_1, S_2, or S_3 by the preceding and Lemmas 6.19, 6.21. Thus if $G \le \mathrm{GL}(3,q)$ is primitive over $\mathbb{F}_p$, has center of odd order, and central quotient T_{C_4}, then a conjugate $\bar{G}$ of G contains some S_i. Let $\mathsf{Z}(\bar{G}) = \langle x\rangle$. Then $\langle S_i,\, x\rangle/\langle x\rangle \cong T_{C_4}$ implies $\bar{G} = \langle S_i,\, x\rangle$. Since $\mathrm{tr}(\iota v) = \iota$, necessarily $q \equiv 1 \bmod 4$ if $i = 3$. □

Now suppose $|Z|$ is even. We then have $H^2(T_{C_4}, Z) = \mathrm{Ext}(C_4, Z_2) \times \mathrm{Hom}(C_3, Z_3)$. Let $[\psi\chi]$ be a 2-cocycle class in $H^2(T_{C_4}, Z)$, where $[\psi] \in \mathrm{Ext}(C_4, Z_2)$ and $[\chi] \in \mathrm{Hom}(C_3, Z_3) \cong C_3$. If $[\chi] = 0$ then a corresponding extension of Z by T_{C_4} has an abelian normal subgroup that is noncyclic (an extension of Z by $C_3 \times C_3$), so $[\chi] \neq 0$, by primitivity. As already observed, the two nontrivial possibilities for $[\chi]$ are related by the inversion automorphism of Z_3. Likewise, if 4 divides $|Z|$ then the two elements of $\mathrm{Ext}(C_4, Z_2)$ of order 4 are related by an automorphism of Z_2 (that fixes the cocycle class of order 2). We deduce that there are exactly two isomorphism types of extensions of Z by T_{C_4} if $|Z| \equiv 2 \bmod 4$, and exactly three types if 4 divides $|Z|$.

Let $H \le \mathrm{GL}(3,\mathbb{F}_p)$ be a primitive extension of Z by T_{C_4}. Suppose $|Z| \equiv 2 \bmod 4$. The two possible isomorphism types for H are distinguished by the fact

that one has a subgroup isomorphic to the Schur cover S of T_{C_4}, while the other does not. In the first case $H = S_1Z = S_2Z$ or $H = S_3Z$, up to conjugacy, and in the second case there exists $h \in H$ of order 8. Let $\nu \in \mathbb{F}_p$ be a primitive eighth root of unity, so that $\langle H, \nu\rangle$ has a subgroup isomorphic to S, and thus contains S_1Z or S_3Z up to conjugacy. Then H/Z is a subgroup of $\langle S_iZ, \nu\rangle/Z \cong T_{C_4} \times C_4$, $i = 1$ or 3, and there are two subgroups of this direct product that could be H/Z, which leads to the conclusion that H is conjugate to one of

$$\langle \nu v, c, u, Z\rangle, \quad \langle \nu^{-1}v, c, u, Z\rangle, \quad \langle \iota\nu v, c, u, Z\rangle, \quad \langle \iota\nu^{-1}v, c, u, Z\rangle.$$

The first and fourth of these groups coincide, as do the second and third. Define $v_2 \in \mathrm{SL}(3, \mathbb{F}_p)$ by

$$v_2 = \frac{1}{\omega - \omega^2}\begin{pmatrix} 1 & \omega & \omega \\ \omega^2 & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{pmatrix}.$$

Then $v^{v_2} = v^{-1}$, and v_2 normalizes $\langle c, u, Z\rangle$. Hence the first and second groups above are conjugate. Since $\mathrm{tr}(\nu v) = \nu$, either group is conjugate to a subgroup of $\mathrm{GL}(3, q)$ only if $q \equiv 1 \bmod 8$, in which case the group is actually in $\mathrm{GL}(3, q)$.

