

# LINEAR GROUPS OF SMALL DEGREE OVER FINITE FIELDS

D. L. FLANNERY AND E. A. O'BRIEN

ABSTRACT. We classify soluble irreducible linear groups of degree 2 and 3 over a finite field up to conjugacy in the relevant general linear group. We provide electronic access to the resulting classification.

## 1. INTRODUCTION

In this paper we construct parametrised lists of soluble irreducible linear groups of degree 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, describable in terms of a string of integer parameters. 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, §8.4, 8.5]), we argue that our work is a considerable 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 (faithful) 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 (small) prime degree and degree four over finite fields. We were originally motivated by the problem of classifying soluble primitive permutation groups as in [22]. Indeed, 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 (greater than 3).

The books [23, 24] by D. A. Suprunenko contain much pioneering work on classification of soluble linear groups; for example, in [24, §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 his monograph [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 identified by Alexander Hulpke, two conjugacy classes of monomial subgroups are missing from [22, Theorem 3.5.2].

---

This work was supported in part by the Marsden Fund of New Zealand via grant UOA124.  
*2000 Mathematics Subject Classification:* Primary 20H30, Secondary 20C15

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 the insoluble groups. Moreover, our approach may be applied successfully to list the soluble groups in degree 3.

Again motivated by classification of soluble primitive permutation groups, Eick & 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 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 & Höfling requires explicit solutions to conjugacy problems, whose inherent complexity grow 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 database of parametrised presentations for the groups. The database is designed for MAGMA [4]; however the data can be incorporated into other computer algebra systems. The construction of the list for a specified degree and finite field is very fast. We report on this in more detail in Section 6.

## 2. 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  $\varsigma$ ,  $M_\varsigma := \mathrm{O}_\varsigma(M)$ . Hence  $M_\varsigma$  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  $\mathrm{GL}(n, \mathbb{K})$ . If  $\mathbb{K}$  has finite order  $k$  then “ $k$ ” replaces “ $\mathbb{K}$ ” in this notation. The projection homomorphism  $\mathrm{M}(n, \mathbb{K}) \rightarrow S_n$  defined by  $ds \mapsto s$ ,  $d \in \mathrm{D}(n, \mathbb{K})$ ,  $s \in S_n$ , will be denoted  $\pi$ .

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 complete and irredundant classification of linear groups all of a certain specified kind, with respect to conjugacy in the ambient general linear group.

## 3. 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  $\mathrm{GL}(n, q)$ -normalisers, 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 & 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  $d^3|\mathbb{E} : \mathbb{K}|$ . We use our 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, §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] have overlapping features, they differ in several key respects.

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.

**Lemma 3.1.** (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  $\pi G$  is cyclic of order  $n$ , generated by  $c = (12 \dots n)$ . Choose  $g \in G$  with  $\pi g = c$ , and let  $\zeta \in \mathbb{K}$  be an  $n$ th 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  $\zeta^{-1}c^{-1}g = (a_1, a_2, \dots, a_n)$  and

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

then  $g^w = \zeta c$  as desired. □

**Proposition 3.2.** *Assume the hypotheses of Lemma 3.1. Suppose  $G$  is finite and  $\mathbb{K}$  has 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 3.1,  $G$  is conjugate to  $\langle \zeta c, \mathrm{D}(n, \mathbb{K}) \cap G \rangle$ , where  $\zeta$  is a scalar whose  $n$ th 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  $3$  are normalisers of Singer cycles.

**Proposition 3.3.** *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. In particular, 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.* 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  $\mathrm{GL}(3, q)$ .

**Proposition 3.4.** *Let  $G$  be a subgroup of  $\mathrm{GL}(n, q)$ . Then there exists  $\hat{G} \leq \mathrm{SL}(n, \mathbb{F}_p)$  such that  $G/Z(G) \cong \hat{G}/Z(\hat{G})$ . 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  $P \in \{\text{irreducible, absolutely irreducible, } \mathbb{K}\text{-primitive}\}$ ,  $\mathbb{K}$  a subfield of  $\mathbb{F}_p$  containing  $\mathrm{GF}(q)$ .

*Proof.* Suppose first that  $n \neq p$ . Let  $\bar{m}$  be the order of  $q \bmod n$ . If  $n$  and  $q - 1$  are coprime then  $n$  divides  $(q^{\bar{m}} - 1)/(q - 1)$ , and thus  $\mathrm{GF}(q^{\bar{m}})$  contains  $n$ th roots of every element of  $\mathrm{GF}(q)$ . If  $q \equiv 1 \pmod n$  then  $n$  divides  $(q^n - 1)/(q - 1)$ , so  $\mathrm{GF}(q^n)$  contains all the  $n$ th roots. Of course the  $n$ th 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  $n \leq 4$  then the first three components of this union consist entirely of soluble groups. We divide  $\mathcal{P}_{n,q}$  into two sublists  $\mathcal{P}_{n,q}^\circ$  and  $\mathcal{P}_{n,q}^\bullet$  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 3.5.** *Let  $G$  be a soluble primitive subgroup of  $\mathrm{GL}(n, \mathbb{F}_p)$ . Then*

- (i)  $\mathrm{Fit}(G)$  is irreducible,
- (ii)  $\mathrm{Fit}(G)/Z(G) \cong C_n \times C_n$ ,
- (iii)  $\mathrm{Fit}(G)/Z(G)$  is self-centralising in  $G/Z(G)$ ,
- (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  $Z(G) = Z$ . 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  $G$ -centraliser of  $F$  is  $Z(F)$ , and, since  $G$  is nonabelian,  $F \neq Z$ . Thus (i) is a consequence of Proposition 3.3. For (ii)–(iv), see [24, §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  $O_n(G/F) = 1$  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  $\theta_h: F/Z \rightarrow Z$  by  $\theta_h: gZ \mapsto [g, h]$ . If  $p = n$  then  $\theta_h$  is trivial, which yields the contradiction that  $F$  is abelian. □

*Remark.* In Theorem 3.5,  $\mathrm{Fit}(G)/Z(G)$  is the unique minimal normal subgroup of  $G/Z(G)$ . Thus  $G/Z(G)$  is centreless.

**Proposition 3.6.** *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)  *$|\mathrm{Z}(G)|$  is divisible by  $n$ .*
- (iii)  *$G/\mathrm{Z}(G)$  splits over  $\mathrm{Fit}(G)/\mathrm{Z}(G)$ , and all complements of  $\mathrm{Fit}(G)/\mathrm{Z}(G)$  in  $G/\mathrm{Z}(G)$  are conjugate.*

*Proof.* We use Theorem 3.5 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  $Z := \mathrm{Z}(G) < \mathrm{D}(n, \mathbb{F}_p) \cap \bar{F}$  and so  $1 < |\bar{F} : \mathrm{D}(n, \mathbb{F}_p) \cap \bar{F}| \leq n^2$ . Since  $\bar{F}$  is irreducible,  $\mathrm{D}(n, \mathbb{F}_p) \cap \bar{F} \neq Z$ , 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  $\mathrm{Z}(C/Z) \cap F/Z$  is a nontrivial normal subgroup of  $G/Z$  in  $F/Z$ , but  $F/Z$  is minimal normal and self-centralising in  $G/Z$ . Hence  $H^i(G/F, F/Z) = 0$  as required.  $\square$

**Corollary 3.7.** *If  $G$  is a finite soluble primitive subgroup of  $\mathrm{GL}(n, \mathbb{F}_p)$  then  $G/\mathrm{Z}(G) \cong (C_n \times C_n) \rtimes H$  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  $\mathcal{P}_{3,q}^\bullet$ , an arduous task as evidenced by [8, Theorem 8.4.2]. We include  $\mathcal{P}_{2,q}^\bullet$  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 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 Dering-Noether Theorem [17, 1.22, p.26]. Let  $\mathbb{K}$  be a field,  $n$  any positive integer, and suppose  $G, H$  are finite subgroups of  $\mathrm{GL}(n, \mathbb{K})$  such that  $G, H$  are conjugate in  $\mathrm{GL}(n, \mathbb{L})$  for an extension field  $\mathbb{L}$  of  $\mathbb{K}$ . Then  $G$  and  $H$  are conjugate in  $\mathrm{GL}(n, \mathbb{K})$ .

#### 4. DEGREE 2

Short [22, Chapters 3–5] describes how to list the soluble irreducible subgroups of  $\mathrm{GL}(2, q)$ . His results were not generally implemented, although lists for  $\mathrm{GL}(2, p)$  where  $p^2 < 256$  form part of the library “Irredsol” 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 degrees.

