International Journal of Algebra and Computation
Vol. 14, No. 3 (2004) 253–294

IRREDUCIBLE MONOMIAL LINEAR GROUPS OF DEGREE FOUR OVER FINITE FIELDS

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

Received 15 May 2002
Revised 3 July 2002

Communicated by M. F. Newman

We describe an algorithm for explicitly listing the irreducible monomial subgroups of $\mathrm{GL}(n,q)$, given a suitable list of finite irreducible monomial subgroups of $\mathrm{GL}(n,\mathbb{C})$, where n is 4 or a prime, and q is a prime power. Particular attention is paid to the case $n = 4$, and the algorithm is illustrated for $n = 4$ and $q = 5$. Certain primitive permutation groups can be constructed from a list of irreducible monomial subgroups of $\mathrm{GL}(n,q)$. The paper's final section shows that the computation of automorphisms of such permutation groups reduces mainly to computation of irreducible monomial subgroups of $\mathrm{GL}(n,q)$, q prime.

Keywords: Monomial linear group; computing lists of irreducible linear groups.

Mathematics Subject Classification 2000: Primary 20H30, Secondary 20C15, 20H20

1. Introduction

Let $\mathbb{E}$ be a field and n be an integer, $n > 1$. A list whose elements are subgroups of $\mathrm{GL}(n,\mathbb{E})$, all with certain specified properties, is said to be *complete* if it contains a $\mathrm{GL}(n,\mathbb{E})$-conjugate of each subgroup with those properties. The list is *irredundant* if distinct elements are not $\mathrm{GL}(n,\mathbb{E})$-conjugate. Constructing a complete and irredundant list of the finite irreducible monomial subgroups of $\mathrm{GL}(n,\mathbb{E})$ for $n = 4$ and $\mathbb{E} = \mathbb{C}$ is the subject of [12]. In this paper we describe how to obtain a similar list for finite $\mathbb{E}$, and carry out the construction when $|\mathbb{E}| = 5$. This work was initially prompted by remarks in [12, Sec. 1] about classifying irreducible soluble linear groups over finite fields, after Short [25].

Throughout the paper, p is a prime and q is a power of p. Also, $\mathrm{M}(n,\mathbb{E})$ will denote the full group of monomial matrices in $\mathrm{GL}(n,\mathbb{E})$; this is the semidirect product $\mathrm{D}(n,\mathbb{E}) \rtimes S_n$, where $\mathrm{D}(n,\mathbb{E})$ is the group of diagonal matrices in $\mathrm{GL}(n,\mathbb{E})$, and S_n is the group of $n \times n$ permutation matrices (identified with the symmetric group of degree n). If $\mathbb{E} = \mathrm{GF}(q)$ then "q" replaces "$\mathbb{E}$" in the notation above.

For details of the long history of classifying finite linear groups, see [10, Sec. 8.5], [20], [26], and [27]. The main problem considered in this paper has a different aspect to classical problems in the area, which are concerned not with imprimitive linear groups at all, but rather with primitive or quasiprimitive unimodular linear groups of small degree over $\mathbb{C}$. Lists of such groups are finite. Some authors only list groups up to isomorphism of their collineation groups (central quotients), and then any finite primitive linear group over $\mathbb{C}$ is an extension of its centre by a collineation group in the relevant list. More recent classifications of finite linear groups employ the classification of finite simple groups, and have been motivated by the question of which nonabelian simple groups can occur as chief factors of absolutely irreducible linear groups over finite fields; see [20, 26]. Here again imprimitive linear groups are not of much interest. For example, the collineation group of a finite irreducible subgroup G of $\mathrm{M}(n, \mathbb{C})$ is almost simple only if the diagonal subgroup $\mathrm{D}(n, \mathbb{C}) \cap G$ of G is scalar. In prime degree n the nonabelian simple group involved therefore has a transitive permutation representation of degree n and an irreducible projective representation of degree n. This rarely happens; it is more likely that G has a rich normal structure (several classes of finite soluble linear groups over $\mathbb{C}$ — such as nilpotent groups — are monomial). Finding complete and irredundant lists of imprimitive linear groups is a hard classification problem in the theory of finite linear groups. These lists are possibly infinite, and moreover complicated in ways connected to the structure of the groups themselves (see also [2, 16]). Nor do we expect that listing groups by isomorphism type would be any easier. For example, finite irreducible linear n-groups of prime degree n over $\mathbb{C}$ are isomorphic if and only if they are conjugate in $\mathrm{GL}(n, \mathbb{C})$.

Using a standard approach, the irreducible subgroups of $\mathrm{M}(n, q)$ may be listed by computer if n and q are small enough. Critical parameters in this computation are $|\mathrm{GL}(n, q)|$, $|\mathrm{M}(n, q)| = n!(q-1)^n$, and the degrees $q^n - 1$ and $n(q-1)$ of natural faithful permutation representations of $\mathrm{GL}(n, q)$ and $\mathrm{M}(n, q)$, respectively, which are not unmanageably large at $n = 4$ and $q = 5$. We recommend our more theoretical solution of the listing problem in $\mathrm{M}(4, 5)$ for two reasons. First, it illustrates an algorithm for solving the general problem, which becomes the only feasible alternative as n and q increase. Second, it provides a way to test correctness both of the algorithm itself, and of the hugely complicated infinite list in [12], of linear groups over $\mathbb{C}$. What this means is comparing our classification of the irreducible subgroups of $\mathrm{M}(4, 5)$, which builds on that list and which has been obtained by hand, against a matching classification done by machine using standard computational techniques.

It is apt to record here that the lists in [11, 12] have errors of omission, rendering them incomplete. Errata are stated in an appendix to this paper. A note justifying the errata is available upon request from the author.

Henceforth $\mathbb{F}_p$ stands for the algebraic closure of $\mathrm{GF}(p)$; we work with a concrete version of $\mathbb{F}_p$, to be defined later. Let $\mathbb{E}$ be a subfield of $\mathbb{F}_p$. A list of the finite absolutely irreducible p'-subgroups of $\mathrm{M}(n, \mathbb{E})$ may be compiled quite straightforwardly from a list $\mathcal{L}_{n,\mathbb{C}}$ of the finite irreducible subgroups of $\mathrm{M}(n, \mathbb{C})$. The major tool is a

particular faithful representation of $\mathrm{M}(n, \mathbb{F}_p)$ in $\mathrm{M}(n, \mathbb{C})$, used to "transfer" groups between characteristics 0 and p. All of this is covered in Sec. 2 of the paper. We point out that when $\mathbb{E}$ is finite, the transfer is done only on a finite sublist of $\mathcal{L}_{n,\mathbb{C}}$, and the effectiveness of the transfer between *lists* hinges upon several requirements of $\mathcal{L}_{n,\mathbb{C}}$. One of these is the choice of $\mathrm{GL}(n, \mathbb{C})$-conjugacy class representatives, insofar as representatives that are p'-groups should contain only matrices with nonzero entries that are p'-roots of unity. Secondly, each listed group is to be given by a generating set whose diagonal elements generate the diagonal subgroup of the group. Thirdly, for given N one can compute the finite sublist of $\mathcal{L}_{n,\mathbb{C}}$ of groups of order N. If $p \geq 5$ then the list in [12] satisfies the above requirements, which are by-products of the construction process for that list.

Finite irreducible but not absolutely irreducible subgroups of $\mathrm{M}(n, \mathbb{E})$ arise in a well-understood way from irreducible subgroups of $\mathrm{GL}(m, \mathbb{F}_p)$, m a proper divisor of n, as explained in Sec. 3. Basically, a group of the former kind is a diagonal in the direct product of n/m isomorphic groups of the latter kind. Of course, if $n = 4$ and $m > 1$ then m is prime, and there is a wealth of information on classifying finite linear groups of prime degree m. The finite primitive subgroups of $\mathrm{GL}(m, \mathbb{C})$ have been described up to isomorphism of collineation group socle by Dixon and Zalesskii [8]. Complete and irredundant lists of imprimitive (hence monomial) subgroups of $\mathrm{GL}(m, \mathbb{C})$ appear in [2, 5]. These may be transferred to lists over $\mathbb{F}_p$ in the manner of Sec. 2.

We show how to list the finite absolutely irreducible subgroups of $\mathrm{M}(n, \mathbb{E})$ for $n = 4$ and $n = 2$ in Secs. 4 and 5, respectively. Section 5 includes additional information about primitive subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$, required for manufacturing the other finite irreducible subgroups of $\mathrm{M}(4, \mathbb{E})$ as per Sec. 3.

Section 6 concludes our solution of the main problem. A list of the irreducible but not absolutely irreducible subgroups of $\mathrm{M}(4, q)$ is found by applying Secs. 3 and 5. The union of that list and a complementary one yielded by the methods of Sec. 4 is a complete and irredundant list of the irreducible subgroups of $\mathrm{M}(4, q)$. In Sec. 7 we verify the list for $q = 5$ is correct, and summarize the listing algorithm developed over the course of the paper.

Finally, Sec. 8 reviews material on automorphisms of primitive permutation groups associated to linear groups. We show that, under mild restrictions, automorphisms are formed in a natural way from normalizers of monomial groups in the full general linear group over a prime field. Furthermore, those normalizers are monomial.

Although we are mostly interested in monomial linear groups of degree 4, the discussion is kept general where possible, with a view to listing irreducible monomial linear groups of other degrees over finite fields.

Notation and terminology from [12] is re-used (π is now projection from a monomial linear group of arbitrary degree n into S_n). We write tr for the trace map on square matrices.

Proofs meant to be routine are omitted and left as exercises for the reader.

2. Finite Absolutely Irreducible Nonmodular Monomial Linear Groups

Let G be a finite subgroup of $\mathrm{M}(n, \mathbb{F}_p)$. For convenience, we sometimes consider that G is a p'-group. One way to arrange this is to take p greater than n, for then p does not divide $|\pi G|$, and hence does not divide $|G| = |\mathrm{D}(n, \mathbb{F}_p) \cap G| \cdot |\pi G|$.

It is easy to demonstrate a faithful representation of G in $\mathrm{M}(n, \mathbb{C})$: just lift nonzero entries in each element of G to appropriate p'-roots of unity in $\mathbb{C}$. Provided G is a p'-group, it is almost as easy to prove that this representation is irreducible if and only if G is irreducible. We perform these tasks in the first part of this section, thereby getting an explicit special case of the following well-known result.

Theorem 2.1. *A finite irreducible p'-subgroup of $\mathrm{GL}(n, \mathbb{F}_p)$ is isomorphic to an irreducible subgroup of $\mathrm{GL}(n, \mathbb{C})$.*

Proof. See e.g. [6, Corollary 3.8, p. 62]. □

We refer to the exposition of Brauer characters in Isaacs' book [19, Chap. 15]. Zorn's Lemma implies that the ring R of algebraic integers in $\mathbb{C}$ has a maximal ideal I, containing p. Fix I and denote natural surjection $R \to R/I$ as ψ. By [19, (15.1), p. 263], R/I is the algebraic closure of $\psi(\mathbb{Z}) = \mathrm{GF}(p)$, so we take $\mathbb{F}_p$ to be R/I. Also ψ maps the largest p'-subgroup W of $\mathbb{C}^\times$ isomorphically onto $\mathbb{F}_p^\times$. Denote the inverse isomorphism θ. Put $\theta(0) = 0$, so that θ is multiplicative on $\mathbb{F}_p$, $\psi\theta$ is the identity on $\mathbb{F}_p$, and $\theta\psi$ is the identity on $W^\circ = W \cup \{0\}$. If x is an R-matrix then let $\Psi(x)$ be the $\mathbb{F}_p$-matrix of the same size with $\Psi(x)_{i,j} = \psi(x_{i,j})$. Obviously Ψ is an additive and multiplicative map on sets of R-matrices. If y is an $\mathbb{F}_p$-matrix then let $\Theta(y)$ be the W°-matrix defined by $\Theta(y)_{i,j} = \theta(y_{i,j})$. We have $\Psi\Theta(y) = y$, and $\Theta\Psi(x) = x$ for a W°-matrix x.