Suppose 4 divides $|Z|$. One isomorphism type of H (the one with cocycle that has a trivial Ext component) contains some S_i up to conjugacy, and since here $\iota \in Z$ there is a single $\mathrm{GL}(3, \mathbb{F}_p)$-conjugacy class of groups isomorphic to H, namely the one with representative $S_1Z = S_2Z = S_3Z$. For H of the other two isomorphism types, we mimic previous arguments to find that H is conjugate to one of

$$\langle \lambda v, c, u, Z\rangle, \quad \langle \lambda^2 v, c, u, Z\rangle$$

where λ is a scalar whose fourth power generates Z_2. Also these two groups are nonconjugate (because a Sylow 2-subgroup of one, $\langle \lambda v\rangle$, is cyclic, but a Sylow 2-subgroup of the other, $\langle \lambda^2 v, Z_2\rangle$, is noncyclic).

The following theorem collects together the various results for $L \cong C_4$.

Theorem 6.23. *Let $q \equiv 1$ mod 3, and fix a primitive eighth root of unity $\nu \in \mathbb{F}_p$. Define $\mathcal{P}^1_{3,q}$ to be the list of all groups*

$$\begin{array}{l}
\langle S_1, x\rangle \\
\langle S_1, x'\rangle \\
\langle S_1, x''\rangle \\
\langle S_2, x\rangle \\
\left.\begin{array}{l}\langle S_3, x\rangle \\ \langle S_3, x'\rangle\end{array}\right\} \ q \equiv 1 \ \textit{mod}\ 4 \ \textit{only} \\
\langle \nu v, c, u, x'\rangle \quad q \equiv 1 \ \textit{mod}\ 8 \ \textit{only} \\
\left.\begin{array}{l}\langle \lambda_{x''} v, c, u, x''\rangle \\ \langle \lambda^2_{x''} v, c, u, x''\rangle\end{array}\right\} \ q \equiv 1 \ \textit{mod}\ 16 \ \textit{and}\ \lambda_{x''} \in \mathrm{GF}(q) \ \textit{only}
\end{array}$$

where $\langle x\rangle$, $\langle x'\rangle$, $\langle x''\rangle$ *run over the distinct scalar subgroups of* $\mathrm{GL}(3,q)$ *such that* $|x|$ *is odd,* $|x'| \equiv 2 \bmod 4$, $|x''| \equiv 0 \bmod 4$, $\lambda_{x''} \in \mathbb{F}_p$ *is a fourth root of* x'', *and for groups* $\langle S_i, x\rangle$, $\langle S_i, x'\rangle$, $\langle S_i, x''\rangle$, *the* 3*-parts of* $|x|, |x'|, |x''|$ *are not* 3.

(i) *Every group in* $\mathcal{P}^1_{3,q}$ *is a soluble* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(3,q)$.
(ii) *Distinct groups in* $\mathcal{P}^1_{3,q}$ *are not conjugate.*
(iii) *An* $\mathbb{F}_p$*-primitive subgroup of* $\mathrm{GL}(3,q)$ *with central quotient* $(C_3 \times C_3) \rtimes C_4$ *is conjugate to a group in* $\mathcal{P}^1_{3,q}$.

The methods used above for $L \cong C_4$ may now be applied with equal effectiveness for $L \cong Q_8$ and $L \cong \mathrm{SL}(2,3)$. We briefly discuss vital ingredients of the construction in those cases and then present the resultant lists.

Let $L \cong Q_8$. As usual 3 divides $|Z|$. Observe that T_{Q_8} has pc-presentation

$$\begin{aligned}\langle x_2, x_3, x_4, x_5, x_6 \mid\ & x_2^2 = x_3^2 = x_4,\ x_4^2 = x_5^3 = x_6^3 = 1,\\ & x_3^{x_2} = x_3x_4,\ x_5^{x_2} = x_5x_6,\ x_5^{x_3} = x_6^2,\ x_5^{x_4} = x_5^2,\\ & x_6^{x_2} = x_5x_6^2,\ x_6^{x_3} = x_5,\ x_6^{x_4} = x_6^2\rangle\end{aligned}$$