##### 4.1. The sublist $\mathcal{A}_{2,q}$ .

**Lemma 4.1.** *Let  $\alpha$  be a generator of  $\text{GF}(q^2)^\times$ , 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  $\text{GL}(2, q)$  of order  $r$ . An irreducible abelian subgroup of  $\text{GL}(2, q)$  is conjugate to  $A(r)$  for some  $r$ .*

*Proof.* See [22, §2.3]. As  $b$  is the companion matrix of  $x^2 - (\alpha + \alpha^q)x + \alpha^{q+1} \in \text{GF}(q)[x]$ , which has roots  $\alpha, \alpha^q$  over  $\mathbb{F}_p$ ,  $b$  is  $\text{GL}(2, \mathbb{F}_p)$ -conjugate to  $(\alpha, \alpha^q)$ . Hence  $|b| = q^2 - 1$  and  $\langle b \rangle$  is an irreducible subgroup of  $\text{GL}(2, q)$ , by Maschke's Theorem.  $\square$

**4.2. The sublist  $\mathcal{M}_{2,q}$ .** This section covers the same ground as [22, Chapter 3] but avoids the error of [22, Theorem 3.5.2].

To list the absolutely irreducible subgroups of  $\text{M}(2, q)$  we apply results from [11]. We first assume that  $p$  is odd. Let  $a$  be the nontrivial  $2 \times 2$  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

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

**Theorem 4.2.** *Let  $G$  be an irreducible subgroup of  $\text{M}(2, \mathbb{F}_p)$  conjugate to a subgroup of  $\text{M}(2, q)$ . Then  $G$  is conjugate to  $G_2 \rtimes G_{2'}$  for some 2-subgroup  $G_2$  of  $\text{M}(2, q)$ , and odd order subgroup  $G_{2'}$  of  $\text{D}(2, q)$  normal in  $\text{M}(2, q)$ .*

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

$$\begin{array}{ll} H(i, j, 1) & 0 \leq i \leq t-1, 1 \leq j \leq t-1 \\ H(i, j, 2) & 0 \leq i \leq t-2, 1 \leq j \leq t-1 \\ \langle a(\alpha, 1), w_j \rangle & 1 \leq j \leq t-1 \\ H(i, j, 3) & 0 \leq i \leq t-2, 1 \leq j \leq t-2 \\ H(t-1, t-1, 3) & \end{array}$$

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

$$\begin{array}{ll} \langle a \rangle & \\ H(i, j, 1) & 0 \leq i, j \leq t-1 \\ H(i, j, 2) & 0 \leq i \leq t-2, 0 \leq j \leq t-1 \\ \langle a(\alpha, 1), w_j \rangle & 0 \leq j \leq t-1 \\ H(i, j, 3) & 0 \leq i, j \leq t-2 \\ H(t-1, t-1, 3) & \end{array}$$

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

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

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

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

$$\begin{aligned} &\langle a \rangle \\ &\langle a, (-1, -1) \rangle \\ &\langle a(1, -1) \rangle \\ &\langle a, (1, -1) \rangle. \end{aligned}$$

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

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

(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  $M(2, q)$ . Although  $H(t-1, j, 2) \not\leq GL(2, q)$ ,  $H(t-1, j, 2)^{w_{t+1}} = \langle a(\omega_{t-1}, 1), w_j \rangle \leq M(2, q)$ .

Now suppose  $G_2 = H(i, j, 3)$ . If  $i, j \leq t-2$  or  $i = j = t-1$  then  $G_2 \leq M(2, q)$ . However, the hypotheses  $\text{tr}(G_2) \subseteq GF(q)$  and (a)  $i \leq t-2$ ,  $j = t-1$ , or (b)  $i = t-1$ ,  $1 \leq j \leq t-2$ , lead to the contradiction  $\omega_t \in GF(q)$ : 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  $D(2, q)$  if  $G_2G_{2'}$  has a conjugate in  $M(2, q)$ . 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  $M(2, q)$ . 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  $D(2, q)$ . 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  $M(2, q)$ , and this group is  $D(2, \mathbb{F}_p)$ -conjugate to  $\langle a(1, -1) \rangle$ .

A group  $G_2G_{2'}$  listed in this theorem is a conjugate of a group listed in [11, Theorem 5.1], so groups appear irredundantly by [11, Theorem 5.3].  $\square$

If  $p \neq 2$  then we take  $\mathcal{M}_{2,q}$  to be the list of all groups  $G_2G_{2'}$  as specified in Theorem 4.2. The odd order normal subgroups  $N$  of  $M(2, q)$  contained in  $D(2, q)$  are easily found; cf. [11, Remark 5.2]. For any prime  $p$  let  $Z$  denote the scalars of  $D(2, \mathbb{F}_p)$  and set  $W = D(2, \mathbb{F}_p) \cap SL(2, \mathbb{F}_p)$ . 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  $N \leq (Z \cap D(2, q)) \times (W \cap D(2, q))$ . Let  $\omega$  be a generator of  $GF(q)^\times$  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  $(\omega_r^i, \omega_r^i), (\omega_r^i, \omega_r^{-r^i})$  respectively. Then  $N_r$  is one of the  $r$ -subgroups of  $\langle z_{i,r}, w_{j,r} \rangle$  of  $D(2, q)$ ,  $0 \leq i, j \leq s$ .

If  $p = 2$  then, by Proposition 3.2, groups in  $\mathcal{M}_{2,q}$  are of the form  $\langle a, N \rangle$  where  $N$  is a nonscalar odd order normal subgroup of  $M(2, q)$  in  $D(2, q)$ . It is straightforward to prove that if  $N \neq \bar{N}$  then  $\langle a, N \rangle$  and  $\langle a, \bar{N} \rangle$  are not  $GL(2, q)$ -conjugate.

**4.3. The sublist  $\mathcal{PM}_{2,q}$ .** In contrast to Section 4.2, it would be arduous to recognise  $\mathcal{PM}_{2,q}$  within a list of the finite irreducible subgroups of  $M(2, \mathbb{F}_p)$ . Instead we use Short's classification [22] of prime degree primitive metacyclic linear groups over finite fields.

**Proposition 4.3.** *Let  $\alpha$  be a generator of  $GF(q)^\times$ , and suppose  $q - 1 = 2^t l$ ,  $l$  odd. Denote the scalars of  $GL(2, q)$  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 Lemma 4.1. Then it is valid to define  $\mathcal{PM}_{2,q}$  to be the list of all groups

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

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  $O_2(A) \not\leq \tilde{A}$ ,  $|\tilde{A}|$  does not divide  $q - 1$ ,  $O_2(\tilde{A} \cap Z) \neq 1$ , and  $k$  is defined by  $O_2(\tilde{A} \cap Z) = \langle b^{(q^2 - 1)/2^k} \rangle$ .

*Proof.* This proposition paraphrases [22, Theorem 4.2.7]. As defined above  $\mathcal{PM}_{2,q}$  consists of pairwise nonconjugate primitive subgroups of  $GL(2, q)$ . An element of this list is  $\mathbb{F}_p$ -monomial because it has a nonscalar abelian normal subgroup. By Proposition 3.3, an  $\mathbb{F}_p$ -monomial primitive subgroup of  $GL(2, q)$  normalises an irreducible abelian subgroup of  $GL(2, q)$ ; hence it is conjugate to a subgroup of the normaliser of  $A$  and so to an element of the stated list.  $\square$

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

**Proposition 4.4.** *Let  $G$  be an  $\mathbb{F}_p$ -primitive subgroup of  $GL(2, q)$ .*

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

- (i)  $A_4$ ,
- (ii)  $S_4$ ,
- (iii)  $A_5$ ,
- (iv)  $PSL(2, \bar{q})$ ,
- (v)  $PGL(2, \bar{q})$ ,

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

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

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

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 Proposition 3.4 there is an  $\mathbb{F}_p$ -primitive subgroup  $\hat{G}$  of  $SL(2, q^2)$  with central quotient  $G^* \cong G/Z(G)$ . If  $p = 2$  then  $\hat{G} \leq SL(2, q)$ , and by Theorem 3.5 (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 proposition, or  $p$  is odd and  $G^* \cong PSL(2, \tilde{q})$  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  $\text{Fit}(G)$ , but  $p$  does not divide  $|\text{Fit}(G)|$  by Theorem 3.5.