Lemma 2.2. *Let x, y, z be $\mathbb{F}_p$-matrices such that x is monomial and xy, zx are defined. Then $\Theta(xy) = \Theta(x)\Theta(y)$ and $\Theta(zx) = \Theta(z)\Theta(x)$.*

Corollary 2.3. *Θ is a faithful representation of $\mathrm{M}(n, \mathbb{F}_p)$ in $\mathrm{M}(n, \mathbb{C})$, with inverse Ψ.*

Remark 2.4. Corollary 2.3 implies that there is an isomorphic copy of $\mathrm{M}(n, q)$ in $\mathrm{GL}(n, \mathbb{C})$ for any q. However, if $p > n$ and $n > 2$ then there is not an isomorphic copy of $\mathrm{GL}(n, q)$ in $\mathrm{GL}(n, \mathbb{C})$. For suppose (by Proposition 2.14 below) that $\mathrm{M}(n, \mathbb{C})$ has a subgroup P isomorphic to a p-subgroup of $\mathrm{GL}(n, q)$. Since $p > n$ we have $\pi P = 1$, so P is a group of diagonal matrices and is therefore abelian. On the other hand, a Sylow p-subgroup of $\mathrm{GL}(n, q)$ is conjugate to the group of all upper triangular unipotent matrices in $\mathrm{GL}(n, q)$, which is nonabelian if $n > 2$. A faithful representation of $\mathrm{GL}(2, q)$ in $\mathrm{GL}(2, \mathbb{C})$ is irreducible. Assuming q is odd, such a representation can exist only when $q = 3$, since the irreducible complex character degrees of $\mathrm{GL}(2, q)$ are 1, $q - 1$, q, and $q + 1$; see e.g. [1, pp. 174–177]. Indeed,

if S and U are the elements of SU(2) defined in [3, Sec. 57], then S and $\sqrt{-1}U$ generate a Schur cover of S_4 in $\mathrm{GL}(2,\mathbb{C})$, isomorphic to $\mathrm{GL}(2,3)$. (The only other Schur cover of S_4 is the binary octahedral group, realized in $\mathrm{GL}(2,\mathbb{C})$ as $\langle S, U \rangle$.) Summing up: when $p > n$, $\mathrm{GL}(n,\mathbb{C})$ has a subgroup isomorphic to $\mathrm{GL}(n,q)$ if and only if $n = 2$ and $q = 3$.

Remark 2.5. Eventually we prove that the lifting Θ is an irreducible representation of each finite irreducible nonmodular subgroup of $\mathrm{M}(n,\mathbb{F}_p)$ in $\mathrm{GL}(n,\mathbb{C})$. Such representations exist for p-soluble groups (and a monomial linear group of degree at most 4 is certainly soluble). This extends Theorem 2.1 and is a consequence of the Fong–Rukolaĭne–Swan Theorem [9, Theorem 72.1, p. 473], which tells us that a Brauer character afforded by the identity automorphism of a finite irreducible p-soluble subgroup G of $\mathrm{GL}(n,\mathbb{F}_p)$ lifts to a complex irreducible character of G. That character must be faithful.

Lemma 2.6. $\Theta(\mathrm{GL}(n,\mathbb{F}_p)) \subset \mathrm{GL}(n,\mathbb{C})$.

Proof. Induction on n establishes that $\psi(\det x) = \det \Psi(x)$ for any $x \in \mathrm{Mat}(n,R)$. Thus, if $g \in \mathrm{GL}(n,\mathbb{F}_p)$ then $\det \Theta(g) \neq 0$. □

So Θ is not generally a homomorphism, but at least it is a bijection from $\mathrm{GL}(n,\mathbb{F}_p)$ onto a subset of $\mathrm{GL}(n,\mathbb{C})$.

Proposition 2.7. *Let G and H be subgroups of $\mathrm{M}(n,\mathbb{F}_p)$. If G is $\mathrm{GL}(n,\mathbb{F}_p)$-conjugate to H then $\Theta(G)$ is $\mathrm{GL}(n,\mathbb{C})$-conjugate to $\Theta(H)$.*

Proof. Suppose $G^x = H$, $x \in \mathrm{GL}(n,\mathbb{F}_p)$. By Lemma 2.2, $\Theta(G)y = y\Theta(H)$ where $y = \Theta(x)$, and y is invertible by Lemma 2.6. □

Lemma 2.8. *If g is a p'-element of $\mathrm{M}(n,\mathbb{F}_p)$ with eigenvalues $e_1,\ldots,e_n$ (counting multiplicities), then the eigenvalues of $\Theta(g)$ are $\theta(e_1),\ldots,\theta(e_n)$.*

Proof. Since g is conjugate to $\mathrm{diag}(e_1,\ldots,e_n)$, the result again follows from Lemmas 2.2 and 2.6. □

The irreducible Brauer characters of a finite p'-group (with respect to the prime p) are exactly the same as its irreducible complex characters ([19, (15.13), p. 268]). This ensures that irreducibility of monomial p'-groups is preserved when transferring between characteristics.

Theorem 2.9. *Let G be a finite irreducible p'-subgroup of $\Theta(\mathrm{M}(n,\mathbb{F}_p))$. Then Ψ is a faithful irreducible representation of G in $\mathrm{M}(n,\mathbb{F}_p)$.*

Proof. If $g \in G$ has eigenvalues $b_1,\ldots,b_n$ then, by Lemma 2.8, the eigenvalues of $\Psi(g)$ are $\psi(b_1),\ldots,\psi(b_n)$. The Brauer character afforded by Ψ has value

$\sum_{i=1}^{n} \theta\psi(b_i)$ on g, so is just tr on G. But tr is an irreducible Brauer character of G. Hence Ψ is irreducible. □

Theorem 2.10. *Let G be a finite irreducible p'-subgroup of $\mathrm{M}(n, \mathbb{F}_p)$. Then Θ is a faithful irreducible representation of G in $\mathrm{M}(n, \mathbb{C})$.*

Proof. Cf. the previous proof. The complex character of G afforded by Θ coincides with the Brauer character afforded by the identity automorphism of G, so is irreducible. □

Remark 2.11. It is not always necessary in Theorem 2.10 that G be a p'-group. Let $G = H$ wr T where H is a nontrivial finite subgroup of $\mathbb{F}_p^\times$, and T is a transitive subgroup of S_n—this includes the possibility $G = \mathrm{M}(n, q)$. Then $\Theta(G) = \theta(H)$ wr T is irreducible, whether or not G is a p'-group. For a second example, let G be a finite irreducible subgroup of $\mathrm{M}(4, \mathbb{F}_p)$ whose diagonal subgroup is self-centralizing in G. Although p may divide $|G|$, $\Theta(G)$ is irreducible by [12, Theorem 4.2]. Actually, $\Theta(G)$ is always irreducible when $\pi G = A_4$. For if $\Theta(G)$ were reducible then G would have scalar diagonal subgroup by [12, Lemma 2.1]; but $|G\colon \mathsf{Z}(G)| \geq 16$ (see e.g. [6, the exercise on p. 36]).

If $\mathbb{E}$ is a subfield of $\mathbb{F}_p$ then the absolutely irreducible subgroups of $\mathrm{GL}(n, \mathbb{E})$ are those subgroups that are irreducible over $\mathbb{F}_p$. We spend the rest of this section discussing how to list the finite absolutely irreducible p'-subgroups of $\mathrm{M}(n, \mathbb{E})$.

Let $\mathcal{L}_{n,\mathbb{C}}$ be a complete and irredundant list of the finite irreducible subgroups of $\mathrm{M}(n, \mathbb{C})$. At the time of writing there have been attempts to construct $\mathcal{L}_{n,\mathbb{C}}$ only for $n = 4$, or n a prime less than 31 (Bácskai in his Ph.D. thesis [2] accounts for the prime degrees). Therefore, realistically the proviso $p > n$ is not too severe: n is small, so the number of exceptional p is small.

In practice we will have an actual list $\ell_{n,\mathbb{C}}$ which we take to be the ideal list $\mathcal{L}_{n,\mathbb{C}}$. Now there may be errors in $\ell_{n,\mathbb{C}}$ as we have seen, and conceivably these may be transmitted to a list of subgroups of $\mathrm{M}(n, \mathbb{F}_p)$ whose construction depends on $\mathcal{L}_{n,\mathbb{C}}$. This point does not affect the validity of our methods; if an error can be detected and corrected in $\ell_{n,\mathbb{C}}$ then it can be detected and corrected in any dependent list of monomial groups over $\mathbb{F}_p$. Nonetheless any statements about completeness of that list must assume $\ell_{n,\mathbb{C}}$ is correct.

We envisage that $\mathcal{L}_{n,\mathbb{C}}$, like the lists of [2, 5, 11, 12], has each element given by a generating set of monomial matrices which can be written down explicitly from an integer parameter string labeling the group. (These strings are arbitrarily long, reflecting the fact that we can add arbitrarily many scalars to a group in $\mathcal{L}_{n,\mathbb{C}}$ without leaving $\mathcal{L}_{n,\mathbb{C}}$. However, for the application to listing subgroups of $\mathrm{M}(n, q)$, lengths of the relevant strings are related to the primes dividing $n!(q-1)$, and so are bounded in terms of n, q.) Suppose that in the generating set of each $G \in \mathcal{L}_{n,\mathbb{C}}$ the diagonal matrices form a generating set for $\mathrm{D}(n, \mathbb{C}) \cap G$; then we have no trouble calculating $|G|$ from $|\mathrm{D}(n, \mathbb{C}) \cap G|$, as πG is obvious from the non-diagonal

generators of G. Thus list groups should come with order functions, and the order of a group is found by direct substitution of its defining integer parameters into its order function (see [11, top paragraph of p. 28] for some diagonal subgroup order functions). When $p > n$, the p'-groups in $\mathcal{L}_{n,\mathbb{C}}$ can be picked out just by looking at diagonal subgroup orders. Furthermore, if for each G all nonzero generator entries are $|G|$th roots of unity then every p'-group in $\mathcal{L}_{n,\mathbb{C}}$ is in $\Theta(\mathrm{M}(n,\mathbb{F}_p))$. This latter condition is a vital requirement of $\mathcal{L}_{n,\mathbb{C}}$ in the algorithm for constructing a list of the finite irreducible p'-subgroups of $\mathrm{M}(n,\mathbb{F}_p)$, and is fulfilled by $\mathcal{L}_{4,\mathbb{C}}$ as in [12] if $p > 3$ (we postpone verification of this until Sec. 4; see the proof of Theorem 4.1). While a given list may not fulfill the requirement — entries of generators may even be torsion-free — it can always be enforced, by replacing list elements G with conjugates as necessary. Replacement is possible because there is a basis of the underlying vector space for $\mathrm{GL}(n,\mathbb{C})$ in the G-orbit of the vector $e_1 = (1, 0, \ldots, 0)$. If x is the (monomial) change of basis matrix from any such basis to the standard orthonormal one $\{e_i \mid 1 \leq i \leq n\}$, where e_i has 1 in the ith position and 0 elsewhere, then G^x has the desired property.

Let $\mathcal{L}_{n,W^\circ}$ be the sublist of $\mathcal{L}_{n,\mathbb{C}}$ consisting of all elements that are p'-subgroups of $\Theta(\mathrm{M}(n,\mathbb{F}_p))$. By the above, we may assume $\mathcal{L}_{n,W^\circ}$ contains every p'-group in $\mathcal{L}_{n,\mathbb{C}}$. Set $\mathcal{L}_{n,\mathbb{F}_p} = \Psi(\mathcal{L}_{n,W^\circ})$. By Theorem 2.9, $\mathcal{L}_{n,\mathbb{F}_p}$ is a list of finite irreducible p'-subgroups of $\mathrm{M}(n,\mathbb{F}_p)$. By Proposition 2.7, $\mathcal{L}_{n,\mathbb{F}_p}$ is irredundant. Deciding completeness of $\mathcal{L}_{n,\mathbb{F}_p}$ can be more difficult. We now set up some machinery to be used in that endeavor.

Proposition 2.12. *Let G be a group, and denote by $\mathcal{K}$ the set of equivalence classes $[\Xi]$ of its faithful irreducible representations Ξ of degree n over a fixed field $\mathbb{K}$. Suppose $\mathcal{K}$ is nonempty.*

(i) *For each $[\Xi] \in \mathcal{K}$ and $\alpha \in \mathrm{Aut}(G)$, define $[\Xi]^\alpha$ to be $[\Xi^\alpha]$, where $\Xi^\alpha(g) = \Xi(\alpha(g))$, $g \in G$. This defines an action of $\mathrm{Aut}(G)$ on $\mathcal{K}$ ($\mathrm{Inn}(G)$ acts trivially).*

(ii) *There is a bijection between the set of $\mathrm{Aut}(G)$-orbits in $\mathcal{K}$, and the set of conjugacy classes of irreducible subgroups of $\mathrm{GL}(n,\mathbb{K})$ isomorphic to G, which maps the $\mathrm{Aut}(G)$-orbit with representative $[\Xi]$ to the conjugacy class with representative $\Xi(G)$.*

Theorem 2.13. *Suppose G is a finite irreducible p'-subgroup of $\mathrm{M}(n,\mathbb{F}_p)$, such that any irreducible subgroup of $\mathrm{GL}(n,\mathbb{C})$ isomorphic to G is conjugate to a group in $\mathcal{L}_{n,W^\circ}$. Then G is conjugate to a group in $\mathcal{L}_{n,\mathbb{F}_p}$.*

Proof. Say $\mathrm{Aut}(G)$ has m orbits in $\{\xi \in \mathrm{Irr}(G) \mid \xi \text{ faithful}, \xi(1) = n\}$, which is nonempty by Theorem 2.10. By Proposition 2.12 and hypothesis, $\mathcal{L}_{n,W^\circ}$ has m elements isomorphic to G. Consequently $\mathcal{L}_{n,\mathbb{F}_p}$ has m elements isomorphic to G. Since $\mathrm{Irr}(G) = \mathrm{IBr}(G)$, there are m orbits of $\mathrm{Aut}(G)$ in $\{\xi \in \mathrm{IBr}(G) \mid \xi \text{ faithful}, \xi(1) = n\}$. This set is bijective with the set of equivalence classes of faithful irreducible

representations of G in $\mathrm{GL}(n, \mathbb{F}_p)$, so there is a conjugate of G in $\mathcal{L}_{n,\mathbb{F}_p}$ by Proposition 2.12 again. □

Theorem 2.13 motivates us to ask which finite irreducible subgroups of $\mathrm{GL}(n, \mathbb{C})$ can be isomorphic to irreducible subgroups of $\mathrm{M}(n, \mathbb{C})$. Some qualified answers to this question follow (the first merely states a well-known class of M-groups).