with $\langle x_2, x_3\rangle \cong Q_8$. Relabel v as v_1, and let v_2 be as defined before Theorem 6.23. The mapping $x_2 \mapsto v_1$, $x_3 \mapsto v_2$ defines an isomorphism $\langle x_2, x_3\rangle \to \langle v_1, v_2\rangle$. We have $T_{Q_8}/T'_{Q_8} \cong C_2 \times C_2$ and $H_2(T_{Q_8}) \cong C_3$, so $H^2(T_{Q_8}, Z) \cong C_2 \times C_2 \times C_3$ if $|Z|$ is even, and $H^2(T_{Q_8}, Z) \cong C_3$ if $|Z|$ is odd. Further, $\mathrm{Aut}(Z) \times \mathrm{Aut}(T_{Q_8})$ action on $H^2(T_{Q_8}, Z)$ (discarding extensions with noncyclic abelian normal subgroups) yields two orbits in the former case and one in the latter, so we have either one or two possible isomorphism types of extensions of Z by T_{Q_8}, depending on whether $|Z|$ is odd or even.

There are two distinct conjugacy classes of subgroups of $\mathrm{GL}(3,\mathbb{F}_p)$ isomorphic to the Schur cover S of T_{Q_8}. (Cf. Lemma 6.17. Again the cover is unique, since $|T_{Q_8}/T'_{Q_8}|$ and $|H_2(T_{Q_8})|$ are coprime.) One of these is represented by the subgroup

$$S_1 = \langle v_1, v_2, c, z, u, w\rangle$$

of $\mathrm{SL}(3,\mathbb{F}_p)$. Note that $v_1^{v_3} = v_2$ where

$$v_3 = (\varepsilon\omega^{-1}, \varepsilon, \varepsilon),$$

$\varepsilon \in \mathbb{F}_p$ a cube root of ω^2. The other class is represented by

$$S_2 = \langle v_1, -v_2, c, z, u, w\rangle.$$

A Sylow 2-subgroup of S_1, but not of S_2, lies in $\mathrm{SL}(3,\mathbb{F}_p)$, so S_1 and S_2 are certainly nonconjugate.

Let H be a primitive extension of Z in $\mathrm{GL}(3,\mathbb{F}_p)$ such that $H/Z \cong T_{Q_8}$. If $|Z|$ is odd then H contains a conjugate of S_1 or S_2, so that H is conjugate to S_1Z or S_2Z. Suppose $|Z|$ is even. Here H splits over its Hall $2'$-subgroup, with complement H_2 that is an extension of Z_2 by Q_8. One isomorphism type of H contains S_1 or S_2, and so contains both; hence $H = S_1Z$. Suppose H has one of the other isomorphism types; then H does not have a subgroup conjugate to S_1 or S_2, meaning that H_2

does not split over Z_2. We can discover the structure of H by considering cocycle classes in $\mathrm{Ext}(Q_8/Q_8', Z_2)$. Let τ be a scalar whose square generates Z_2, so that $\langle H, \tau\rangle$ contains S_1. Looking at $\langle H, \tau\rangle/Z \cong T_{Q_8} \times C_2$, we recognize

$$\langle v_1\tau, v_2, c, u, Z\rangle, \quad \langle v_1, v_2\tau, c, u, Z\rangle, \quad \langle v_1\tau, v_2\tau, c, u, Z\rangle$$

as candidates for H. Using $v_1^{v_3} = v_2$ and $v_2^{v_3} = v_1 v_2^{-1}$, we see that all three groups are conjugate.

Theorem 6.24. *Let $q \equiv 1$ mod 3. Define $\mathcal{P}^2_{3,q}$ to be the list of all groups*

$$\begin{array}{ll}
\langle S_1, x\rangle & \\
\langle S_2, x\rangle & \\
\langle S_1, x'\rangle & \\
\langle \tau_{x'} v_1, v_2, c, u, x'\rangle & q \equiv 1 \text{ mod } 4 \text{ and } \tau_{x'} \in \mathrm{GF}(q) \text{ only}
\end{array}$$

where $\langle x\rangle$, $\langle x'\rangle$ run over the distinct odd order and even order scalar subgroups of $\mathrm{GL}(3,q)$, *respectively, $\tau_{x'} \in \mathbb{F}_p$ is a square root of x', and for groups $\langle S_i, x\rangle$, $\langle S_i, x'\rangle$, the 3-parts of $|x|$, $|x'|$ are not 3.*