We now show that  $\log_p \tilde{q}$  divides  $\log_p q$  when  $p$  is odd,  $G^* \cong \text{PSL}(2, \tilde{q})$ , 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  $\text{PGL}(2, q)$ , 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.  $\square$

To list  $p^l$ -subgroups of  $\text{GL}(2, q)$  as in (a)(i)–(a)(iii) and (b)(i) of Proposition 4.4 we use some very old results, due to Jordan and Klein, which amount to a classification of the finite subgroups of  $\text{SL}(2, \mathbb{C})$  (see Blichfeldt [3, Chapter 3]). The classification rests on an isomorphism  $\iota: \text{PSU}(2) \rightarrow \text{SO}(3)$ , coming from conjugation action of  $\text{SU}(2)$  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  $\text{SO}(3)$  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  $\text{SO}(3)$  are permutation groups of finite degree such that each nontrivial element has precisely two fixed points, and each point stabiliser is a maximal cyclic subgroup. Such a group is the union of its maximal cyclic subgroups, which are the point stabilisers. Different point stabilisers intersect trivially.) Given that all homomorphisms involved are explicit, and that one may get explicit generating rotations for the finite subgroups of  $\text{SO}(3)$ , it is possible to write down generators for corresponding inverse images in  $\text{SU}(2)$  of those groups under the composite of the natural homomorphism  $\text{SU}(2) \rightarrow \text{PSU}(2)$  and  $\iota$ . (For our purposes this is the vital point. Analogues of the elements  $S$ ,  $U$ ,  $V$ , and  $W_1$  of  $\text{SL}(2, \mathbb{C})$  given in [3, §57, 58, pp. 70–73] will be chosen as generators for the  $\mathbb{F}_p$ -primitive subgroups of  $\text{GL}(2, \mathbb{F}_p)$  defined in Sections 4.5 and 4.6.) Moreover, it is clear that a finite subgroup of  $\text{SU}(2)$ , and thus a finite subgroup of  $\text{SL}(2, \mathbb{C})$ , is  $\text{SL}(2, \mathbb{C})$ -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 centre, 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  $\text{PSU}(2)$  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.

**4.5. The sublist  $\mathcal{P}_{2,q}^\circ$ .** If  $r > 3$  then  $\mathrm{PSL}(2, r)$  and  $\mathrm{PGL}(2, r)$  are insoluble. Thus, by Theorem 3.5 (vi) and Proposition 4.4, 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 3.7:  $\mathrm{SL}(2, 2) \cong S_3$  has irreducible subgroups  $C_3$  and  $S_3$  acting on the underlying  $\mathrm{GF}(2)$ -space  $\mathrm{Fit}(G)/\mathrm{Z}(G) \cong C_2 \times C_2$ ; 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 4.5.** *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  $q \equiv 1 \pmod{3}$ , 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  $\mathcal{P}_{2,q}^1$  to be the following list of subgroups of  $\mathrm{GL}(2, \mathbb{F}_p)$ :*

$$\begin{aligned} & \langle s, (\omega, -\omega), z \rangle \\ & \langle \nu_z s, (\omega, -\omega) \rangle \quad q \equiv 1 \pmod{3} \text{ and } \nu_z \in \mathrm{GF}(q) \text{ only} \end{aligned}$$

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

*Proof.* This is an application of [11, Theorem 5.4]. The conditions on  $\nu_z$  ensure  $|\nu_z| = 3|z|$ . An element of  $\mathbb{F}_p$  of order divisible by 3 lies in  $\mathrm{GF}(q)$  only if  $q \equiv 1 \pmod{3}$ , 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  $\mathcal{P}_{2,q}^1$  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].  $\square$

*Remark.* If  $q \equiv 3 \pmod{4}$  then no element of  $\mathcal{P}_{2,q}^1$  is in  $\mathrm{GL}(2, q)$ , but all groups may be rewritten over  $\mathrm{GF}(q)$  using the algorithm of Glasby & Howlett [14]. This issue does not arise if  $q \equiv 1 \pmod{4}$ .

*Remark.* Let  $\langle \alpha \rangle$  be the scalar subgroup of  $\mathrm{GL}(2, q^3)$ . In Theorem 4.5,  $z = \alpha^{(q^3-1)/r}$  for some (even)  $r$  dividing  $q-1$ , and if  $q \equiv 1 \pmod{3}$  then we can take  $\nu_z = \alpha^{(q^3-1)/3r}$ .

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

**Theorem 4.6.** *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 4.5, and*

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

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

$$\begin{aligned} & \langle s, u, z \rangle \\ & \langle s, \mu_z u, z \rangle \quad \mu_z \in \text{GF}(q) \text{ only} \end{aligned}$$

$(z, \mu_z)$  ranging over  $E$ ; otherwise  $\mathcal{P}_{2,q}^2$  is the list of all  $\langle s, \mu_z u, z \rangle$  such that  $\mu_z \alpha \in \text{GF}(q)$ . An  $\mathbb{F}_p$ -primitive subgroup of  $\text{GL}(2, q)$  with central quotient  $S_4$  has centre of even order, and is conjugate to a group in  $\mathcal{P}_{2,q}^2$ . Each group in  $\mathcal{P}_{2,q}^2$  is conjugate to an  $\mathbb{F}_p$ -primitive subgroup of  $\text{GL}(2, q)$  with central quotient  $S_4$ . Distinct groups in  $\mathcal{P}_{2,q}^2$  are not  $\text{GL}(2, \mathbb{F}_p)$ -conjugate.

*Proof.* Suppose  $G$  is an  $\mathbb{F}_p$ -primitive subgroup of  $\text{GL}(2, q)$  with centre  $Z = \langle z \rangle$  such that  $G/Z \cong S_4$ . By Proposition 3.6 (ii),  $|Z|$  is even. By the Universal Coefficient Theorem,

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

Say the extension-equivalence class of  $G$  corresponds to  $[\xi] \in H^2(G/Z, Z)$ . We cannot have  $[\xi] \in \text{Ext}(S_4/S_4', Z)$ , as  $\xi$  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. Proposition 3.3). Thus there are only two possible isomorphism types for  $G$ . Each type of group contains a copy of  $\text{SL}(2, 3)$ , 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  $\text{GL}(2, 3)$ , or the binary octahedral group, call it  $B$ . Now  $\text{GL}(2, 3)$  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  $\text{GL}(2, 3)$ , so there is a single conjugacy class of irreducible subgroups of  $\text{GL}(2, \mathbb{F}_p)$  isomorphic to the  $p'$ -group  $\text{GL}(2, 3)$ . Similarly there is a single conjugacy class of irreducible subgroups of  $\text{GL}(2, \mathbb{F}_p)$  isomorphic to  $B$ . Let  $K_1 = \langle s, u \rangle$  and  $K_2 = \langle s, \omega u \rangle$  where  $\omega \in \text{GF}(p^2)$  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  $K_2 \cong \text{GL}(2, 3)$ . Note that  $K_1$  but not  $K_2$  is in  $\text{SL}(2, \mathbb{F}_p)$ , 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  $\text{SL}(2, 3)$  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  $K_1 Z = K_2 Z = \langle s, u, z \rangle$ . 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  $\mu_z \in \text{GL}(2, q^2)$  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  $\text{SL}(2, 3)$ ; say  $K^x = K_2$ ,  $x \in \text{GL}(2, \mathbb{F}_p)$ . Then  $G^x/Z \cong S_4$  is a subgroup of  $H = \langle K_2 Z, \mu_z \rangle / Z \cong S_4 \times C_2$ . Now  $H$  has only two subgroups isomorphic to  $S_4$ , namely  $K_2 Z / Z$  and  $\langle s, \mu_z u, z \rangle / Z$ . We can discard  $K_2 Z / Z$  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  $\text{GL}(2, \mathbb{F}_p)$  to  $G_1 = \langle s, u, z \rangle$  or  $G_2 = \langle s, \mu_z u, z \rangle$ , and  $G_1 \not\cong G_2$ . Since  $G_1 X = G_2 X = K_1 X$ , 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  $H \leq G_1 \cap G_2$  and  $|G_1 : H| = |G_2 : H| = 2$ , and, as noted in the proof of Theorem 4.5,  $\mathrm{tr}(H) \subseteq \mathrm{GF}(q)$ . 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,  $p \equiv \pm 1 \pmod{8}$ . 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  $p \equiv \pm 3 \pmod{8}$  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  $\mathrm{tr}(\mu_z u) = \mu_z \alpha \in \mathrm{GF}(q)$ .  $\square$

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

**Theorem 4.7.** *Suppose  $p \geq 5$ . After all necessary rewriting,  $\mathcal{P}_{2,q}^{\circ} = \mathcal{P}_{2,q}^1 \cup \mathcal{P}_{2,q}^2$  is a list of the soluble  $\mathbb{F}_p$ -primitive subgroups of  $\mathrm{GL}(2, q)$ .*

#### 4.6. The sublist $\mathcal{P}_{2,q}^{\bullet}$ .

**Theorem 4.8.** *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 4.5, 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  $q \equiv \pm 1 \pmod{5}$ .*
- (ii) *Suppose  $q \equiv \pm 1 \pmod{5}$ . Let  $\mathcal{P}_{2,q}^3$  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  $\mathcal{P}_{2,q}^3$  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  $\mathcal{P}_{2,q}^3$ .*