Proposition 2.14. *Let G be a finite soluble subgroup of $\mathrm{GL}(n, \mathbb{C})$ with a normal subgroup N such that all Sylow subgroups of N are abelian, and G/N is supersoluble. Then G is conjugate to a subgroup of $\mathrm{M}(n, \mathbb{C})$.*

Proof. See [19, (6.22), (6.23), p. 87]. □

Theorem 2.15. *Let n be prime. If G is a finite irreducible subgroup of $\mathrm{M}(n, \mathbb{C})$ then G is not isomorphic to a primitive subgroup of $\mathrm{GL}(n, \mathbb{C})$.*

Proof. Denote the group of all scalars in $\mathrm{GL}(n, \mathbb{C})$ by Z. Suppose G is isomorphic to a primitive subgroup H of $\mathrm{GL}(n, \mathbb{C})$. Then $n \geq 5$: otherwise we get the contradiction that H is abelian-by-supersoluble and conjugate to a subgroup of $\mathrm{M}(n, \mathbb{C})$ by Proposition 2.14.

An abelian normal subgroup of a primitive linear group over an algebraically closed field is scalar (this famous result usually attributed to Blichfeldt). Hence $\mathsf{Z}(G) = G \cap Z$ is a maximal abelian normal subgroup of G. The diagonal subgroup of G contains $\mathsf{Z}(G)$, so it is precisely $\mathsf{Z}(G)$, and $G/\mathsf{Z}(G) \cong \pi G$.

There is an inclusion-preserving map from each finite subgroup K of $\mathrm{GL}(n, \mathbb{C})$ to a finite subgroup $\hat{K}$ of $\mathrm{SL}(n, \mathbb{C})$, such that $KZ = \hat{K}Z$ and $\hat{K}/\mathsf{Z}(\hat{K}) \cong K/\mathsf{Z}(K)$. Clearly $\hat{H}$ is primitive, and $\hat{H}/\mathsf{Z}(\hat{H}) \cong \pi G$. The finite primitive subgroups of $\mathrm{SL}(n, \mathbb{C})$ are described in [8]. By [8, Lemma 1.1], $S := \mathrm{soc}(\pi G)$ is either elementary abelian of order n^2, or is a nonabelian simple group and has trivial centralizer in πG (that is, πG is almost simple). As a transitive permutation group of prime degree, πG has a transitive normal simple subgroup N by [17, Satz 21.1(e), pp. 607–608], so $N \leq S$. If N were abelian then G would have an abelian normal subgroup properly containing $\mathsf{Z}(G)$, contradicting maximality of $\mathsf{Z}(G)$. Thus $S = N$ is a nonabelian simple group, and is listed in [8, Theorem 1.2].

Let L be a (normal) subgroup of H such that $\mathsf{Z}(H) \leq L$ and $L/\mathsf{Z}(H) \cong S$. Since L is nonabelian and we are in prime degree, L is irreducible by Clifford's Theorem. Thus $\mathsf{Z}(H) = \mathsf{Z}(L)$, $\mathsf{Z}(\hat{H}) = \mathsf{Z}(\hat{L})$ and $\hat{L}/\mathsf{Z}(\hat{H}) \cong S$. $\hat{L}$ splits over $\mathsf{Z}(\hat{H})$ (see [8, remarks after Theorem 1.2]), and so there is a subgroup T of $\hat{L}$ such that $T \trianglelefteq \hat{H}$, $T \cap Z = 1$, and $T \cong S$. Since $L \trianglelefteq \hat{L}Z$ we have $L \trianglelefteq TZ$. Denote the projection of TZ onto T by ϱ. Certainly $\varrho(L) \trianglelefteq T$, and $L \not\leq Z$ implies $\varrho(L) = T$. Define a homomorphism $\alpha\colon T \to Z/\mathsf{Z}(L)$ by $\alpha(t) = z\mathsf{Z}(L)$, where $tz \in L$, $z \in Z$. Of course $\ker \alpha = T$, so $T \leq L$. Moreover $T \trianglelefteq H$. Hence $\mathrm{M}(n, \mathbb{C})$ has an irreducible subgroup isomorphic to S. As noted in [8, proof of Theorem 1.2], a faithful permutation representation of S has degree greater than n, unless $n = 11$ and $S \cong \mathrm{PSL}(2, 11)$.

But the single conjugacy class of irreducible subgroups of $\mathrm{GL}(11,\mathbb{C})$ isomorphic to $\mathrm{PSL}(2,11)$ contains only primitive groups. This completes the proof. □

Remark 2.16. We commented in Sec. 1 on the rarity of nonabelian simple groups S possessing a transitive permutation representation of the same prime degree as an irreducible projective representation of S. If $q > 2$, $m \geq 3$ and $d = (q^m - 1)/(q-1)$ is prime, then $\mathrm{PSL}(m,q)$ in degree d is such a group. Also, $\mathrm{M}(5,\mathbb{C})$ has a subgroup $S \cong A_5$.

Theorem 2.17. *Let G be a finite irreducible p'-subgroup of $\mathrm{M}(n,\mathbb{F}_p)$, so $\Theta(G)$ is conjugate to a group in $\mathcal{L}_{n,\mathbb{C}}$. Assuming every p'-group in $\mathcal{L}_{n,\mathbb{C}}$ is in $\mathcal{L}_{n,W^\circ}$, if any of the following hold then G is conjugate to a group in $\mathcal{L}_{n,\mathbb{F}_p}$.*

(i) *πG is supersoluble.*
(ii) *n is prime.*
(iii) *$|\pi G| = n$.*

Proof. All parts are instances of Theorem 2.13. By that result, (i) and (ii) follow from Proposition 2.14 and Theorem 2.15. For (iii), let H be an irreducible subgroup of $\mathrm{GL}(n,\mathbb{C})$ isomorphic to G and let χ be an irreducible constituent of tr on H restricted to an abelian normal subgroup of index n. The induced character χ^H has degree n and hence $\chi^H = \mathrm{tr}$ by Frobenius reciprocity. Since χ^H is afforded by a monomial representation, this proves (iii). (Cf. [11, Proposition 1.3.6].) □

In degree 4, Theorem 2.17 is not enough to determine whether $\mathcal{L}_{n,\mathbb{F}_p}$ is complete. The next result provides extra assistance (and a partial converse of Proposition 2.7).

Proposition 2.18. *Let G and H be subgroups of $\mathrm{M}(n,\mathbb{F}_p)$, with πG transitive. Then G is $\mathrm{M}(n,\mathbb{F}_p)$-conjugate to H if and only if $\Theta(G)$ is $\mathrm{M}(n,\mathbb{C})$-conjugate to $\Theta(H)$.*

Proof. (Cf. [11, Remark 1.3.8] and [12, Lemma 5.6].) Suppose $\Theta(G)^{sx} = \Theta(H)$ for some $x \in \mathrm{D}(n,\mathbb{C})$ and $s \in S_n$. That is, $\Theta(G^s)^x = \Theta(H)$, so $xx^{-t} \in \Theta(\mathrm{D}(n,\mathbb{F}_p))$ for all $t \in \pi G^s$. Since πG^s is transitive, $x = \Theta(y)$ for some $y \in \mathrm{D}(n,\mathbb{F}_p)$, modulo scalars. Thus $G^{sy} = H$. Corollary 2.3 takes care of the other implication. □

Corollary 2.19. *Let G be a finite irreducible p'-subgroup of $\mathrm{M}(n,\mathbb{F}_p)$. If $\Theta(G)$ is $\mathrm{M}(n,\mathbb{C})$-conjugate to $K \in \mathcal{L}_{n,W^\circ}$ then G is $\mathrm{M}(n,\mathbb{F}_p)$-conjugate to $\Psi(K) \in \mathcal{L}_{n,\mathbb{F}_p}$.*

We say no more about how to prove that $\mathcal{L}_{n,\mathbb{F}_p}$ is complete, and suppose that it is complete. The next step in listing absolutely irreducible subgroups of $\mathrm{M}(n,\mathbb{E})$ for a subfield $\mathbb{E}$ of $\mathbb{F}_p$ is to recognize the $\mathbb{E}$-*monomial* elements of $\mathcal{L}_{n,\mathbb{F}_p}$, which is to say, the groups that are $\mathrm{GL}(n,\mathbb{F}_p)$-conjugate to subgroups of $\mathrm{M}(n,\mathbb{E})$. By deleting from $\mathcal{L}_{n,\mathbb{F}_p}$ the groups that are not $\mathbb{E}$-monomial, and replacing each $\mathbb{E}$-monomial group with a conjugate in $\mathrm{M}(n,\mathbb{E})$, we obtain a list $\mathcal{L}_{n,\mathbb{E}}$. The Deuring–Noether

Theorem [18, Theorem 1.22, p. 26] asserts that representations of a finite group over a given field are equivalent if and only if they are equivalent over every extension of the field. This theorem guarantees that $\mathcal{L}_{n,\mathbb{E}}$ is a complete list of the finite absolutely irreducible p'-subgroups of $\mathrm{M}(n,\mathbb{E})$. We know already that $\mathcal{L}_{n,\mathbb{E}}$ is irredundant, so it is a list of the kind sought.

The subgroups of $\mathrm{M}(n,\mathbb{E})$ in $\mathcal{L}_{n,\mathbb{F}_p}$ are readily apparent. To recognize the other $\mathbb{E}$-monomial groups in $\mathcal{L}_{n,\mathbb{F}_p}$, we calculate traces.

Theorem 2.20. *Let $\mathbb{K}$ be a subfield of $\mathbb{F}_p$, $\mathbb{E} \subseteq \mathbb{K}$. A finite irreducible subgroup G of $\mathrm{GL}(n,\mathbb{K})$ is conjugate to a subgroup of $\mathrm{GL}(n,\mathbb{E})$ if and only if $\mathrm{tr}(G) \subseteq \mathbb{E}$.*

Proof. See [19, (9.23), p. 155]. □

Corollary 2.21. *Let $\mathbb{K}$ be a subfield of $\mathbb{F}_p$, $\mathbb{E} \subseteq \mathbb{K}$. Let G be a finite irreducible r-subgroup of $\mathrm{GL}(n,\mathbb{K})$, where $r \neq p$ is a prime. Suppose $\mathbb{E}$ has a primitive rth root of unity if $r > 2$, and a primitive fourth root of unity if $r = 2$. Then G is $\mathbb{E}$-monomial if and only if $\mathrm{tr}(G) \subseteq \mathbb{E}$.*

Proof. Note that if G is absolutely irreducible then n must be a power of r. By [21, Theorems II.4 and III.4], there is a Sylow r-subgroup of $\mathrm{GL}(n,\mathbb{E})$ in $\mathrm{M}(n,\mathbb{E})$. Then the result follows from Theorem 2.20. □

Now let $\mathbb{E} = \mathrm{GF}(q)$, $q \geq 3$. Suppose $G \in \mathcal{L}_{n,\mathbb{F}_p}$ and $\mathrm{tr}(G) \subseteq \mathrm{GF}(q)$. We seek $x \in \mathrm{GL}(n,\mathbb{F}_p)$ such that $G^x \leq \mathrm{M}(n,q)$. Clearly $G \leq \mathrm{GL}(n,q^m)$ for some $m \geq 1$; $\mathrm{GF}(q^m)$ could be the subfield of $\mathbb{F}_p$ generated by $\mathrm{GF}(q)$ and the entries of all elements of G.

Suppose x is monomial. This can happen only if $\mathrm{D}(n,\mathbb{F}_p) \cap G \leq \mathrm{D}(n,q)$. We assume that x is diagonal, because $y = x(\pi x)^{-1}$ is diagonal and $G^y \leq \mathrm{M}(n,q)$. Then reasoning as in the proof of Proposition 2.18 shows that x acts as an element of $\mathrm{D}(n,q^m)$. The assumption that x is monomial therefore leads to a significant reduction in size of a search space for x. However, if we know enough about the πG-module structure of $\mathrm{D}(n,\mathbb{F}_p)$ then we do not need to search all of $\mathrm{D}(n,q^m)$, since that knowledge would inform the (possibly heuristic) choice of x. When n is prime or $n = 4$, this last point is illustrated in the proofs of [5, Lemma 1.7], [11, Theorem 3.2.9], [12, Theorem 7.2], and Theorem 4.5 below.