(i) *Every group in $\mathcal{P}^2_{3,q}$ is a soluble $\mathbb{F}_p$-primitive subgroup of* $\mathrm{GL}(3,q)$.
(ii) *Distinct groups in $\mathcal{P}^2_{3,q}$ are not conjugate.*
(iii) *An $\mathbb{F}_p$-primitive subgroup of* $\mathrm{GL}(3,q)$ *with central quotient $(C_3 \times C_3) \rtimes Q_8$ is conjugate to a group in $\mathcal{P}^2_{3,q}$.*

Finally, let $L \cong \mathrm{SL}(2,3)$. Since $T_{\mathrm{SL}(2,3)}/T'_{\mathrm{SL}(2,3)} \cong H_2(T_{\mathrm{SL}(2,3)}) \cong C_3$, we can assume for the moment that Z is a 3-group, so $H^2(T_{\mathrm{SL}(2,3)}, Z) \cong C_3 \times C_3$. There are three distinct isomorphism types for a primitive extension H of Z in $\mathrm{GL}(3,\mathbb{F}_p)$ such that $H/Z \cong T_{\mathrm{SL}(2,3)}$. In particular we have the following three pairwise non-isomorphic Schur covers of $T_{\mathrm{SL}(2,3)}$ in $\mathrm{GL}(3,\mathbb{F}_p)$:

$$S_1 = \langle v_1, v_2, v_3, c, z, u, w\rangle, \quad S_2 = \langle v_1, v_2, \nu v_3, c, z, u, w\rangle,$$
$$S_3 = \langle v_1, v_2, \nu^2 v_3, c, z, u, w\rangle$$

where $\nu \in \mathbb{F}_p$ is a cube root of z. Any Schur cover of $T_{\mathrm{SL}(2,3)}$ in $\mathrm{GL}(3,\mathbb{F}_p)$ is conjugate to some S_i. Suppose $|Z| = 3^i, i \geq 1$, and let x be a generator of Z. Let ν_i be a scalar of 3-power order such that $\nu_i^3 = x^{1-2.3^{i-1}}$ (thus $\nu_i \notin Z$), and define

$$G(i,1) = \langle v_1, v_2, v_3, c, x, u, w\rangle, \quad G(i,2) = \langle v_1, v_2, \nu_i v_3, c, x, u, w\rangle,$$
$$G(i,3) = \langle v_1, v_2, \nu_i^2 v_3, c, x, u, w\rangle.$$

Note that $G(1,j) = S_j$.

Theorem 6.25. *Let $q \equiv 1$ mod 3. A primitive absolutely irreducible subgroup G of* $\mathrm{GL}(3,q)$ *with center $Z = \langle x\rangle$ of 3-power order and central quotient $T_{\mathrm{SL}(2,3)}$ is* $\mathrm{GL}(3,\mathbb{F}_p)$*-conjugate to $G(i,j)$ for a unique pair of values (i,j).*

Proof. We have already dealt with the case $i = 1$, so let $i \geq 2$. From our cohomological deliberations we know that either (a conjugate of) G contains some S_i,

or G has an element cubing to x or x^2, modulo Z^3. In the first case $G = G(i,1)$; note that $G(i,1)$ for $i \geq 2$ contains all the S_js. Otherwise, G/Z is a subgroup of $\langle S_j Z, \nu_i \rangle / Z \cong \mathrm{SL}(2,3) \times C_3$ for some j. We can take $j = 1$. Since $\mathrm{SL}(2,3)$ has a unique subgroup of index 3, there are two choices for G, and these are precisely $G(i,2)$, $G(i,3)$. □

Corollary 6.26. *Let $q \equiv 1$ mod 3, and let 3^t be the largest power of 3 dividing $q-1$. Define $\mathcal{P}^3_{3,q}$ to be the list of all groups*

$$\begin{array}{ll} \langle G(i,1), x \rangle & q \equiv 1 \text{ mod } 9 \text{ only} \\ \langle G(i,2), x \rangle & \varepsilon\nu_i \in \mathrm{GF}(q) \text{ only} \\ \langle G(i,3), x \rangle & \varepsilon\nu_i^2 \in \mathrm{GF}(q) \text{ only} \end{array}$$

where $1 \leq i \leq t$, and $\langle x \rangle$ ranges over the scalar subgroups of $\mathrm{GL}(3,q)$ of $3'$-order.