*Proof.* Let  $G$  an  $\mathbb{F}_p$ -primitive subgroup of  $\mathrm{GL}(2, q)$  with centre  $Z$  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

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

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 centre. Therefore  $H \cong \mathrm{SL}(2, 5)$ , and  $G$  is conjugate to  $HZ$ . Clearly  $\mathcal{P}_{2,q}^3$  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  $\beta \in \text{GF}(q)$ , which is equivalent to  $q \equiv \pm 1 \pmod{5}$ , by quadratic reciprocity.  $\square$

**Proposition 4.9.** *Let  $p = 5$ . The list  $\mathcal{P}_{2,q}^4$  consisting of all groups  $\langle \text{SL}(2, 5), z \rangle$ ,  $z$  an even order scalar in  $\text{GL}(2, q)$ , is a list of the  $\mathbb{F}_p$ -primitive subgroups of  $\text{GL}(2, q)$  with central quotient  $A_5$ .*

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

**Lemma 4.10.** *If  $p$  is odd then  $\text{PSL}(2, q)$  does not have a faithful representation of degree 2 over  $\text{GF}(q)$ .*

**Lemma 4.11.**  *$A_5 \cong \text{PSL}(2, q)$  if and only if  $q = 5$ ;  $A_5 \cong \text{PGL}(2, q)$  if and only if  $q = 4$ .*

**Lemma 4.12.** *Let  $\mathbb{K}$  be an algebraically closed field and  $\mathbb{L}$  a subfield of  $\mathbb{K}$ . Suppose  $G$  is a subgroup of  $\text{GL}(n, \mathbb{L})$  that is irreducible over  $\mathbb{K}$ . Then, modulo scalars,  $\text{N}_{\text{GL}(n, \mathbb{K})}(G) \leq \text{GL}(n, \mathbb{L})$ .*

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

**Proposition 4.13.** *Suppose  $n \geq 3$ , or  $n = 2$  and  $q > 3$ . Let  $\mathbb{E}$  be any extension of  $\text{GF}(q)$ . If  $G$  is a subgroup of  $\text{GL}(n, \mathbb{E})$  isomorphic to  $\text{SL}(n, q)$  then  $G$  is irreducible over  $\mathbb{E}$ , and is conjugate to  $\text{SL}(n, q)$ .*

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

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

Suppose the  $\mathbb{E}G$ -module  $\mathbb{E}^{(n)}$  has a composition series factor of dimension  $m < n$ , so there is an irreducible representation  $G \rightarrow \text{GL}(m, q)$ . If  $m \neq 1$  then this further implies that  $\text{GL}(m, q)$  has a subgroup with quotient  $\text{PSL}(n, q)$  (if  $m = 1$  then the representation is trivial). But  $q^{n(n-1)/2}$  divides  $|\text{PSL}(n, q)|$ , whereas the highest power of  $p$  dividing  $|\text{GL}(m, q)|$  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.  $\square$

**Theorem 4.14.** *Suppose  $p$  is odd and  $q > 5$ . Let  $\alpha$  be a generator of  $\text{GF}(q)^\times$  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  $\text{GL}(2, q)$  as follows:*

$$\begin{aligned} & \langle (\alpha^s, \alpha^s), \text{SL}(2, \bar{q}) \rangle && \text{only if } p \neq 5, \text{ or } p = 5 \text{ and } \bar{q} > 5 \\ & \langle (\alpha^{r/2}, \alpha^{-r/2}), (\alpha^s, \alpha^s), \text{SL}(2, \bar{q}) \rangle && r \text{ even} \\ & \langle (\alpha^{(s+r)/2}, \alpha^{(s-r)/2}), (\alpha^s, \alpha^s), \text{SL}(2, \bar{q}) \rangle && s, r \text{ both odd or both even,} \end{aligned}$$

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

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

- (i) Every group in  $\mathcal{P}_{2,q}^5$  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  $\mathcal{P}_{2,q}^5$ .
- (iii) Distinct groups in  $\mathcal{P}_{2,q}^5$  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  $\mathcal{P}_{2,q}^5$ . By Lemma 4.11, and because  $(\alpha^{r/2}, \alpha^{-r/2}) \equiv (\alpha^r, 1) \pmod{\text{scalars}}$  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  $Z(G) = X = \langle (\alpha^s, \alpha^s) \rangle$ , where  $s$  divides  $q - 1$ . By Proposition 4.4 (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  $Z(H) = X$  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 not relevant by Lemma 4.10. 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 Proposition 4.13,  $K$  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  $(\alpha^s, \alpha^s)$ . Consequently, from now on let the index be 2, that is,  $G/X \cong \mathrm{PGL}(2, \bar{q})$ . Lemma 4.12 tells us that  $G \leq \mathrm{GL}(2, \bar{q})Z$ , and so  $GZ = \mathrm{GL}(2, \bar{q})Z$ . Thus

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

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  $\delta/\alpha^r$  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  $\bar{q}$  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  $(\dagger)$ ,  $x$  would have trivial conjugation action.  $\square$

- Theorem 4.15.** (i) *After rewriting over  $\text{GF}(q)$ ,  $\mathcal{P}_{2,q}^3 \cup \mathcal{P}_{2,q}^5$  ( $p > 5$ ) or  $\mathcal{P}_{2,q}^4 \cup \mathcal{P}_{2,q}^5$  ( $q > p = 5$ ) is a list  $\mathcal{P}_{2,q}^\bullet$  of the insoluble  $\mathbb{F}_p$ -primitive subgroups of  $\text{GL}(2, q)$ .*  
 (ii) *If  $q = 5$  then  $\mathcal{P}_{2,5}^\bullet = \{\text{SL}(2, 5), \langle \text{SL}(2, 5) \rangle, (4, 1)\}$ ,  $\text{GL}(2, 5)\}$  is a list of the insoluble irreducible subgroups of  $\text{GL}(2, 5)$ .*

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

## 5. DEGREE 3

### 5.1. The sublist $\mathcal{A}_{3,q}$ .

**Theorem 5.1.** *Let  $\alpha$  be a generator of  $\text{GF}(q^3)^\times$ , 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  $\text{GL}(3, q)$  of order  $r$ . An irreducible abelian subgroup of  $\text{GL}(3, q)$  is conjugate to  $A(r)$  for some  $r$ .

*Proof.* Cf. the proof of Lemma 4.1. □

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

Denote by  $c$  and  $d$  the  $3 \times 3$  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.

**Proposition 5.2.** *Let  $\mathbb{K}$  be an algebraically closed field and  $G$  be a finite subgroup of  $\text{M}(3, \mathbb{K})$ . Set  $M = \text{D}(3, \mathbb{K}) \cap G$ .*

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

*Proof.* (i) is clear by Lemma 3.1 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  $\text{D}(3, \mathbb{K})$ -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  $m \in \text{D}(3, \mathbb{K})$ . 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  $\text{SL}(3, \mathbb{F}_p)$ . 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  $(\omega, \omega, \omega^{-2}) \equiv z_d^{-2} \pmod{M_2M_3}$ , from which we conclude that in  $H$  (and relabelling 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 relabelling. 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  $(cz_c)^d \equiv (cz_c)^{-1} \pmod{M_2M_3}$ , which implies  $z_c^2 \in M_3$  and hence  $z_c \in M_3$ .  $\square$

*Remark.* For a generalisation of the claim in Proposition 5.2 (ii) that  $G$  has a (monomial) conjugate containing  $\pi G$  up to scalars, see [2, Theorem 6.10].

**Lemma 5.3.** *A group as in Proposition 5.2 (i) is not isomorphic to a group as in Proposition 5.2 (ii).*

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

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

*Proof.* Suppose  $G$  is irreducible; then  $\pi G$  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 Proposition 5.2; 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  $H \cap D(3, \mathbb{F}_p) = M$ . The  $p'$ -group  $H$  is isomorphic to a subgroup of  $GL(3, \mathbb{C})$ , 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.  $\square$

We now determine the finite  $C$ -submodules and  $S_3$ -submodules of  $D(3, \mathbb{F}_p)$ . Bácskai does this in Chapters 3 and 4 of [2]. 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  $GL(3, \mathbb{F}_p)$ ,  $U$  be the subgroup of  $D(3, \mathbb{F}_p)$  consisting of all diagonal matrices  $(\omega, \omega^{-1}, 1)$ , and set  $W = U^c$ . Neither  $U$  nor  $W$  is a  $C$ -module, but  $U \times W = D(3, \mathbb{F}_p) \cap SL(3, \mathbb{F}_p)$  is. Also  $D(3, \mathbb{F}_p) = ZUW$ , and  $|Z \cap UW| = 3$ .