If x is not monomial then to rewrite G in $\mathrm{M}(n,q)$ one can turn to the computer. We now give a procedure for rewriting G using Magma [4]. First, we find the smallest subfield $\mathbb{K}$ of $\mathrm{GF}(q^m)$ such that $\mathrm{GL}(n,\mathbb{K})$ contains a $\mathrm{GL}(n,q^m)$-conjugate G^* of G. This may be done with the Magma function `IsOverSmallerField` (based on [14]). Then the function `LineOrbits` is used to compute all orbits of G^* on one-dimensional subspaces of the underlying space $\mathrm{GF}(q)^{(n)}$. We should have that (i) $\mathbb{K} \subseteq \mathrm{GF}(q)$, and (ii) there is an orbit of G^* consisting of n one-dimensional subspaces $\langle\, l_j \,\rangle$, whose sum is $\mathrm{GF}(q)^{(n)}$. (If (i) or (ii) is false then G is not $\mathrm{GF}(q)$-monomial, so we discard G and move on to another group in $\mathcal{L}_{n,\mathbb{F}_p}$.) The Magma convention

is that elements of a matrix group act on the right of the underlying space, so that $mG^*m^{-1} \leq \mathrm{M}(n,q)$ for the change of basis matrix m whose jth row is l_j. Then mG^*m^{-1} replaces G in $\mathcal{L}_{n,\mathbb{E}}$.

Sometimes the above procedure for computing G^x in $\mathrm{M}(n,q)$ can be avoided when $n = 4$. In the proof of Theorem 4.5 we utilize the following lemma to good effect, in working out conjugacy between finite irreducible subgroups of $\mathrm{M}(4,\mathbb{F}_p)$ by elements of $\mathrm{GL}(4,\mathbb{F}_p)\backslash\mathrm{M}(4,\mathbb{F}_p)$.

Lemma 2.22. *Let G, H be subgroups of $\mathrm{GL}(n,\mathbb{C})$ consisting of R-matrices, and suppose $G^x = H$ for some R-matrix $x \in \mathrm{GL}(n,\mathbb{C})$ such that $\psi(\det x) \neq 0$ (for example, $\det x$ is an integer not divisible by p). Then $\Psi(G)$ is $\mathrm{GL}(n,\mathbb{F}_p)$-conjugate to $\Psi(H)$.*

3. Irreducible but not Absolutely Irreducible Linear Groups

The theory of irreducible representations of a finite group over extensions of the ground field is treated in several texts, such as [6, 18, 19].

Theorem 3.1. *Let $\mathbb{E}$ be a field of characteristic p.*

(i) *Let G be an irreducible but not absolutely irreducible finite subgroup of $\mathrm{GL}(n,\mathbb{E})$. Then there are*

(a) *an integer $m > 1$ dividing n,*
(b) *a Galois extension $\mathbb{K}$ of $\mathbb{E}$ of degree m with Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) = \{\sigma_i \,|\, 1 \leq i \leq m\}$,*
(c) *an absolutely irreducible subgroup H of $\mathrm{GL}(n/m,\mathbb{K})$, where $\mathrm{tr}(H) \not\subseteq \mathbb{L}$ for any proper subfield $\mathbb{L}$ of $\mathbb{K}$ containing $\mathbb{E}$,*

such that G is $\mathrm{GL}(n,\mathbb{K})$-conjugate to the group $\tilde{G}$ of block diagonal matrices

$$(h^{\sigma_1}, h^{\sigma_2}, \ldots, h^{\sigma_m}) := \begin{pmatrix} h^{\sigma_1} & 0 & \cdots & 0 \\ 0 & h^{\sigma_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h^{\sigma_m} \end{pmatrix}, \qquad h \in H\,.$$

Therefore,

$$(h^{\sigma_1}, h^{\sigma_2}, \ldots, h^{\sigma_m}) \mapsto h^{\sigma_i} \qquad (\dagger)$$

defines a faithful absolutely irreducible representation of $\tilde{G}$ in $\mathrm{GL}(n/m,\mathbb{K})$ for each i. In particular, $G \cong H$.

(ii) *Conversely, suppose m, $\mathbb{K}$, and H satisfy* (a), (b), *and* (c) *in* (i). *Then $\tilde{G}$ is conjugate to an irreducible but not absolutely irreducible subgroup of $\mathrm{GL}(n,\mathbb{E})$.*

Proof. Part (i) paraphrases [19, (9.21), p. 154] and its proof. Note that $\mathbb{E}$ and $\mathrm{tr}(H)$ generate $\mathbb{K}$.

Conversely, let Λ be the representation (†) for $i = 1$, assuming σ_1 is the identity of $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$. (The elements of $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ may be ordered any way we like: conjugation by a permutation matrix yields $\tilde{G}$ as indicated with a chosen ordering.) By [19, (9.5)(c), p. 147] and [19, (9.23), p. 155] there is a faithful irreducible representation Γ of G in $\mathrm{GL}(n, \mathbb{E})$ such that Λ is an irreducible constituent of Γ viewed as a $\mathbb{K}$-representation. Certainly Λ^{σ_i} is an irreducible constituent of $\Gamma = \Gamma^{\sigma_i}$ for all i, $1 \leq i \leq m$. These constituents are pairwise inequivalent. Otherwise, some nonidentity element τ of $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ would fix the character afforded by Λ; but then τ would fix $\mathrm{tr}(H)$ elementwise and so be the identity on $\mathbb{K}$. Comparing degrees, we then see that the $\mathbb{K}$-irreducible constituents of Γ are precisely the Λ^{σ_i}. Since Γ is completely reducible over any extension of $\mathbb{E}$, with irreducible constituents uniquely determined up to equivalence, $\Gamma(G)$ is conjugate to $\tilde{G}$. □

The notation of Theorem 3.1 is used in the next two results.

Corollary 3.2. *If n is prime then G is abelian.*

Corollary 3.3. *Let G be abelian.*

(i) *G is conjugate to a cyclic subgroup of $\mathrm{D}(n, \mathbb{K})$, every element of which has all nonzero entries of the same order (thus $|G|$ is not divisible by p).*
(ii) *By* (i), *G is isomorphic to a subgroup of $\mathbb{K}^\times$. However, G is not isomorphic to a subgroup of $\mathbb{L}^\times$ for any proper subfield $\mathbb{L}$ of $\mathbb{K}$ containing $\mathbb{E}$.*
(iii) *If H is an abelian irreducible subgroup of $\mathrm{GL}(n, \mathbb{E})$ of order $|G|$ then H is $\mathrm{GL}(n, \mathbb{E})$-conjugate to G.*

Proof. An absolutely irreducible abelian linear group has degree 1. Then by Theorem 3.1, G is $\mathrm{GL}(n, \mathbb{K})$-conjugate to the cyclic group generated by $(\omega^{\sigma_1}, \omega^{\sigma_2}, \ldots, \omega^{\sigma_n})$, where $\omega \in \mathbb{K}$ is a primitive $|G|$th root of unity not in any proper subfield of $\mathbb{K}$ containing $\mathbb{E}$, and $\sigma_1, \sigma_2, \ldots, \sigma_n$ are the elements of $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ in some fixed order. This gives (i) and (ii); (iii) follows from the Deuring–Noether Theorem. □

The following criterion for absolute irreducibility supplements Theorem 2.9.

Corollary 3.4. *Let $\mathbb{E}$ be a subfield of $\mathbb{F}_p$. If G is a finite irreducible subgroup of $\mathrm{M}(n, \mathbb{E})$ such that $\Theta(G)$ (in the notation of Sec.* 2) *is an irreducible subgroup of $\mathrm{M}(n, \mathbb{C})$, then G is absolutely irreducible.*

Proof. Of course, if G is a p'-group then by Theorem 2.9 there is nothing to do.

Only scalars in $\mathrm{GL}(n, \mathbb{C})$ centralize $\Theta(G)$. However, if G is not absolutely irreducible then $\mathsf{C}_{\mathrm{GL}(n,\mathbb{F}_p)}(G)$ has nonscalar elements by Theorem 3.1. This is a contradiction, by the argument in the proof of Proposition 2.7. □

Next, we derive some more consequences of Theorem 3.1 in degrees relevant to our main problem. Denote the qth-powering automorphism of $\mathbb{F}_p$ as σ.

Corollary 3.5. *Suppose $n = rs$, r and s prime. Let G be an irreducible but not absolutely irreducible nonabelian subgroup of $\mathrm{GL}(n, q)$. Then there is an absolutely irreducible subgroup H of $\mathrm{GL}(n/m, q^m)$, where $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$ and $m = r$ or $m = s$, such that G is $\mathrm{GL}(n, q^m)$-conjugate to $\{(h, h^\sigma, h^{\sigma^2}, \ldots, h^{\sigma^{m-1}}) \,|\, h \in H\}$. Conversely, any such group of block diagonal matrices is conjugate to an irreducible but not absolutely irreducible subgroup of $\mathrm{GL}(n, q)$.*

Proof. The Galois group here is cyclic of order m, generated by σ, so the first part is clear. For the second, we need only observe that $\mathrm{GF}(q^m)$ is generated by $\mathrm{GF}(q)$ and $\mathrm{tr}(H)$, because m is prime and $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$. □

Proposition 3.6. *Let G be an irreducible but not absolutely irreducible nonabelian subgroup of $\mathrm{M}(4, q)$, with diagonal subgroup N. As in Corollary* 3.5, *let H be an absolutely irreducible subgroup of $\mathrm{GL}(2, q^2)$ isomorphic to G, such that $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$ and G is $\mathrm{GL}(4, q^2)$-conjugate to $\{(h, h^\sigma) \,|\, h \in H\}$. Then, up to conjugacy, one of the following occurs.*

(i) *πG is A_4 or S_4, $\mathsf{Z}(G) = N$ is scalar, and H is a primitive subgroup of $\mathrm{GL}(2, q^2)$.*
(ii) *πG is a transitive 2-subgroup of S_4, and $H \leq \mathrm{M}(2, q^2)$.*

Moreover, a group as in (i) *is not isomorphic to a group as in* (ii).

Proof. Let $\Lambda: G \to H$ be an isomorphism. Suppose πG is A_4 or S_4. If H is imprimitive then (as we are in prime degree) $H \leq \mathrm{M}(2, q^2)$ up to conjugacy. But then G has an abelian subgroup of index 2, which is clearly false. Thus H is primitive. By Blichfeldt's result (referenced in the proof of Theorem 2.15), $\Lambda(N) \leq \mathsf{Z}(H)$. Since $\mathsf{Z}(A_4) = \mathsf{Z}(S_4) = 1$, it follows that $\Lambda(N) = \mathsf{Z}(H)$, and thus $N = \mathsf{Z}(G)$. The conjugation action of G on the diagonal entries of an element of N is transitive, so N must be scalar.

If πG is not A_4 nor S_4 then it is a transitive 2-subgroup of S_4, so has order 4 or is dihedral of order 8. Therefore H has a series $\Lambda(N) = H_0 < H_1 < \cdots < H_k = H$ of normal subgroups, where $k = 2$ or 3 and $|H_{i+1} : H_i| = 2$. Then H cannot be isomorphic to a primitive subgroup of $\mathrm{GL}(2, q^2)$; otherwise, we discover by repeated use of Blichfeldt's result that H is abelian. This completes the proof. □

Remark 3.7. In Proposition 3.6(ii), G has an abelian subgroup A of index 2 such that $N \leq A$. When πG is dihedral of order 8, A can be the image of $\mathrm{D}(2, q^2) \cap H$ under an isomorphism $H \to G$. Suppose $|\pi G| = 4$; then $N \neq \mathsf{C}_G(N)$. For if $\mathsf{C}_G(N) = N$ then $\Theta(G)$ is irreducible by [12, Theorem 4.2], but the degree of an irreducible complex character of G is 1 or 2 by [19, (6.15), p. 84]. Thus $\mathsf{C}_G(N)/N$ has a subgroup of order 2, and we may take A to be its inverse image in G.

Remark 3.8. More than the last claim in Proposition 3.6 is true, by [12, Proposition 9.1]: if G, H are isomorphic finite subgroups of $\mathrm{M}(4, \mathbb{F}_p)$ then either $\pi G = \pi H$ is A_4 or S_4, or πG and πH are both 2-groups.

By Proposition 3.6, to list the irreducible but not absolutely irreducible nonabelian subgroups of $\mathrm{M}(4,q)$, we need information about absolutely irreducible subgroups of $\mathrm{GL}(2,q^2)$. This is supplied in Sec. 5.

If H is an absolutely irreducible subgroup of $\mathrm{GL}(2,q^2)$ not conjugate to a subgroup of $\mathrm{GL}(2,q)$ then we prove in Sec. 6 that $G = \{(h,h^\sigma) \mid h \in H\}$ is conjugate to an irreducible subgroup of $\mathrm{M}(4,q)$ when $q \equiv 1 \bmod 4$ and $H \leq \mathrm{M}(2,q^2)$. We do the same for $p \geq 5$, $q \equiv 2 \bmod 3$, and $H/\mathsf{Z}(H) \cong A_4$ (the second condition is necessary, given the other two). If $H/\mathsf{Z}(H) \cong S_4$ then by the next proposition G cannot be conjugate to a subgroup of $\mathrm{M}(4,q)$.