(i) *Every group in $\mathcal{P}^3_{3,q}$ is a soluble $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(3,q)$.*
(ii) *Distinct groups in $\mathcal{P}^3_{3,q}$ are not conjugate.*
(iii) *An $\mathbb{F}_p$-primitive subgroup of $\mathrm{GL}(3,q)$ with central quotient $(C_3 \times C_3) \rtimes \mathrm{SL}(2,3)$ is conjugate to a group in $\mathcal{P}^3_{3,q}$.*

Remark 6.27. Groups in $\mathcal{P}^3_{3,q}$ are pairwise nonisomorphic.

Theorem 6.28. *If $q \equiv 1$ mod 3 then $\mathcal{P}^1_{3,q} \cup \mathcal{P}^2_{3,q} \cup \mathcal{P}^3_{3,q}$ is a list $\mathcal{P}^\circ_{3,q}$ of the soluble absolutely irreducible $\mathbb{F}_p$-primitive subgroups of $\mathrm{GL}(3,q)$; if $q \not\equiv 1$ mod 3 then no such groups exist.*

This completes our listing of the soluble irreducible subgroups of $\mathrm{GL}(3,q)$ for all odd q.

7. Concluding Remarks

Lists of generating sets for our groups are publicly available as MAGMA procedures. These procedures, which encode the generating sets and constructions presented here, take as input the degree and field size and return the relevant list of groups.

The conjugating element constructed by the rewriting algorithm of Glasby and Howlett [14] depends on various random selections; hence the rewritten group returned may vary up to conjugacy. In all other respects the outcome of our procedures — including the ordering of the groups in the list — is completely determined.

In Table 1 we report the time t in CPU seconds to construct all k conjugacy classes of soluble irreducible subgroups of $\mathrm{GL}(3,q)$ using MAGMA V2.10 on an 800 MHz processor.

We have taken steps to ensure that our lists are accurate. For sufficiently "small" finite fields $\mathbb{E}$, we can compute directly with MAGMA all irreducible subgroups of $\mathrm{GL}(n,\mathbb{E})$ for $n = 2, 3$, and determine whether two given subgroups are conjugate.

Table 1. Number of soluble irreducible subgroups of $\mathrm{GL}(3, q)$.

q	k	t
5	22	0.01
5^4	2274	6
5^5	520	0.1
5^{10}	29416	27
5^{15}	62528	95
17^5	362	1
97^5	61032	105

For all prime powers up to 100, we established a complete correspondence between our lists and the results of these direct computations. We also obtained (numerical) agreement between our results and those of [7] and its extension.

Further, we have compared our lists with Suprunenko's classification [24, Theorem 6, p. 167] of the maximal irreducible soluble subgroups of $\mathrm{GL}(n, q)$, $n \leq 3$.

- Up to conjugacy, $\mathrm{GL}(n, q)$ has a single imprimitive maximal irreducible soluble subgroup, namely $\mathrm{M}(n, q)$. Suprunenko's $G_{2,1}$ is conjugate to $H(t-1, t-1, 3)G_{2'}$ or $\langle a, (1, -1)\rangle G_{2'}$ as defined in Theorem 5.2, whereas $G_{3,1}$ is conjugate to a group defined in Theorem 6.15: either $S(t, t, s, s, 1, 0)M$ if $t = 0$, or $S(t, t, s, s, 3, 0)M$ if $t \geq 1$; both $G_{2'}$ and M have maximal order. The isomorphism type is $C_{q-1}^{(n)} \rtimes S_n$.
- There are two kinds of primitive maximal irreducible soluble subgroups of $\mathrm{GL}(n, q)$. One of these is the normalizer of a Singer cycle: Suprunenko's $G_{2,2}$ and $G_{3,2}$ are the maximal order groups in $\mathcal{PM}_{n,q}$ defined in Theorems 5.3 and 6.18. The isomorphism type is $C_{q^n-1} \rtimes C_n$.
- The second kind of primitive maximal irreducible soluble subgroup of $\mathrm{GL}(n, q)$ is absolutely irreducible. Suprunenko's $G_{2,3}$ and $G_{3,3}$ are the maximal order groups in $\mathcal{P}^2_{2,q}$ and $\mathcal{P}^3_{3,q}$ defined in Theorem 5.8 and Corollary 6.26 respectively. The isomorphism types are stated there.