Let  $r \neq p$  be a prime, and for  $i \geq 0$  inductively select primitive  $r^i$ th 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  $l^2 - l + 1 \equiv 0 \pmod{r^k}$ . Conversely, if  $l^2 - l + 1 \equiv 0 \pmod{r^k}$  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  $r \equiv 1 \pmod{3}$ . Summing up: if  $r \equiv 2 \pmod{3}$  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  $r \equiv 1 \pmod{3}$  then there are additionally the  $C$ -submodules

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

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

Now suppose  $r = 3$ . There is a solution of  $l^2 - l + 1 \equiv 0 \pmod{3^k}$  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 5.5.** *Let  $r$  be a prime,  $r \neq p$ .*

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

$$\begin{aligned} & \langle z_{i,r}, u_{j,r}, w_{j,r} \rangle \\ & \langle z_{i,r}, u_{j+k,r}^l w_{j+k,r}, u_{j,r}, w_{j,r} \rangle \quad r \equiv 1 \pmod{3} \text{ only} \end{aligned}$$

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

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

*if  $r = 3$ .*

(ii) *A finite  $S_3$ -submodule of  $D(3, \mathbb{F}_p)$  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*

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

*if  $r = 3$ .*

*Proof.* Cf. [9, §3.1] and [2, Chapter 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.  $\square$

The next proposition resolves  $S_3$ -conjugacy among  $C$ -submodules of  $D(3, q)$  of  $3'$ -order.

**Proposition 5.6.** *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*

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

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

$$\mathcal{C}_{2,r} = \{ \langle z_{i,r}, u_{j+k,r}^{l_{r,k}} w_{j+k,r}, u_{j,r}, w_{j,r} \rangle \mid 0 \leq i, j \leq e_r, k \leq e_r - j \},$$

$$\mathcal{C}_{3,r} = \{ \langle z_{i,r}, u_{j+k,r}^{l_{r,k}} w_{j+k,r}, u_{j,r}, w_{j,r} \rangle, \langle z_{i,r}, u_{j+k,r}^{1-l_{r,k}} w_{j+k,r}, u_{j,r}, w_{j,r} \rangle \mid 0 \leq i, j \leq e_r, k \leq e_r - j \}.$$

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  $D(3, q)$  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

$$C(i, j, 1, \varepsilon) = \langle cz_{i+1,3}^\varepsilon, z_{i,3}, u_{j,3}, w_{j,3} \rangle, \quad \varepsilon \in \{0, 1\}, \quad i, j \geq 1$$

$$C(i, j, 2, \varepsilon) = \langle cz_{i+1,3}^\varepsilon, z_{i,3}, u_{j+1,3}^2 w_{j+1,3}, u_{j,3}, w_{j,3} \rangle, \quad \varepsilon \in \{0, 1\}, \quad i \geq 1, \quad j \geq 0$$

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

$$C(i, j, 4) = \langle c, z_{i+1,3}^2 u_{j+1,3}^2 w_{j+1,3}, u_{j,3}, w_{j,3} \rangle, \quad i, j \geq 1$$

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

All these groups bar the  $C(i, 0, 2, \varepsilon)$  are nonabelian. Aided by the order formulae  $|C(i, j, 1, \varepsilon)| = 3^{i+2j}$ ,  $|C(i, j, 2, \varepsilon)| = |C(i, j, 3)| = |C(i, j, 4)| = 3^{i+2j+1}$ ,  $|C(i, j, 5)| = 3^{i+2j+2}$ , 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  $i, j, k, \varepsilon$ .

**Theorem 5.7.** *Let  $G$  be a finite irreducible subgroup of  $M(3, \mathbb{F}_p)$  with  $\pi G = C$ . Then  $G$  is  $GL(3, \mathbb{F}_p)$ -conjugate to  $G_3 \times G_{3'}$  where  $G_{3'} := O_{3'}(G) \leq D(3, \mathbb{F}_p)$ , and if  $G_{3'}$  is scalar then  $G_3$  is one of  $C(i, j, 1, \varepsilon)$ ,  $C(i, j, 2, \varepsilon)$ ,  $C(i, j, 3)$ ,  $C(i, j, 4)$ ,  $C(i, j, 5)$ ,  $i, j \geq 1$  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 Proposition 5.2 (i),  $G$  is  $D(3, \mathbb{F}_p)$ -conjugate to  $\langle cz, M_3 \rangle M_{3'}$ , where  $z \in Z_3$  and  $z^3 \in M_3$ . Referring to Theorem 5.5

(i), we discover that either  $z \in \text{SL}(3, \mathbb{F}_p) \bmod M_3$  and then  $G$  is  $\text{D}(3, \mathbb{F}_p)$ -conjugate to  $\langle c, M_3 \rangle M_{3'}$  by Lemma 3.1, or  $M_3$  is an  $S_3$ -module and  $z = z_{i+1,3}^\eta \bmod M_3$ ,  $\eta \in \{0, 1, 2\}$ , 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  $\eta$  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  $\text{M}(3, \mathbb{F}_p)$ -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  $\text{M}(3, \mathbb{F}_p)$  of order 3 is conjugate to  $C$ ). Further, if  $M_{3'}$  is indeed nonscalar then  $G_3 M_{3'}$  is irreducible by Proposition 5.4.

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 Proposition 5.4  $G$  is irreducible if and only if  $G_3$  is nonabelian. We ensure this by taking  $j$  greater than 0 when  $G_3 = C(i, j, 2, \varepsilon)$ .  $\square$

**Lemma 5.8.** *Every group listed in Theorem 5.7, 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 5.7 and the order formulae before the theorem, we see that this can happen only if  $G_3 = C(i, 1, 1, \varepsilon)$ .  $\square$

**Lemma 5.9.** *Let  $G$  and  $H$  be isomorphic finite irreducible subgroups of  $\text{M}(3, \mathbb{F}_p)$ .*

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

*Proof.* (i) is just Proposition 5.4 and Lemma 5.3. For (ii) we use the fact that the groups of diagonal matrices  $\mathcal{O}_{\{2,3\}'}(G)$  and  $\mathcal{O}_{\{2,3\}'}(H)$  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 5.5 (ii).  $\square$

**Proposition 5.10.** *Let  $G, H$  be finite subgroups of  $\text{M}(3, \mathbb{F}_p)$  such that  $\pi G = \pi H = C$ . If  $G^m = H$  and  $M^m = N$  for some  $m \in \text{GL}(3, \mathbb{F}_p)$  and nonscalar subgroups  $M$  of  $\text{D}(3, \mathbb{F}_p) \cap G$ ,  $N$  of  $\text{D}(3, \mathbb{F}_p) \cap H$ , then  $m \in \text{M}(3, \mathbb{F}_p)$ .*

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

**Proposition 5.11.** *Let  $\mathcal{T}$  be the list of all  $G_3$  appearing in the semidirect products  $G_3 G_{3'}$  of Theorem 5.7, 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  $\text{M}(3, \mathbb{F}_p)$  with the notation  $P_{kl0}, P_{kl1}, P_{kl2}, P_{kl3}$  of [5, §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  $C(i, 0, 2, 0) \not\cong C(i, 0, 2, 1)$ , 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 5.7 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.  $\square$

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

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

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

**Lemma 5.12.** *Let  $G$  be a finite subgroup of  $M(3, \mathbb{K})$ ,  $\mathbb{K}$  any field, such that  $\pi G = S_3$ . Then  $G$  has a unique subgroup  $H$  of index 2 such that  $|H : A| = 3$  for some abelian normal subgroup  $A$  of  $H$ .*

*Proof.* We claim that  $H$  is the subgroup of  $G$  containing  $A = D(3, \mathbb{K}) \cap G$  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  $\pi K \leq S_3$  and  $K$  is not diagonal nor contains 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  $B/(B \cap A^*)$ .  $\square$

**Theorem 5.13.** *A finite irreducible subgroup  $G$  of  $M(3, \mathbb{F}_p)$  such that  $\pi G = S_3$  is  $GL(3, \mathbb{F}_p)$ -conjugate to one and only one group  $S(i, j, k, l, m, \eta)M$  where  $M$  is a finite  $S_3$ -submodule of  $D(3, \mathbb{F}_p)$  of  $\{2, 3\}'$ -order, and either  $M$  is nonscalar, or  $M$  is scalar and  $l \geq 1$  or  $j \geq 1$ .*