Proposition 3.9. *Suppose $p \geq 5$, and let G be an irreducible subgroup of $\mathrm{M}(4,q)$ such that $\pi G = S_4$. Then G is absolutely irreducible.*

Proof. Suppose G is not absolutely irreducible. By Proposition 3.6, let H be an absolutely irreducible primitive subgroup of $\mathrm{GL}(2,q^2)$ isomorphic to G such that $H/\mathsf{Z}(H) \cong S_4$. Denote the centre of G by Z and the Hall $2'$-subgroup of Z by $\bar{Z}$. As $H^i(Z/\bar{Z},\bar{Z})$ is trivial for all $i \geq 1$, we have $H^2(G/\bar{Z},\bar{Z}) = H^2(G/Z,\bar{Z})$, and the latter cohomology group is $\mathrm{Ext}(C_2,\bar{Z}) \times \mathrm{Hom}(H_2(S_4),\bar{Z}) = 1$ by the Universal Coefficient Theorem. That is, G splits over its subgroup of odd order scalars, and we may assume Z is a 2-group.

The rest of the proof incorporates suggestions by L. G. Kovács. Let K be a subgroup of G such that $\pi K \cong S_3$. Choose $g \in K'$ of order 3, so $\det g = 1$. For some $s \in G$, $(\pi g)^{\pi s} = \pi g^{-1}$, meaning $g^s \equiv g^{-1}$ modulo Z. Thus $g^s = g^{-1}$. If g is conjugate to (h,h^σ), $h \in H$, then h is inverted by an inner automorphism of H, and so $\mathrm{tr}(h) = \mathrm{tr}(h^{-1})$. Hence h is conjugate to a diagonal matrix (α,α^{-1}), α a primitive cube root of unity. It follows that $\mathrm{tr}(h) = -1$ and $\mathrm{tr}(g) = -2$.

The permutation group πK is intransitive, with a single fixed point. Thus K fixes a one-dimensional subspace of $\mathrm{GF}(q)^{(4)}$. In turn K' fixes a nonzero vector, and g has eigenvalue 1. The product of the other three eigenvalues of g (cube roots of unity in $\mathbb{F}_p$) is therefore 1, and their sum is -3. This is impossible in characteristic greater than 3. □

Corollary 3.10. *If $p \geq 5$, then an irreducible subgroup of $\mathrm{M}(4,q)$ isomorphic to an absolutely irreducible subgroup of $\mathrm{M}(4,q)$ is absolutely irreducible.*

Proof. Suppose $G \leq \mathrm{M}(4,q)$ is absolutely irreducible. If $\pi G = A_4$ then $\mathsf{Z}(G) \neq \mathrm{D}(4,q) \cap G$, and if πG is a 2-group then G does not have an abelian subgroup of index 2. The result follows from Proposition 3.6, Remark 3.8, and Proposition 3.9. □

Proposition 3.11. *Let p be odd. If G is an irreducible nonabelian subgroup of $\mathrm{M}(4,q)$ then $|G| \geq 16$.*

Proof. If G is absolutely irreducible then $|G : \mathsf{Z}(G)| \geq 16$, so we assume G is not absolutely irreducible. Thus G is isomorphic to an absolutely irreducible subgroup H of $\mathrm{GL}(2, q^2)$ such that $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$. Denote the diagonal subgroup of H by M.

$|G|$ is properly divisible by 4. Suppose $|G| = 8$. Then H is (conjugate to) a subgroup of $\mathrm{M}(2, q^2)$. On $H \backslash M$ the trace map is zero. Let $h \in M$. Either $h \in \mathrm{D}(2, q)$ or $\mathrm{tr}(h) = \omega + \omega^{-1} = 0$ for a primitive fourth root of unity ω. Thus $\mathrm{tr}(H) \subseteq \mathrm{GF}(q)$, a contradiction.

Suppose $|G| = 12$. Since A_4 has a noncentral abelian normal subgroup, H is monomial by Proposition 3.6. In this case M is generated by a scalar involution and a nonscalar element of order 3 in $\mathrm{SL}(2, q^2)$. We then calculate that $\mathrm{tr}(H) \subseteq \{0, \pm 1, \pm 2\} \subseteq \mathrm{GF}(q)$. □

The next result extends Proposition 3.11 to all irreducible $G \leq \mathrm{M}(4, q)$.

Proposition 3.12. (i) $\mathrm{M}(4, q)$ *has irreducible abelian* (*i.e. cyclic*) *subgroups if and only if* $q \equiv 1 \bmod 4$.

(ii) *Suppose* $q \equiv 1 \bmod 4$. *A cyclic subgroup of* $\mathrm{M}(4, q)$ *is irreducible if and only if it is* $\mathrm{GL}(4, q)$*-conjugate to* $\langle\, c(\omega, 1, 1, 1) \,\rangle$, *where* $\omega \in \mathrm{GF}(q)^\times$ *has order* $(q-1)/r$ *for some odd divisor* r *of* $q - 1$, *and* c *is a* 4*-cycle in* S_4.

Proof. Let G be a cyclic irreducible subgroup of $\mathrm{M}(4, q)$. Since πG is conjugate to $\langle\, c \,\rangle$, $|G|$ is divisible by 4 and G has scalar diagonal subgroup. Thus $|G| = 4s$ for some divisor s of $q - 1$. By Corollary 3.3, $|G|$ divides $q^4 - 1$ but not $q^2 - 1$. Consequently q is odd. Also $q \equiv 1 \bmod 4$, because otherwise $q^2 - 1$ is divisible by $4(q - 1)$ and hence by $|G|$. Similarly, if $(q - 1)/s$ were even then $|G|$ would divide $q^2 - 1 = ((q - 1)/s)(q + 1)s$.

Now suppose $q \equiv 1 \bmod 4$ and let G be a cyclic subgroup of $\mathrm{M}(4, q)$, $|G| = 4(q - 1)/r$, r odd ($G = \langle\, c(\omega, 1, 1, 1) \,\rangle$ fits the bill). Note then that $|G|$ divides $q^4 - 1$ but not $q^2 - 1$, and that G is completely reducible by Maschke's Theorem. Suppose G is reducible. Then the irreducible components of G have orders dividing $q - 1$, $q^2 - 1$, or $q^3 - 1$, and therefore dividing $q^2 - 1$, since $\gcd(q^4 - 1, q^3 - 1) = q - 1$. However, $|G|$ is the least common multiple of these orders: contradiction. By Corollary 3.3(iii), we are done. □

4. Finite Absolutely Irreducible Monomial Linear Groups of Degree Four

Recall the notation of Sec. 2. In this section we let $\mathcal{L}_{4,\mathbb{C}}$ be the list $\ell_{4,\mathbb{C}}$ of [12, Theorem 9.2], amended as per the Appendix. Define $\mathcal{L}_{4,W^\circ}$ and $\mathcal{L}_{4,\mathbb{F}_p}$ accordingly. We first prove that $\mathcal{L}_{4,\mathbb{F}_p}$ is a complete list of the finite irreducible subgroups of $\mathrm{M}(4, \mathbb{F}_p)$ when $p \geq 5$, assuming correctness of $\ell_{4,\mathbb{C}}$. Then we go on to list the absolutely irreducible subgroups of $\mathrm{M}(4, 5)$.

From now on, the letters a, b, c, d, and e are reserved to denote the permutation matrices obtained from the 4×4 identity matrix by permuting its columns as (12)(34), (13)(24), (1234), (123), and (12), respectively. Up to conjugacy, the

transitive subgroups of S_4 are $V_4 = \langle a, b \rangle$, $C = \langle c \rangle$, $D = \langle a, c \rangle$, $A_4 = \langle a, b, d \rangle$, and $S_4 = \langle a, d, e \rangle$. For relations between generators of S_4, see [12, Sec. 1]. We have $\mathrm{D}(4, \mathbb{C}) = XYUV$, where X is all scalars, Y is the subgroup of $\mathrm{D}(4, \mathbb{C})$ whose elements are fixed by a and inverted by b, $U = Y^{de}$, and $V = Y^d$. Note that $YUV \leq \mathrm{SL}(4, \mathbb{C})$. The torsion subgroup of $\mathrm{D}(4, \mathbb{C})$ is denoted B. If M is a group of diagonal matrices (over any field) and ς is a set of primes then $M_\varsigma := \mathsf{O}_\varsigma(M)$. Clearly B_ς is the direct product $\prod_{r \in \varsigma} B_r$, and $B_r = X_r Y_r U_r V_r$, a direct product only if r is odd. Every group in $\mathcal{L}_{4,\mathbb{C}}$ consists of R-matrices. Even more is true: by consulting $\mathcal{L}_{4,\mathbb{C}}$ (and cf. [12, Theorem 3.11]), we see that

> each $H \in \mathcal{L}_{4,\mathbb{C}}$ is the semidirect product of a diagonal matrix group with a subgroup of $B_2 B_3 S_4$, and $H = (B_2 X_3 S_4 \cap H)\,(B \cap H)$. (∗)

Theorem 4.1. *Let $p \geq 5$, and assume $\ell_{4,\mathbb{C}}$ is correct. Then a finite irreducible subgroup G of $\mathrm{M}(4, \mathbb{F}_p)$ is conjugate to a group in $\mathcal{L}_{4,\mathbb{F}_p}$.*

Proof. By Theorem 2.10, [12, Theorem 9.2] (and assuming $\ell_{4,\mathbb{C}}$ is correct), $\Theta(G)$ is conjugate to a group $H \in \mathcal{L}_{4,\mathbb{C}}$. Since a finite p'-subgroup of $\mathrm{D}(n, \mathbb{C})$ is contained in $\Theta(\mathrm{D}(n, \mathbb{F}_p))$, every p'-group in $\mathcal{L}_{4,\mathbb{C}}$ is a subgroup of $\Theta(\mathrm{M}(n, \mathbb{F}_p))$ by (∗), so is in $\mathcal{L}_{4,W^\circ}$. If $\pi H \leq D$ then the theorem follows from Theorem 2.17(i). If πH is A_4 or S_4 then [12, Theorems 7.2, 8.1] show that $\Theta(G)$ is $\mathrm{M}(4, \mathbb{C})$-conjugate to H. This completes the proof by Corollary 2.19. □

Now we focus on finite subfields of $\mathbb{F}_p$. By Proposition 3.6, the absolutely irreducible subgroups of $\mathrm{GL}(4, q)$ are precisely the nonabelian subgroups that are irreducible over $\mathrm{GF}(q^2)$.

Lemma 4.2. *Suppose $\omega \in \mathbb{F}_p^\times$ has 2-power order and $\omega + \omega^{-1} \in \mathrm{GF}(q)$.*

(i) *If $q \equiv 1 \bmod 4$ then $\omega \in \mathrm{GF}(q)$.*
(ii) *If $q \equiv 3 \bmod 4$ then $\omega \in \mathrm{GF}(q^2)$.*

Proof. (i) Let $j \geq 0$ be the least integer such that $\omega^{2^j} \in \mathrm{GF}(q)$. Suppose $j \geq 1$. By induction, $\omega^{2^{j-1}} + \omega^{-2^{j-1}} \in \mathrm{GF}(q)$. If $\omega^{2^{j-1}} + \omega^{-2^{j-1}} = 0$ then $\omega^{2^{j-1}}$ is a fourth root of unity, hence $\omega^{2^{j-1}} \in \mathrm{GF}(q)$. But this contradicts minimality of j. Otherwise $\omega^{2^{j-1}} = (\omega^{2^j} + 1)(\omega^{2^{j-1}} + \omega^{-2^{j-1}})^{-1} \in \mathrm{GF}(q)$, the same contradiction. Thus $j = 0$.
(ii) This is immediate from (i). □

Lemma 4.3. *Suppose $G \leq \mathrm{M}(4, \mathbb{F}_p)$ is $\mathrm{GF}(q)$-monomial, and set $N = \mathrm{D}(4, \mathbb{F}_p) \cap G$.*

(i) $\mathsf{O}_{\{2,3\}'}(G) = N_{\{2,3\}'} \leq \mathrm{D}(4, q)$.
(ii) $N_3 \leq \mathrm{D}(4, q^3)$. *Also,* $N_3 \leq \mathrm{D}(4, q^2)$ *if $q - 1$ is not divisible by 3, and* $N_3 \leq \mathrm{D}(4, q)$ *if $\pi G \leq D$.*
(iii) $N_2 \leq \mathrm{D}(4, q^4)$. *Also,* $N_2 \leq \mathrm{D}(4, q^2)$ *if $q \equiv 3 \bmod 4$. If $q \equiv 1 \bmod 4$, $g \in N_2$, and $\Theta(g)$ lies in one of X_2, Y_2, U_2, or V_2, then $g \in \mathrm{D}(4, q)$.*
(iv) *Suppose $p \geq 5$ and $q - 1$ is a power of 2. If $G \in \mathcal{L}_{4,\mathbb{F}_p}$ then $\Theta(G) \leq B_2 S_4$.*

Proof. We observe at the outset that an element of $\mathrm{D}(n, \mathbb{F}_p)$ that is $\mathrm{GL}(n, \mathbb{F}_p)$-conjugate to an element of $\mathrm{D}(n, q)$ must be in $\mathrm{D}(n, q)$.