Our extensive cross-referencing to Short [22] facilitates a similar comparison with his (corrected) lists. Once again these coincide with ours.

Acknowledgements

We thank the referees for useful comments and suggestions on the content and exposition. This work was supported in part by the Marsden Fund of New Zealand via grant UOA124.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984) 469–514.

[2] Z. Bácskai, Finite irreducible monomial groups of small prime degree, Ph.D. thesis, Australian National University (1999).
[3] H. F. Blichfeldt, *Finite Collineation Groups* (University of Chicago Press, 1917).
[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235–265.
[5] S. B. Conlon, p-groups with an abelian maximal subgroup and cyclic center, *J. Aust. Math. Soc. Ser. A* **22** (1976) 221–233.
[6] J. D. Dixon, *The Structure of Linear Groups* (Van Nostrand-Reinhold, 1971).
[7] B. Eick and B. Höfling, The solvable primitive permutation groups of degree at most 6560, *LMS J. Comput. Math.* **6** (electronic) (2003) 29–39.
[8] W. Feit, The current situation in the theory of finite simple groups, *Actes du Congrès International des Mathématiciens* (Nice, 1970), *Tome 1* (Gauthier-Villars, Paris, 1971), pp. 55–93.
[9] D. L. Flannery, The finite irreducible linear 2-groups of degree 4, *Mem. Amer. Math. Soc.* **129**(613) (American Mathematical Society, 1997).
[10] D. L. Flannery, The finite irreducible monomial linear groups of degree 4, *J. Algebra* **218**(2) (1999) 436–469.
[11] D. L. Flannery, Irreducible monomial linear groups of degree four over finite fields, *Int. J. Algebra Comput.* **14**(3) (2004) 253–294.
[12] D. L. Flannery and E. A. O'Brien, Computing 2-cocycles for central extensions and relative difference sets, *Comm. Algebra* **28** (2000) 1935–1955.
[13] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.3 (2002). http://www.gap-system.org
[14] S. P. Glasby and R. B. Howlett, Writing representations over minimal fields, *Comm. Algebra* **25**(6) (1997) 1703–1711.
[15] D. F. Holt, The calculation of the Schur multiplier of a permutation group, in *Computational Group Theory*, Durham, 1982 (Academic Press, London, New York, 1984), pp. 307–318.
[16] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, 1967).
[17] B. Huppert and N. Blackburn, *Finite Groups II* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).
[18] I. M. Isaacs, *Character Theory of Finite Groups* (Dover, 1994).
[19] G. Karpilovsky, *Projective Representations of Finite Groups* (Marcel Dekker, 1985).
[20] L. G. Kovács, Some representations of special linear groups, The Arcata Conference on Representations of Finite Groups, Arcata, Calif., 1986, *Proc. Sympos. Pure Math.* **47**(2) (1987) 207–218.
[21] R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter Expositions in Mathematics 14 (Walter de Gruyter & Co., 1994).
[22] M. W. Short, The primitive soluble permutation groups of degree less than 256, *Lecture Notes in Math.* **1519** (Springer-Verlag, 1992).
[23] D. A. Suprunenko, Soluble and nilpotent linear groups, *Transl. Math. Monogr.*, Vol. 9 (American Mathematical Society, Providence, Rhode Island, 1963).
[24] D. A. Suprunenko, Matrix groups, *Transl. Math. Monogr.*, Vol. 45 (American Mathematical Society, Providence, Rhode Island, 1976).