*Proof.* By Proposition 5.2,  $G$  is  $D(3, \mathbb{F}_p)$ -conjugate to  $\langle c, dz, N_{\{2,3\}} \rangle N_{\{2,3\}'}$  where  $N := D(3, \mathbb{F}_p) \cap G$  and  $z \in Z_2$ ,  $z^2 \in N_2$ . The choices for  $N_2$  and  $N_{\{2,3\}'}$  are given in Theorem 5.5 (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 Proposition 5.4, 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  $x \in GL(3, \mathbb{F}_p)$ . Then  $M = M'$  by Lemma 5.9, and the equalities  $i = i'$ ,  $j = j'$ ,  $k = k'$ ,  $l = l'$ , and  $m = m'$  follow from Lemma 5.12, Proposition 5.4, and Proposition 5.11. By [11, Theorem 8.10 (i)],  $x$  is monomial – the sole situation in which conceivably  $x \notin M(3, \mathbb{F}_p)$  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  $x \in M(3, \mathbb{F}_p)$ . Therefore  $x^{1-d} \equiv z_{k+1,2} \pmod{\langle z_{k,2}, u_{l,2}, w_{l,2} \rangle}$ , further implying that  $\langle z_{k+1,2} \rangle \subseteq \text{SL}(3, \mathbb{F}_p)$ . This is absurd. Hence  $\eta = \eta'$ .  $\square$

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

**Theorem 5.14.** *Let  $G$  be an irreducible subgroup of  $M(3, \mathbb{F}_p)$  conjugate to a subgroup of  $M(3, q)$ . Let  $\alpha$  be a generator of  $\text{O}_3(\text{GF}(q)^\times)$ ,  $|\alpha| = 3^t$ , and set  $|\text{O}_2(\text{GF}(q)^\times)| = 2^s$ .*

- (i) *Suppose  $\pi G = C$ . Let  $\mathcal{C}$  be as in Proposition 5.6. 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  $M(3, q)$ ,  $G_{3'}$  a  $C$ -submodule of  $D(3, q)$  of order not divisible by 3, and  $G_3$  one of*

$C, G_{3'}$  nonscalar only

$$\left. \begin{array}{l} C(i, j, 1, 0) \\ C(i, j, 1, 1) \\ \langle c(\alpha, 1, 1), u_{j,3}, w_{j,3} \rangle \end{array} \right\} \begin{array}{l} 1 \leq i \leq t \\ 1 \leq i \leq t-1 \\ \end{array} \quad 1 \leq j \leq t$$

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

$$C(i, j, 3) \quad 1 \leq i, j \leq t-1 \text{ or } i = j = t$$

$$C(i, j, 4) \quad 1 \leq i, j \leq t-1$$

$$C(i, j, 5) \quad 1 \leq i \leq t-1, 0 \leq j \leq t-1, \text{ but } j \geq 1 \text{ when } G_{3'} \text{ is scalar,}$$

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  $M(3, q)$ , where  $M$  is an  $S_3$ -submodule of  $D(3, q)$  of  $\{2, 3\}^l$ -order, and  $S(i, j, k, l, m, \eta)$  is as defined before Lemma 5.12, with  $0 \leq k, l \leq s, \eta \in \{0, 1\}, \eta = 0$  if  $k = s$ , and the other parameters range as follows:*

$$m = 1, \quad 1 \leq i, j \leq t$$

$$m = 1, \quad i = j = 0, \quad M \text{ nonscalar or } l \geq 1 \text{ only}$$

$$m = 2, \quad 1 \leq i \leq t, \quad 0 \leq j \leq t-1, \text{ but } j \geq 1 \text{ if } M \text{ is scalar and } l = 0$$

$$m = 3, \quad 1 \leq i, j \leq t-1 \text{ or } i = j = t \geq 1$$

$$m = 4, \quad 1 \leq i, j \leq t-1.$$

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

- (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 5.7. Clearly  $G_{3'} \leq D(3, q)$ , and if  $G_3$  is normalised by  $S_3$  then by Proposition 5.6 we may take

$G_{3'} \in \mathcal{C}$ . For some  $i, j \geq 0$ ,  $\langle z_{i,3}, u_{j,3}, w_{j,3} \rangle \leq G$ , and  $i \leq t$ . Since a conjugate of  $G_3$  lies in a Sylow 3-subgroup of  $M(3, q)$ , and the latter has exponent  $3^{t+1}$ , we have  $|u_{j,3}| \leq 3^{t+1}$ , so  $j \leq t+1$ . If  $j = t+1$  then  $u_{j,3}$  is conjugate to  $cm$  for some  $m \in D(3, q)$ . But  $\text{tr}(cm) = 0$ , and if  $\omega_{j,3} + \omega_{j,3}^{-1} + 1 = 0$  then  $j = 1$ . Thus if  $t \geq 1$  then  $j \leq t$ . If  $\text{GF}(q)^\times$  has trivial Sylow 3-subgroup then  $G_3 = C$  and  $G_{3'}$  is nonscalar. From now on,  $t \geq 1$ .

If  $G_3 = C(i, j, 1, \varepsilon)$ ,  $1 \leq j \leq t$ , and  $1 \leq i \leq t$  or  $1 \leq i \leq t-1$  according as  $\varepsilon = 0$  or  $\varepsilon = 1$ , respectively, then  $G \leq M(3, q)$ . However  $C(t, j, 1, 1) \not\leq M(3, q)$ . By Lemma 5.8, the diagonal subgroup of every other  $G$  is conjugate to a subgroup of  $D(3, q)$ , so must also be in  $D(3, q)$ . Since  $C(i, t, 2, \varepsilon)$  has an element  $(\omega^2, \omega^{-1}, \omega^{-1})$ ,  $\omega^3 = \alpha$ , not in  $D(3, q)$ , 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  $i \leq t-1$  then  $j \leq t-1$ , 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  $i \leq t-1$  too.

With parameter ranges as indicated, all groups are visibly in  $M(3, q)$  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  $M(3, q)$ , generated by the same diagonal subgroup and  $c(\alpha, 1, 1)$ .

(ii) By Theorem 5.13,  $G$  is the product of some  $S(i, j, k, l, m, \eta)$  and an  $S_3$ -submodule of  $D(3, \mathbb{F}_p)$  of  $\{2, 3\}'$ -order. It follows from Lemma 5.12 that the diagonal subgroup of  $G$  is in  $D(3, q)$ , 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  $\text{GF}(q)$ , 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 Proposition 5.4.

(iv) We appeal to Lemma 5.3 and Theorem 5.13 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 Proposition 5.11, 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  $M(3, \mathbb{F}_p)$ -conjugate, by Lemma 5.8 and Proposition 5.10 we have  $G_3^{\tilde{m}} = H_3 = G_3$  and  $G_{3'}^{\tilde{m}} = H_{3'}$  for some  $\tilde{m}, m \in M(3, \mathbb{F}_p)$ ,  $\pi\tilde{m} = \pi m$ . If  $\pi m \in C$  then  $G_{3'} = H_{3'}$ . If  $\pi m \notin C$  then  $G_3^d$  is  $D(3, \mathbb{F}_p)$ -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.  $\square$

*Remark.* The list of  $S_3$ -submodules of  $D(3, q)$  of  $\{2, 3\}'$ -order may be easily written down from Proposition 5.6.

We leave as an exercise the formulation of an equivalent to Theorem 5.14 for fields of characteristic 3, by employing Proposition 3.2 for projection  $C$ .

### 5.3. The sublist $\mathcal{PM}_{3,q}$ .

**Proposition 5.15.** *Let  $G$  be an absolutely irreducible  $\text{GF}(q)$ -primitive  $\mathbb{F}_p$ -monomial subgroup of  $\text{GL}(3, q)$ . Then  $G$  has an irreducible abelian normal subgroup.*

*Proof.* We invoke Proposition 3.3 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.  $\square$

**Proposition 5.16.** *Let  $\alpha$  be a generator of  $\text{GF}(q)^\times$ , and write  $q - 1 = 3^t l$ ,  $l$  coprime to 3. Denote the scalars of  $\text{GL}(3, q)$  by  $Z$ . Let  $A$  be the Singer cycle generated by  $b$  as in Theorem 5.1, and let  $a$  be the matrix whose  $i$ th 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*

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

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  $\text{O}_3(A) \not\leq \tilde{A}$ ,  $|\tilde{A}|$  does not divide  $q-1$ ,  $\text{O}_3(\tilde{A} \cap Z) \neq 1$ , and  $k$  is defined by  $\text{O}_3(\tilde{A} \cap Z) = \langle b^{(q^3-1)/3^k} \rangle$ .

*Proof.* Heeding Proposition 5.15, we follow Short's prescription [22, Theorem 4.2.7] as in Proposition 4.3.  $\square$

**5.4. The sublist  $\mathcal{P}_{3,q}^\circ$ .** By Proposition 3.6 (ii),  $\mathcal{P}_{3,q}^\circ$  is nonempty only if  $q \equiv 1 \pmod{3}$ , implying  $p \neq 3$  and if  $p = 2$  then  $\log_2 q$  is even. Henceforth  $p \geq 5$ .