(i) Let $g \in \mathsf{O}_{\{2,3\}'}(G)$. If $m \in \mathrm{GL}(4, \mathbb{F}_p)$ and $g^m \in \mathrm{M}(4, q)$ then $\pi g = \pi(g^m) = 1$. Hence $g \in N$ and $g^m \in \mathrm{D}(4, q)$, implying $g \in \mathrm{D}(4, q)$.

(ii) There is a Sylow 3-subgroup of $\mathrm{M}(4, q)$ with projection group $\langle\, d \,\rangle$, and exponent thrice the exponent of the Sylow 3-subgroup of $\mathrm{GF}(q)^\times$. Thus, each diagonal entry of $g \in N_3$ belongs to an extension of $\mathrm{GF}(q)$ that has an element whose cube generates the Sylow 3-subgroup of $\mathrm{GF}(q)^\times$. If the latter is trivial then 3 divides $q + 1$ and the extension is $\mathrm{GF}(q^2)$; otherwise, it is $\mathrm{GF}(q^3)$. If $\pi G \leq D$ then g and any conjugate of g is diagonal, so $g \in \mathrm{D}(4, q)$.

(iii) We prove only the third assertion in (iii); the others are proved as in (ii). If g is not scalar (that is, $\Theta(g) \notin X_2$) then g is an S_4-conjugate of $(\omega, \omega, \omega^{-1}, \omega^{-1})$ for some 2-element ω of $\mathbb{F}_p$. By Lemma 4.2, $\omega \in \mathrm{GF}(q)$ as required.

(iv) Let $g \in G$. According to $(*)$, $\Theta(g) = txyuv$ for some $t \in S_4$ and p'-elements x, y, u, v of X, Y, U, V respectively. Since $\psi(\det(txyuv)) = \det g \in \mathrm{GF}(q)^\times$ and $\det(tyuv) = \pm 1$, it follows that $x \in X_2$.

Let $t = 1$. If $|yuv|$ is not divisible by 3 then it is a power of 2, because $\mathrm{M}(4, q)$ is a $\{2, 3\}$-group and G is $\mathrm{GF}(q)$-monomial. Say $|yuv| = 2^s$, so $y^{2^s} \in Y \cap UV \leq Y_2$ and thus $y \in Y_2$. Similarly $u \in U_2$ and $v \in V_2$. If $|yuv|$ is divisible by 3 then there exists a diagonal matrix $w = (w_1, w_2, w_3, w_4) \in G$ of order 3. Since $\langle\, d \,\rangle$ is a Sylow 3-subgroup of $\mathrm{M}(4, q)$, w is conjugate to d or d^2. Therefore

$$w_1 w_2 w_3 w_4 = w_1 + w_2 + w_3 + w_4 = 1\,. \qquad (\ddagger)$$

As the Sylow 3-subgroup of $\mathrm{D}(4, q) \cap G$, $\langle\, w \,\rangle$ is normalized by πG, and hence normalized by C or V_4. This means that an involution of V_4 acts trivially on w. Then $(\ddagger)$ forces $2(w_1 + w_1^{-1}) = 1$ or $2(w_1 - w_1^{-1}) = 1$, and consequently w_1 is a primitive cube root of unity. But $w_1 + w_1^{-1} = -1$, whereas the characteristic p is greater than 3. If $2(w_1 - w_1^{-1}) = 1$ then $w_1 \in \mathrm{GF}(q)$, which is likewise absurd.

Now let $t \neq 1$. By $(*)$ and the previous paragraph, $yuv \in B_2 X_3 = X_2 X_3 Y_2 U_2 V_2$. Since $X \cap YUV \leq X_2$, we have $\Theta(g) \in B_2 S_4$ as claimed. □

Lemma 4.3 only frames necessary conditions for a group in $\mathcal{L}_{4,\mathbb{F}_p}$ to be $\mathrm{GF}(q)$-monomial (although in Lemma 4.3(iv), if $q \equiv 1 \bmod 4$, $\pi G \leq D$, and $\mathrm{tr}(G) \subseteq \mathrm{GF}(q)$, then G is $\mathrm{GF}(q)$-monomial by Corollary 2.21). Using this result we cut down the infinite list $\mathcal{L}_{4,\mathbb{F}_p}$ to finitely many potential candidates for a list $\mathcal{L}_{4,q}$ of the absolutely irreducible subgroups of $\mathrm{M}(4, q)$.

We are now ready to assemble $\mathcal{L}_{4,q}$. For $q = p = 5$, such a list is presented in Theorem 4.5 below. (If $q - 1$ is a power of 2 then the diagonal subgroup of $G \leq \mathrm{M}(4, q)$ is a 2-group, and this greatly simplifies things when $\pi G = V_4$. Also, only E.1 of the Appendix is relevant.) In the theorem, we write a diagonal matrix w as the vector $(1, 1, 1, 1)w$ of its nonzero entries. Those entries are determined by setting $\psi(\sqrt{-1})$ to be $2 = \psi(2) \in \mathrm{GF}(5)$. Listed groups are given by generating sets, which need not be minimal. The 2-elements $x_k \in X$, $y_k \in Y$, $u_k \in U$, and $v_k \in V$ (all

denoted with a second subscript "2" in [12]) are as defined in [11, p. 23]:

$$x_k = (\omega_k, \omega_k, \omega_k, \omega_k)\,, \qquad y_k = (\omega_k, \omega_k, \omega_k^{-1}, \omega_k^{-1})\,, \qquad u_k = y_k^{de}\,, \qquad v_k = y_k^{d}\,.$$

Lemma 4.4. *Let* $F(i,j,k,l,\delta,\xi,\alpha)$, $C(i,j,k,\delta,\xi,\alpha)$ *be the* V_4*- and* C*-submodules of* B_2 *defined in* [11, (3.2)–(3.8)] *and* [11, Theorem 4.4]. *Let* $p = 5$. *If* $G \in \mathcal{L}_{4,\mathbb{F}_p}$ *is* GF(5)*-monomial then either the diagonal subgroup* $\mathrm{D}(4,\mathbb{F}_p) \cap G$ *of* G *is scalar, or its image under* Θ *is one of the following*:

$F(1,1,1,1,0,0)$	$F(1,1,1,1,0,0,-1,-1)$	$F(1,1,1,1,0,1)$
$F(1,1,0,0,0,1,1)$	$F(1,1,1,1,0,1,0)$	$F(0,0,1,1,1,0)$
$F(1,1,1,1,1,0)$	$F(1,1,1,1,1,0,1)$	$F(0,0,1,1,1,0,-1)$
$F(0,0,1,1,1,1)$	$F(1,1,1,1,1,1)$	$F(1,1,0,0,1,1,1)$
$F(0,0,0,0,1,1,1)$	$F(1,1,1,1,1,1,1)$	$F(0,0,0,0,1,1,2,1)$
$F(0,0,0,0,1,1,2,-1)$	$F(1,1,0,0,1,1,2,-1)$	$F(1,1,1,1,1,1,2,-1)$
$C(1,1,1,0,1)$	$C(1,1,1,0,1,0)$	$C(1,1,1,0,0,-1)$
$C(1,1,1,0,1,1)$	$C(0,0,1,1,1)$	$C(1,1,1,1,1)$
$C(0,0,1,1,0,1)$	$C(1,1,1,1,1,1)$	$C(0,0,0,1,1,2,1)$
$C(0,0,0,1,1,2,-1)$	$C(1,1,0,1,1,2,-1)$	$C(1,1,1,1,1,2,-1)\,.$

Proof. Set $H = \Theta(G)$. By Lemma 4.3(iv), $H \leq B_2S_4$. Suppose $\pi H \leq D$. Then H is in the list of [11, Theorem 6.1.1], amended as per the errata E.1, so that $M = H \cap \mathrm{D}(4,\mathbb{C})$ is $F(i,j,k,l,\delta,\xi,\alpha)$ or $C(i,j,k,\delta,\xi,\alpha)$ for some values of parameters. If $M = F(i,j,k,l,\delta,\xi,\alpha)$ then $M \cap X_2$, $M \cap Y_2$, $M \cap U_2$, and $M \cap V_2$ have orders 2^{i+1}, 2^{j+1}, 2^{k+1}, and 2^{l+1} respectively. If $M = C(i,j,k,\delta,\xi,\alpha)$ then $M \cap X_2$, $M \cap U_2$, and $M \cap Y_2 = M \cap V_2$ have orders 2^{i+1}, 2^{j+1}, and 2^{k+1} respectively. Thus $i,j,k,l \leq 1$ by Lemma 4.3(iii). Since G is GF(5)-monomial, $\psi(\mathrm{tr}(H)) \subseteq \mathrm{GF}(5)$. The elements $x_2u_2v_2$, $u_2y_2v_2$, $x_2y_2v_2$, $x_2u_2y_2$, x_1u_2, x_1y_2, $x_2u_2^{-1}y_3v_3$, $x_3u_3y_2v_2$, $x_3y_3u_2v_2$, and $x_3u_3y_3v_3x_2u_2$ of B_2 have traces in

$$\{2\omega,\ 2(\omega+\omega^3),\ 2+\omega+\omega^3,\ \omega+\omega^3\}\,,$$

ω a primitive eighth root of unity. Hence M cannot contain any of these elements, because $\mathrm{GF}(5)^\times = \langle\, \psi(\omega^2)\,\rangle$ but $\psi(\omega) \notin \mathrm{GF}(5)$ and $\psi(\omega+\omega^3) \notin \mathrm{GF}(5)$. With reference to [11, Theorem 6.1.1] and errata E.1, and heeding permissible parameter ranges, we may then rule out as possible M all submodules of B_2 except those stated in this lemma. If $\pi H = A_4$ or $\pi H = S_4$ then by the foregoing and [12, Theorems 7.2 and 8.1], either M is scalar or one of the $F(i,j,k,l,\delta,\xi,\alpha)$ not already ruled out. □

Theorem 4.5. *As* μ *ranges over* $\{0,1,2\}$ *and* ε,η *range over* $\{0,1\}$, *the following constitutes a list of* 142 *absolutely irreducible subgroups of* $\mathrm{M}(4,5)$. *An absolutely irreducible subgroup of* $\mathrm{M}(4,5)$ *is* $\mathrm{GL}(4,5)$*-conjugate to one and only one group in*

this list. (*The notation* $[o, z]$ *beside each group gives the order* o *of the group and the order* z *of its centre.*)