Corollary 3.7 tells us that a soluble primitive subgroup of  $\text{GL}(3, \mathbb{F}_p)$  has central quotient  $T_L := (C_3 \times C_3) \rtimes L$  where  $L$  is an irreducible subgroup of  $\text{SL}(2, 3)$ , and the conjugation action of  $L$  on  $C_3 \times C_3$  is the natural action of a subgroup of  $\text{SL}(2, 3)$  on its underlying vector space. The possible isomorphism types for  $L$  are  $C_4, Q_8$  and  $\text{SL}(2, 3)$ . Since, for each isomorphism type, there is a single conjugacy class of subgroups of  $\text{SL}(2, 3)$  of that type, each choice of  $L$  determines a single isomorphism type of  $T_L$ . An easy exercise establishes that  $T_{\text{SL}(2,3)}$  has the following power-conjugate presentation:

$$\langle x_1, x_2, x_3, x_4, x_5, x_6 \mid \begin{array}{l} x_1^3 = 1, x_2^2 = x_3^2 = x_4, x_4^2 = x_5^3 = x_6^3 = 1, \\ x_2^{x_1} = x_2 x_3 x_4, x_3^{x_1} = x_2, x_3^{x_2} = x_3 x_4, \\ x_5^{x_1} = x_5 x_6^2, x_5^{x_2} = x_5 x_6, x_5^{x_3} = x_6^2, x_5^{x_4} = x_5^2, \\ x_6^{x_2} = x_5 x_6^2, x_6^{x_3} = x_5, x_6^{x_4} = x_6^2 \end{array} \rangle$$

with the usual convention that trivial conjugate relations are omitted (for example,  $x_6^{x_1} = x_6$ ). We have  $\langle x_2, x_3 \rangle \cong Q_8$ ,  $\langle x_2, x_3 \rangle \rtimes \langle x_1 \rangle \cong \text{SL}(2, 3)$ , and  $\langle x_5, x_6 \rangle \cong C_3 \times C_3$  is the underlying  $\text{GF}(3)$ -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 noncyclic abelian normal subgroup), from its character table and knowledge of its automorphism group, we find the number of  $\text{GL}(3, \mathbb{F}_p)$ -conjugacy classes of irreducible primitive subgroups of  $\text{GL}(3, \mathbb{F}_p)$  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  $\text{Aut}(Z) \times \text{Aut}(T_L)$ -action accounts for all possible isomorphisms between extensions of  $Z$  by  $T_L$ , because such an extension has centre precisely  $Z$  ( $T_L$  is centreless).

In the sequel we use the results of routine computations in MAGMA: Holt's algorithm [15] to determine Schur multipliers of permutation groups and our 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,  $H^2(T_{C_4}, Z) = \text{Hom}(H_2(T_{C_4}), Z) = \text{Hom}(C_3, Z) \cong C_3$ . Denote the elements of  $\text{Hom}(H_2(T_{C_4}), Z)$  as  $[\chi_i]$ ,  $1 \leq i \leq 3$ ,  $[\chi_1]$  trivial. We may write  $\chi_i$  as  $\mu_i \phi$  where  $\phi$  is a 2-cocycle  $T_{C_4} \rightarrow H_2(T_{C_4})$  and  $\mu_i \in \text{Hom}(H_2(T_{C_4}), Z)$ . Further, if  $\theta$  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 splitting extension of  $Z$  by  $T_{C_4}$  is forbidden here (by primitivity), and since  $\chi_2$  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

$$\begin{aligned} \langle y_1, y_2, y_3, y_4, y_5 \mid & y_1^2 = y_2, y_2^2 = y_3^3 = y_4^3 = y_5^3 = 1, \\ & y_3^{y_1} = y_3 y_4, y_3^{y_2} = y_3^2, \\ & y_4^{y_1} = y_3 y_4^2 y_5, y_4^{y_2} = y_4^2 y_5^2, y_4^{y_3} = y_4 y_5^2 \rangle. \end{aligned} \quad (*)$$

**Lemma 5.17.** *The subgroups of  $\mathrm{GL}(3, \mathbb{F}_p)$  isomorphic to  $S$  are in 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.  $\square$

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 Section 5.2. 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 5.7,  $(\omega - \omega^2)v$  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 5.7) by a cycle of order 4. Thus  $|S_i| = 108$  for all  $i$ .

*Remark.* If  $H$  is a soluble absolutely irreducible  $\mathbb{F}_p$ -primitive subgroup of  $\mathrm{GL}(3, q)$  then by Theorem 3.6,  $\mathrm{Fit}(H)$  is conjugate to a subgroup of  $\mathrm{M}(3, \mathbb{F}_p)$ . Indeed, if  $|Z(H)| = 3^i$  then a Sylow 3-subgroup of  $\mathrm{Fit}(H)$  is conjugate to  $C(i, 1, 1, 0)$ .

**Lemma 5.18.**  $S_1 \cong S_2 \cong S_3 \cong S$ .

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

**Proposition 5.19.** *Let  $q \equiv 1 \pmod{3}$ . Let  $\mathcal{L}$  be the list consisting of all groups*

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

and

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

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 centre is conjugate to a group in  $\mathcal{L}$ .



*Proof.*  $\text{Fit}(S_i) = C(1, 1, 1, 0)$  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 centre  $Z = \langle z, x \rangle = \langle z, x' \rangle$ , and  $S_i Z_3$  and  $S_j Z_3$  are conjugate. By Proposition 3.6 (iii), if  $K, \tilde{K}$  are complements of  $\text{Fit}(S_i Z_3)$  in  $S_i Z_3$  of order 4 then  $K Z_3, \tilde{K} Z_3$  are conjugate; since  $v \in \text{SL}(3, \mathbb{F}_p)$  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  $\text{GL}(3, \mathbb{F}_p)$  isomorphic to  $S_1$  is conjugate to one and only one of  $S_1, S_2$ , or  $S_3$  by the preceding and Lemmas 5.17, 5.18. Thus if  $G \leq \text{GL}(3, q)$  is primitive over  $\mathbb{F}_p$ , has centre of odd order, and central quotient  $T_{C_4}$ , then a conjugate  $\bar{G}$  of  $G$  contains some  $S_i$ . Let  $Z(\bar{G}) = \langle x \rangle$ . Then  $\langle S_i, x \rangle / \langle x \rangle \cong T_{C_4}$  implies  $\bar{G} = \langle S_i, x \rangle$ . Since  $\text{tr}(\iota v) = \iota$ , necessarily  $q \equiv 1 \pmod{4}$  if  $i = 3$ .  $\square$

Now suppose  $|Z|$  is even. We then have  $H^2(T_{C_4}, Z) = \text{Ext}(C_4, Z_2) \times \text{Hom}(C_3, Z_3)$ . Let  $[\psi\chi]$  be a 2-cocycle class in  $H^2(T_{C_4}, Z)$ , where  $[\psi] \in \text{Ext}(C_4, Z_2)$  and  $[\chi] \in \text{Hom}(C_3, Z_3) \cong C_3$ . 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  $\text{Ext}(C_4, Z_2)$  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  $|Z| \equiv 2 \pmod{4}$ , and exactly three types if 4 divides  $|Z|$ .

Let  $H \leq \text{GL}(3, \mathbb{F}_p)$  be a primitive extension of  $Z$  by  $T_{C_4}$ . Suppose  $|Z| \equiv 2 \pmod{4}$ . 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  $H = S_1 Z = S_2 Z$  or  $H = S_3 Z$ , 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  $S_1 Z$  or  $S_3 Z$  up to conjugacy. Then  $H/Z$  is a subgroup of  $\langle S_i Z, \nu \rangle / Z \cong T_{C_4} \times C_4$ ,  $i = 1$  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  $v_2 \in \text{SL}(3, \mathbb{F}_p)$  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  $v_2$  normalises  $\langle c, u, Z \rangle$ . Hence the first and second groups above are conjugate. Since  $\text{tr}(\nu v) = \nu$ , either group is conjugate to a subgroup of  $\text{GL}(3, q)$  only if  $q \equiv 1 \pmod{8}$ , in which case the group is actually in  $\text{GL}(3, q)$ .

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  $\text{GL}(3, \mathbb{F}_p)$ -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  $\lambda$  is a scalar whose fourth power generates  $Z_2$ . Also these two groups are non-conjugate (for 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 5.20.** *Let  $q \equiv 1 \pmod{3}$ , and fix a primitive eighth root of unity  $\nu \in \mathbb{F}_p$ . Define  $\mathcal{P}_{3,q}^1$  to be the list of all groups*

$$\begin{aligned} & \langle S_1, x \rangle \\ & \langle S_1, x' \rangle \\ & \langle S_1, x'' \rangle \\ & \langle S_2, x \rangle \\ & \left. \begin{aligned} & \langle S_3, x \rangle \\ & \langle S_3, x' \rangle \end{aligned} \right\} q \equiv 1 \pmod{4} \text{ only} \\ & \langle \nu v, c, u, x' \rangle \quad q \equiv 1 \pmod{8} \text{ only} \\ & \left. \begin{aligned} & \langle \lambda_{x''} v, c, u, x'' \rangle \\ & \langle \lambda_{x''}^2 v, c, u, x'' \rangle \end{aligned} \right\} q \equiv 1 \pmod{16} \text{ and } \lambda_{x''} \in \text{GF}(q) \text{ only} \end{aligned}$$

where  $\langle x \rangle, \langle x' \rangle, \langle x'' \rangle$  run over the distinct scalar subgroups of  $\text{GL}(3, q)$  such that  $|x|$  is odd,  $|x'| \equiv 2 \pmod{4}$ ,  $|x''| \equiv 0 \pmod{4}$ ,  $\lambda_{x''} \in \mathbb{F}_p$  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. Every group in  $\mathcal{P}_{3,q}^1$  is a soluble  $\mathbb{F}_p$ -primitive subgroup of  $\text{GL}(3, q)$ , distinct groups in  $\mathcal{P}_{3,q}^1$  are not conjugate, and an  $\mathbb{F}_p$ -primitive subgroup of  $\text{GL}(3, q)$  with central quotient  $(C_3 \times C_3) \rtimes C_4$  is conjugate to a group in  $\mathcal{P}_{3,q}^1$ .

The methods used above for  $L \cong C_4$  may now be applied with equal effectiveness when  $L \cong Q_8$  and  $L \cong \text{SL}(2, 3)$ . 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

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

with  $\langle x_2, x_3 \rangle \cong Q_8$ . Relabel  $v$  as  $v_1$ , and let  $v_2$  be as defined before Theorem 5.20. The mapping  $x_2 \mapsto v_1, x_3 \mapsto v_2$  defines an isomorphism  $\langle x_2, x_3 \rangle \rightarrow \langle v_1, v_2 \rangle$ . 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,  $\text{Aut}(Z) \times \text{Aut}(T_{Q_8})$  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  $\text{GL}(3, \mathbb{F}_p)$  isomorphic to the Schur cover  $S$  of  $T_{Q_8}$ . (Cf. Lemma 5.17. 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  $\omega^2$ . 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  $\tau$  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 recognise

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

as candidates for  $H$ . Using  $v_1^{v_3} = v_2$  and  $v_2^{v_3} = v_1v_2^{-1}$ , we see that all three groups are conjugate.

**Theorem 5.21.** *Let  $q \equiv 1 \pmod{3}$ . Define  $\mathcal{P}_{3,q}^2$  to be the list of all groups*

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

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. Every group in  $\mathcal{P}_{3,q}^2$  is a soluble  $\mathbb{F}_p$ -primitive subgroup of  $\mathrm{GL}(3, q)$ , distinct groups in  $\mathcal{P}_{3,q}^2$  are not conjugate, and 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  $\mathcal{P}_{3,q}^2$ .

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 nonisomorphic Schur covers of  $T_{\mathrm{SL}(2,3)}$  in  $\mathrm{GL}(3, \mathbb{F}_p)$ :

$$\begin{aligned} S_1 &= \langle v_1, v_2, v_3, c, z, u, w \rangle, & S_2 &= \langle v_1, v_2, \nu v_3, c, z, u, w \rangle, \\ & & S_3 &= \langle v_1, v_2, \nu^2 v_3, c, z, u, w \rangle \end{aligned}$$

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  $\nu_i$  be a scalar of 3-power order such that  $\nu_i^3 = x^{1-2 \cdot 3^{i-1}}$  (thus  $\nu_i \notin Z$ ), and define

$$\begin{aligned} G(i, 1) &= \langle v_1, v_2, v_3, c, x, u, w \rangle, & G(i, 2) &= \langle v_1, v_2, \nu_i v_3, c, x, u, w \rangle, \\ & & G(i, 3) &= \langle v_1, v_2, \nu_i^2 v_3, c, x, u, w \rangle. \end{aligned}$$

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

**Proposition 5.22.** *Let  $q \equiv 1 \pmod{3}$ . A primitive absolutely irreducible subgroup  $G$  of  $\mathrm{GL}(3, q)$  with centre  $Z = \langle x \rangle$  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  $S_j$ s. 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  $G(i, 2)$ ,  $G(i, 3)$ .  $\square$

**Corollary 5.23.** *Let  $q \equiv 1 \pmod{3}$ , and let  $3^t$  be the largest power of 3 dividing  $q - 1$ . Define  $\mathcal{P}_{3,q}^3$  to be the list of all groups*

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

*$1 \leq i \leq t$ ,  $\langle x \rangle$  ranging over the scalar subgroups of  $\mathrm{GL}(3, q)$  of  $3^t$ -order. Groups in  $\mathcal{P}_{3,q}^3$  are pairwise nonconjugate soluble  $\mathbb{F}_p$ -primitive subgroups of  $\mathrm{GL}(3, q)$ . 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  $\mathcal{P}_{3,q}^3$ .*

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

**Theorem 5.24.** *If  $q \equiv 1 \pmod{3}$  then  $\mathcal{P}_{3,q}^1 \cup \mathcal{P}_{3,q}^2 \cup \mathcal{P}_{3,q}^3$  is a list  $\mathcal{P}_{3,q}^\circ$  of the soluble absolutely irreducible  $\mathbb{F}_p$ -primitive subgroups of  $\mathrm{GL}(3, q)$ ; if  $q \not\equiv 1 \pmod{3}$  then no such groups exist.*

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

## 6. ELECTRONIC ACCESS TO THE CLASSIFICATION

A database of parametrised presentations for the groups is publicly available; it is designed for MAGMA [4], but the data is available to other computer algebra systems. Its contents are procedures which encode the generating sets and constructions presented here: these take as input the degree and field and return the relevant list of groups.

The conjugating element constructed by the rewriting algorithm of Glasby & 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 is completely determined.

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

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

$q$	$k$	$t$
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

TABLE 1. Number of soluble irreducible subgroups of  $GL(3, q)$

REFERENCES

- [1] M. Aschbacher, “On the maximal subgroups of the finite classical groups”, *Invent. Math.*, **76**, 469–514, 1984.
- [2] Z.ácskai, “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**, 235–265, 1997.
- [5] S. B. Conlon, “ $p$ -groups with an abelian maximal subgroup and cyclic center”, *J. Austral. Math. Soc. Ser. A* **22**, 221–233, 1976.
- [6] J. D. Dixon, *The structure of linear groups*, Van Nostrand-Reinhold, 1971.
- [7] B. Eick and B. Höffing, “The solvable primitive permutation groups of degree at most 6560”, *LMS J. Comput. Math.* **6**, 29–39 (electronic), 2003.
- [8] W. Feit, “The current situation in the theory of finite simple groups”, *Actes du Congrès International des Mathématiciens* (Nice, 1970), *Tome 1*, pp. 55–93. Gauthier-Villars, Paris, 1971.
- [9] D. L. Flannery, *The finite irreducible linear 2-groups of degree 4*, Mem. Amer. Math. Soc. **129** no. 613, American Mathematical Society, 1997.
- [10] D. L. Flannery, “The finite irreducible monomial linear groups of degree 4”, *J. Algebra* **218** (2), 436–469, 1999.
- [11] D. L. Flannery, “Irreducible monomial linear groups of degree four over finite fields”, *Internat. J. Algebra Comput.*, to appear.
- [12] D. L. Flannery and E. A. O’Brien, “Computing 2-cocycles for central extensions and relative difference sets”, *Comm. Algebra*, **28**, 1935–1955, 2000.
- [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), 1703–1711, 1997.
- [15] D. F. Holt. “The calculation of the Schur multiplier of a permutation group”, *Computational Group Theory*, 307–318, London, New York, 1984. (Durham, 1982), Academic Press.
- [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), 207–218. *Proc. Sympos. Pure Math.* **47** (2), Amer. Math. Soc., 1987.
- [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*, Lect. 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.

Last revised December 2003

DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND, GALWAY, IRELAND  
*E-mail address:* `dane.flannery@nuigalway.ie`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF AUCKLAND, PRIVATE BAG 92019, AUCKLAND,  
NEW ZEALAND  
*E-mail address:* `obrien@math.auckland.ac.nz`