1. $[64, 4]$ $\langle a(2,1,1,3)^{\varepsilon},\ b(2,1,1,3)^{\varepsilon}(1,2,1,3)^{\eta},\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\rangle$
2. $[64, 4]$ $\langle a(2,1,2,1),\ b(2,1,1,3)^{\varepsilon},\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\rangle$
3. $[64, 4]$ $\langle a(2,2,1,1),\ b(2,1,1,3)^{\varepsilon}(1,2,1,3)^{\eta},\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\rangle$
4. $[128, 4]$ $\langle a(2,1,2,1)^{\varepsilon},\ b(2,1,1,3)^{\eta},\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3),\ (2,2,2,3)\rangle$
5. $[128, 4]$ $\langle a(2,1,1,3)^{\varepsilon},\ b(2,2,1,1)^{\eta},\ (2,2,2,2),\ (2,3,2,3),\ (1,1,2,3)\rangle$
6. $[128, 4]$ $\langle a(2,1,2,1)(2,1,1,3)^{\varepsilon},\ b,\ (2,2,2,2),\ (2,3,2,3),\ (1,1,2,3)\rangle$
7. $[64, 4]$ $\langle c(2,1,1,1),\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\rangle$
8. $[64, 4]$ $\langle a(2,1,1,3),\ b,\ (2,2,2,2),\ (2,2,3,3),\ (4,1,2,3)\rangle$
9. $[64, 4]$ $\langle c(1,1,2,1),\ (2,2,2,2),\ (2,3,2,3),\ (4,2,1,3)\rangle$
10. $[256, 4]$ $\langle a(2,1,2,1)^{\varepsilon},\ b,\ (2,2,2,2),\ (2,2,3,3),\ (1,1,2,3),\ (2,1,1,3)\rangle$
11. $[32, 2]$ $\langle a(2,2,2,2)^{\varepsilon},\ b(2,1,1,3)(1,2,1,3)^{\eta},\ (2,3,2,3),\ (3,2,2,3)\rangle$
12. $[32, 2]$ $\langle a(2,2,2,2)^{\varepsilon},\ b,\ (2,3,2,3),\ (3,2,2,3)\rangle$
13. $[128, 4]$ $\langle a(2,1,2,1)^{\varepsilon},\ b(2,1,1,3)(1,2,1,3)^{\eta},\ (2,2,1,1),\ (2,2,3,3),\ (2,3,2,3)\rangle$
14. $[128, 4]$ $\langle a(2,1,2,1)^{\varepsilon},\ b,\ (2,2,1,1),\ (2,2,3,3),\ (2,3,2,3)\rangle$
15. $[256, 4]$ $\langle a(2,1,1,1)^{\varepsilon},\ b(2,1,1,1)^{\varepsilon}(1,2,1,3)^{\eta},\ (2,2,2,2),\ (2,2,1,1),\ (2,1,2,1)\rangle$
16. $[64, 2]$ $\langle a,\ b(1,2,1,3)^{\varepsilon},\ (2,3,2,3),\ (2,2,4,1)\rangle$
17. $[64, 2]$ $\langle a(2,2,2,2)^{\varepsilon},\ b,\ (2,3,2,3),\ (1,1,2,3)\rangle$
18. $[256, 4]$ $\langle a(2,1,2,1)^{\varepsilon},\ b,\ (2,2,3,3),\ (2,3,2,3),\ (2,2,1,1),\ (1,1,2,3)\rangle$
19. $[128, 4]$ $\langle c(2,1,1,1),\ (2,1,2,1),\ (2,2,3,3),\ (2,3,2,3)\rangle$
20. $[128, 4]$ $\langle a(1,2,2,1),\ c(3,2,2,4),\ (2,1,2,1),\ (2,3,2,3)\rangle$
21. $[32, 2]$ $\langle a,\ b(2,2,2,3),\ (4,4,1,1),\ (1,1,4,4)\rangle$
22. $[512, 4]$ $\langle a,\ b(1,1,2,1)^{\varepsilon},\ (2,2,3,3),\ (2,2,1,1),\ (1,1,2,3),\ (2,1,2,1)\rangle$
23. $[64, 2]$ $\langle a,\ b,\ (4,4,1,1),\ (4,1,4,1),\ (2,2,2,3)\rangle$
24. $[64, 2]$ $\langle a,\ b,\ (4,1,1,1)\rangle \cong C_2 \text{ wr } V_4$
25. $[256, 4]$ $\langle a,\ c(2,1,1,1),\ (2,2,2,2),\ (2,2,3,3),\ (2,1,2,1)\rangle$
26. $[1024, 4]$ $\langle a,\ b,\ (2,1,1,1)\rangle = \mathrm{D}(4,5) \rtimes V_4 \cong C_4 \text{ wr } V_4$
27. $[128, 4]$ $\langle c(2,1,1,1)^{\mu},\ (2,2,2,2),\ (2,2,3,3),\ (1,2,1,3)\rangle$
28. $[256, 4]$ $\langle c(2,1,1,1)^{\mu},\ (2,2,2,2),\ (1,2,1,3),\ (2,1,1,3)\rangle$
29. $[128, 4]$ $\langle c(2,1,1,1)^{\varepsilon},\ (2,2,2,2),\ (2,3,2,3),\ (2,2,3,3),\ (2,2,2,3)\rangle$
30. $[256, 4]$ $\langle c(2,1,1,1)^{\varepsilon},\ (2,2,2,2),\ (1,2,1,3),\ (2,2,1,1)\rangle$
31. $[64, 2]$ $\langle c(4,1,1,1)^{\varepsilon},\ (2,2,3,3),\ (1,2,1,3)\rangle$
32. $[256, 4]$ $\langle c(2,1,1,1)^{\varepsilon},\ (2,2,2,2),\ (2,2,3,3),\ (2,1,2,1),\ (1,2,1,3)\rangle$
33. $[64, 2]$ $\langle c(4,1,1,1)^{\varepsilon},\ (2,2,3,3),\ (2,4,2,1)\rangle$
34. $[512, 4]$ $\langle c(2,1,1,1)^{\varepsilon},\ (2,1,2,1),\ (2,3,2,3),\ (1,2,1,3),\ (2,2,1,1)\rangle$
35. $[64, 2]$ $\langle c,\ (4,1,4,1),\ (4,1,1,4),\ (2,2,2,3)\rangle$
36. $[64, 2]$ $\langle c,\ (4,1,1,1)\rangle \cong C_2 \text{ wr } C$
37. $[256, 4]$ $\langle a(1,2,1,3),\ c(1,1,2,1),\ (2,2,2,2),\ (2,1,2,1)\rangle$
38. $[1024, 4]$ $\langle c,\ (2,1,1,1)\rangle = \mathrm{D}(4,5) \rtimes C \cong C_4 \text{ wr } C$
39. $[256, 4]$ $\langle a(1,2,1,3)^{\varepsilon},\ c,\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3),\ (2,2,2,3)\rangle$
40. $[256, 4]$ $\langle a(2,2,1,1)^{\varepsilon}(2,1,1,2)^{1-\varepsilon},\ c(2,1,1,1),\ (2,2,3,3),\ (2,3,2,3),\ (2,2,2,3)\rangle$

41. $[256,4]$ $\langle\, a(2,1,2,1)^{\varepsilon},\ c(2,1,2,1)^{1-\varepsilon},\ (2,2,2,2),\ (2,2,3,3),\ (1,2,1,3)\,\rangle$
42. $[256,4]$ $\langle\, a(2,2,1,1)^{\varepsilon}(2,1,1,3)^{1-\varepsilon},\ c(2,1,2,1)^{\eta},\ (2,2,2,2),\ (2,2,3,3),\ (1,2,1,3)\,\rangle$
43. $[512,4]$ $\langle\, a(2,1,2,1)^{\varepsilon},\ c,\ (2,2,2,2),\ (1,2,1,3),\ (2,2,1,1)\,\rangle$
44. $[512,4]$ $\langle\, a(1,2,1,1)^{\varepsilon}(1,1,1,3)^{1-\varepsilon},\ c(2,1,1,1),\ (1,2,1,3),\ (2,2,1,1)\,\rangle$
45. $[512,4]$ $\langle\, a(2,1,2,1)^{\varepsilon},\ c(2,1,2,1)^{\eta},\ (2,2,2,2),\ (1,2,1,3),\ (2,1,1,3)\,\rangle$
46. $[128,2]$ $\langle\, a(2,1,1,3)^{\varepsilon},\ c(2,1,2,1)^{\varepsilon\eta},\ (2,2,3,3),\ (2,4,2,1)\,\rangle$
47. $[128,2]$ $\langle\, a(2,2,2,2)^{\varepsilon},\ c(2,1,2,1)^{\eta},\ (2,2,3,3),\ (1,2,1,3)\,\rangle$
48. $[512,4]$ $\langle\, a(2,2,1,1)^{\varepsilon},\ c(2,1,1,1)^{\eta},\ (2,2,2,2),\ (2,2,3,3),\ (2,1,2,1),\ (1,2,1,3)\,\rangle$
49. $[1024,4]$ $\langle\, a(1,2,1,1),\ c(2,1,1,1)^{\varepsilon},\ (2,1,2,1),\ (2,3,2,3),\ (1,2,1,3),\ (2,2,1,1)\,\rangle$
50. $[1024,4]$ $\langle\, a(1,1,2,3)^{\varepsilon},\ c(1,2,1,1)^{\varepsilon},\ (2,1,2,1),\ (2,3,2,3),\ (1,2,1,3),\ (2,2,1,1)\,\rangle$
51. $[2048,4]$ $\langle\, a,\ c,\ (2,1,1,1)\,\rangle = \mathrm{D}(4,5) \rtimes D \cong C_4 \text{ wr } D$
52. $[192,4]$ $\langle\, a(2,1,1,3)^{\varepsilon},\ b(1,1,2,3)^{\varepsilon},\ d,\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\,\rangle$
53. $[384,4]$ $\langle\, a(1,2,2,1)^{\varepsilon},\ b(1,1,2,3)^{\varepsilon},\ d,\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3),\ (2,2,2,3)\,\rangle$
54. $[768,4]$ $\langle\, a,\ b,\ d,\ (2,2,2,2),\ (1,1,2,3),\ (2,1,1,3)\,\rangle$
55. $[96,2]$ $\langle\, a,\ b,\ d,\ (4,4,1,1),\ (1,1,4,4),\ (4,1,4,1)\,\rangle$
56. $[1536,4]$ $\langle\, a,\ b,\ d,\ (2,2,1,1),\ (2,2,3,3),\ (1,1,2,3),\ (2,1,2,1)\,\rangle$
57. $[192,2]$ $\langle\, a,\ b,\ d,\ (4,4,1,1),\ (4,1,4,1),\ (2,2,2,3)\,\rangle$
58. $[192,2]$ $\langle\, a,\ b,\ d,\ (4,1,1,1)\,\rangle \cong C_2 \text{ wr } A_4$
59. $[3072,4]$ $\langle\, a,\ b,\ d,\ (2,1,1,1)\,\rangle = \mathrm{D}(4,5) \rtimes A_4 \cong C_4 \text{ wr } A_4$
60. $[48,2]$ $\langle\, a(2,2,2,2),\ b(2,3,2,3),\ d(2,3,1,1),\ e(2,2,2,2)^{\varepsilon}(4,1,2,3)\,\rangle$
61. $[96,4]$ $\langle\, a,\ b(2,3,2,3),\ d(2,3,1,1),\ e(4,1,2,3),\ (2,2,2,2)\,\rangle$
62. $[384,4]$ $\langle\, a,\ b,\ d,\ e(2,2,2,3)^{\varepsilon},\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3)\,\rangle$
63. $[768,4]$ $\langle\, a,\ b,\ d,\ e,\ (2,2,2,2),\ (2,2,3,3),\ (2,3,2,3),\ (2,2,2,3)\,\rangle$
64. $[768,4]$ $\langle\, a(2,1,2,1),\ b(2,1,1,3),\ d(1,1,2,3),\ e(1,1,3,1),\ (2,2,2,3)\,\rangle$
65. $[1536,4]$ $\langle\, a,\ b,\ d,\ e(2,2,1,1)^{\varepsilon},\ (2,2,2,2),\ (1,1,2,3),\ (2,1,1,3)\,\rangle$
66. $[192,2]$ $\langle\, a,\ b,\ d,\ e(2,2,2,3)^{\varepsilon}(2,2,2,2)^{\eta},\ (4,4,1,1),\ (1,1,4,4),\ (4,1,4,1)\,\rangle$
67. $[3072,4]$ $\langle\, a,\ b,\ d,\ e(1,1,1,3)^{\varepsilon},\ (2,2,1,1),\ (2,2,3,3),\ (1,1,2,3),\ (2,1,2,1)\,\rangle$
68. $[384,2]$ $\langle\, a,\ b,\ d,\ e(2,2,2,2)^{\varepsilon},\ (4,4,1,1),\ (4,1,4,1),\ (2,2,2,3)\,\rangle$
69. $[384,2]$ $\langle\, a,\ b,\ d,\ e,\ (4,1,1,1)\,\rangle \cong C_2 \text{ wr } S_4$
70. $[384,2]$ $\langle\, a,\ b,\ d,\ e(2,2,2,2),\ (4,1,1,1)\,\rangle$
71. $[6144,4]$ $\langle\, a,\ b,\ d,\ e,\ (2,1,1,1)\,\rangle = \mathrm{M}(4,5) \cong C_4 \text{ wr } S_4\,.$

Proof. Let $\mathcal{L}_{4,\mathbb{F}_p}$ be defined for $p = 5$. As before, $\psi(\sqrt{-1}) = 2 \in \mathrm{GF}(5)$. This proof makes heavy use of the S_4-conjugation action on YUV, exhibited in [12, preamble of Sec. 2]. Suppose $G \in \mathcal{L}_{4,\mathbb{F}_p}$ is GF(5)-monomial and set $H = \Theta(G)$. Lemma 4.4 lists the diagonal subgroup M of H.

Let $M = F(1,1,1,1,0,0)$. By [11, Theorem 6.1.1] and errata E.1, H is one of the groups

$$\langle\, ay_2^{\varepsilon},\ bu_2^{\varepsilon}v_2^{\eta},\ M\,\rangle\,, \qquad \langle\, ax_2,\ bu_2^{\varepsilon},\ M\,\rangle\,, \qquad \langle\, ax_2y_2,\ bu_2^{\varepsilon}v_2^{\eta},\ M\,\rangle\,.$$

We have

$$\langle\, ay_2^{\varepsilon},\ bu_2^{\varepsilon}v_2^{\eta},\ M\,\rangle \sim_{u_3^{\varepsilon}y_3^{\varepsilon+\eta}} \langle\, a(y_2u_2)^{\varepsilon},\ b(u_2y_2)^{\varepsilon}(v_2y_2)^{\eta},\ M\,\rangle$$

$$\langle\, ax_2,\, bu_2^{\varepsilon},\, M\,\rangle \sim_{y_3^{\varepsilon}} \langle\, ax_2u_2,\, b(u_2y_2)^{\varepsilon},\, M\,\rangle$$

$$\langle\, ax_2y_2,\, bu_2^{\varepsilon}v_2^{\eta},\, M\,\rangle \sim_{y_3^{\varepsilon+\eta}} \langle\, ax_2y_2,\, b(u_2y_2)^{\varepsilon}(v_2y_2)^{\eta},\, M\,\rangle,$$

where, for K, $\bar{K} \leq \mathrm{GL}(4,\mathbb{F}_p)$ and $m \in \mathrm{GL}(4,\mathbb{F}_p)$, $K \sim_m \bar{K}$ signifies that $K^m = \bar{K}$. The images of u_2y_2, v_2y_2, x_2y_2, x_2u_2, x_1, y_1, and u_1 under Ψ are, in the same order, $(2,1,1,3)$, $(1,2,1,3)$, $(2,2,1,1)$, $(2,1,2,1)$, $(2,2,2,2)$, $(2,2,3,3)$, and $(2,3,2,3)$. By Corollary 2.19, G is therefore $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to a group at lines 1–3 in the list $\mathcal{L}_{4,5}$ of this theorem. Group orders are calculated from the formula in [11, p. 28]. If $M = F(i,j,k,l,\delta,\xi,\alpha)$ or $M = C(i,j,k,\delta,\xi,\alpha)$ then $|\mathsf{Z}(G)| = 2^{i+1}$.

The bulk of $\mathcal{L}_{4,5}$ is compiled as above. In particular this is true for the groups at lines 4–6, which have diagonal subgroup $\Psi(M)$, $M = F(1,1,1,1,0,0,-1,-1)$ or $M = F(1,1,1,1,0,1)$.

If $M = F(1,1,0,0,0,1,1)$ then G has diagonal subgroup

$$\Psi(M) = \langle\, (2,2,2,2), (2,2,3,3), (2\omega, 3\omega, 2\omega, 3\omega)\,\rangle$$

where $\omega \in \mathrm{GF}(25)$ is a square root of 2. Thus G is not $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to a subgroup of $\mathrm{M}(4,5)$. However $\mathrm{tr}(g) = 0$ for all $g \in G \backslash \langle\, (2,2,2,2),\, (2,2,3,3)\,\rangle$, so $\mathrm{tr}(G) \subseteq \mathrm{GF}(5)$ and G is $\mathrm{GF}(5)$-monomial by Corollary 2.21. We could adopt the MAGMA procedure at the end of Sec. 2 to compute a conjugate of G in $\mathrm{M}(4,5)$. Instead, as it is no extra effort, we do the rewriting by hand with the aid of Lemma 2.22. Let f be the Kronecker product $I_2 \otimes h = (h,h)$, where

$$h = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

The conjugation action of f on various monomial matrices is given by [11, (3.22)–(3.24)]; note f acts trivially on elements of Y. Also $(u_2v_2)^f = aex_2^{-1}y_2$ and $e^f = x_2y_2u_2^{-1}v_2$. Hence if $H = \langle\, a, bx_3u_2v_2, M\,\rangle$ then

$$\begin{aligned} H &\sim_f \langle\, bex_3y_2,\, x_1,\, y_1,\, u_1\,\rangle \\ &\sim_{de} \langle\, cx_3u_2,\, x_1,\, y_1,\, u_1\,\rangle \\ &\sim_{y_3} \langle\, cx_3y_3v_3^{-1}u_2,\, x_1,\, y_1,\, u_1\,\rangle \\ &\sim_{u_4^{-1}} \langle\, cx_3y_3u_3v_3^{-1},\, x_1,\, y_1,\, u_1\,\rangle. \end{aligned}$$

Now $\Psi(x_3y_3u_3v_3^{-1}) = (2,1,1,1)$ and $\det(fdey_3u_4^{-1}) = -\det f = 1$, so by Lemma 2.22, G is $\mathrm{GL}(4,\mathbb{F}_p)$-conjugate to

$$\Psi(\langle\, cx_3y_3u_3v_3^{-1},\, x_1,\, y_1,\, u_1\,\rangle) = \langle\, c(2,1,1,1),\, (2,2,2,2),\, (2,2,3,3),\, (2,3,2,3)\,\rangle,$$

the group at line 7. Similarly, if $H = \langle\, ay_2,\, b,\, M\,\rangle$ then

$$H \sim_{fu_2fu_3} \langle\, ay_2u_2,\, b,\, x_2y_2u_1,\, x_1,\, y_1\,\rangle$$

and it follows that G is conjugate to

$$\langle\, a(2,1,1,3),\, b,\, (2,2,2,2),\, (2,2,3,3),\, (4,1,2,3)\,\rangle,$$

which is at line 8. For the third group $H \in \mathcal{L}_{4,\mathbb{C}}$ with $M = F(1,1,0,0,0,1,1)$,

$$\begin{aligned} H = \langle\, ay_2,\, bx_3u_2v_2,\, M \,\rangle &\sim_f \quad \langle\, bex_3y_2,\, x_1,\, y_1,\, y_2u_1 \,\rangle \\ &\sim_{y_4^{-3}u_2^{-1}} \langle\, bex_3y_3u_2v_2,\, x_1,\, y_1,\, y_2u_1 \,\rangle \\ &\sim_f \quad \langle\, ay_2,\, bex_3y_3^{-1}u_2v_2^{-1},\, x_1,\, y_1 \,\rangle \\ &\sim_{y_3u_3} \langle\, ay_2u_2,\, bex_3y_3u_3^{-1}v_3,\, x_1, y_1 \,\rangle \\ &\sim_{de} \quad \langle\, by_2u_2,\, cx_3y_3^{-1}u_3v_3,\, x_1,\, u_1 \,\rangle \\ &= \quad \langle\, cx_3y_3^{-1}u_3v_3,\, x_1,\, u_1,\, x_2u_2y_1 \,\rangle. \end{aligned}$$

Therefore we list $\langle\, c(1,1,2,1),\, (2,2,2,2),\, (2,3,2,3),\, (4,2,1,3) \,\rangle$, at line 9.

Groups at lines 10–18 correspond to G with M one of

$$\begin{aligned} &F(1,1,1,1,0,1,0), \quad F(0,0,1,1,1,0), F(1,1,1,1,1,0),\ F(1,1,1,1,1,0,1), \\ &F(0,0,1,1,1,0,-1), F(0,0,1,1,1,1), F(1,1,1,1,1,1)\,. \end{aligned}$$

For all such G, $\Psi(M) \leq \mathrm{D}(4,5)$ and G is $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to a subgroup of $\mathrm{M}(4,5)$.

At lines 19 and 20, $M = F(1,1,0,0,1,1,1) = \langle\, x_2y_2,\, y_1,\, x_2u_1 \,\rangle$. Since

$$\langle\, a,\, bx_3u_2v_2,\, M \,\rangle \sim_{fu_3y_4^{-1}de} \langle\, cx_3y_3u_3v_3^{-1},\, x_2u_2,\, u_1,\, y_1 \,\rangle$$

and

$$\begin{aligned} \langle\, ax_3y_3,\, bv_2,\, M \,\rangle &\sim_{u_2u_3v_3fv_3} \langle\, bex_3^{-1}y_3u_3v_3v_1,\, bx_2v_2,\, x_2y_2,\, y_1 \,\rangle \\ &\sim_{de} \quad \langle\, ax_2v_2,\, cx_3^{-1}u_3y_3v_3v_1,\, x_2u_2,\, u_1 \,\rangle, \end{aligned}$$

G is conjugate to

$$\langle\, c(2,1,1,1),\, (2,1,2,1),\, (2,2,3,3),\, (2,3,2,3) \,\rangle$$

in the first case and

$$\langle\, a(1,2,2,1),\, c(3,2,2,4),\, (2,1,2,1),\, (2,3,2,3) \,\rangle$$

in the second.

The groups at lines 21–24 and 26 are $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to elements of $\mathcal{L}_{4,\mathbb{F}_p}$. (At line 24, $G \cong C_2$ wr V_4 because H splits over $M = F(0,0,0,0,1,1,2,-1)$, and $(1,1,1,-1) = x_2^{-1}y_2u_2v_2 \in M$.) For line 25 we invoke errata E.1 and

$$\langle\, a,\, b,\, F(1,1,0,0,1,1,2,-1) \,\rangle \sim_{fu_3de} \langle\, a, cx_3y_3u_3v_3^{-1},\, x_1,\, y_1,\, x_2u_2 \,\rangle\,.$$

From line 27 to line 38, M is one of the $C(i,j,k,\delta,\xi,\alpha)$, $\pi G = C$, and the Appendix is irrelevant. It may be shown that $G^m \leq \mathrm{M}(4,5)$ for some power m of $\Psi(u_4y_3)$, except when $M = C(1,1,0,1,1,2,-1)$: then $H = \langle\, c,\, M \,\rangle$ and

$$\begin{aligned} H &\sim_{f'} \langle\, ax_2y_2^{-1}u_2v_2,\, x_2u_2,\, bu_2,\, x_3u_3^{-1}ac^{-1}x_2^{-1}u_2 \,\rangle \\ &= \quad \langle\, ay_2v_2,\, cx_3u_3y_2^{-1}v_2,\, ,x_2u_2,\, x_1 \,\rangle \\ &\sim_{y_3} \langle\, ay_2v_2,\, cx_3y_3^{-1}u_3v_3,\, x_2u_2,\, x_1 \,\rangle \end{aligned}$$

where $f' = f^{de}$, using $c^{f'} = ax_2y_2^{-1}u_2v_2$. Thus G is conjugate to

$$\langle\, a(1,2,1,3),\, c(1,1,2,1),\, (2,2,2,2),\, (2,1,2,1)\,\rangle\,.$$

Fortunately $\Psi(M) \leq \mathrm{D}(4,5)$ for all remaining groups H. If $w = (w_1, w_2, w_3, w_4)$, note that $\mathrm{tr}(acw) = w_2+w_4$, $\mathrm{tr}(dw) = w_4$, $\mathrm{tr}(ew) = w_3+w_4$, and $\mathrm{tr}(aew) = w_1+w_2$. The rest of $\mathcal{L}_{4,5}$ is then found in the familiar way, by taking $\mathrm{M}(4,\mathbb{F}_p)$-conjugates of groups in $\mathcal{L}_{4,\mathbb{F}_p}$ not excluded by trace evaluations and Lemma 4.4. (Remember $H \leq B_2S_4$. We include $\langle\, ax_2u_2,\, c,\, C(1,1,1,0,1)\,\rangle$, not in [11, Theorem 6.1.1], by the Appendix. No other errata are relevant.) There is a single group in $\mathcal{L}_{4,\mathbb{F}_p}$ that is not GF(5)-monomial yet is conjugate to a subgroup of $\mathrm{GL}(4,5)$, namely

$$G = \langle\, a,\, b(2,3,2,3),\, d(2,3,1,1),\, g\,\rangle\,,$$

where $g = e(2\omega, 3\omega, \omega, 4\omega)$. For suppose $G^m \leq \mathrm{M}(4,5)$, $m \in \mathrm{GL}(4,\mathbb{F}_p)$. Then $\pi(G^m) = S_4$ by [12, Proposition 9.1] and Proposition 2.7. Since $V_4 = \mathrm{soc}(S_4)$ is characteristic in S_4 and m induces an automorphism of S_4, $\pi(g^m) = t$ for some involution $t \in S_4\backslash V_4$. But whereas $g^2 = (2,2,2,2)$, there is no $\bar{g} \in \mathrm{M}(4,5)$ such that $\pi\bar{g} = t$ and $\bar{g}^2 = (2,2,2,2)$. □

Remark 4.6. If $H = \langle\, a,\, c,\, C(0,0,1,1,1)\,\rangle = \langle\, a,\, c,\, y_1,\, y_2v_2\,\rangle$ then

$$H \sim_{f'y_2} \langle\, a,\, c,\, x_2y_2^{-1}u_2v_2\,\rangle \cong C_2 \text{ wr } D$$

and $\Psi(H) = \langle\, a,\, c,\, (2,2,3,3),\, (1,2,1,3)\,\rangle \in \mathcal{L}_{4,5}$ (line 47). This completes identification in $\mathcal{L}_{4,5}$ of all wreath products C_{2^r} wr T, $1 \leq r \leq 2$, and T a transitive subgroup of S_4.

Remark 4.7. $\mathrm{M}(n,\mathbb{E})$ is almost always a maximal subgroup of $\mathrm{GL}(n,\mathbb{E})$ for a field (or even division ring) $\mathbb{E}$; see [22, Theorem 1]. Thus $\mathrm{GL}(4,\mathbb{F}_p) = \langle\, f,\, \mathrm{M}(4,\mathbb{F}_p)\,\rangle$. Since f^2 is monomial, it is not surprising that only f and monomial matrices can be used to rewrite the GF(q)-monomial elements of $\mathcal{L}_{4,\mathbb{F}_p}$ in $\mathrm{M}(4,q)$.

We should be aware of an intrinsic ambiguity in the construction of $\mathcal{L}_{n,q}$ from $\mathcal{L}_{n,\mathbb{C}}$. To get explicit matrix generators for groups in $\mathcal{L}_{4,5}$, one must decide the value of $\psi(\sqrt{-1})$ in GF(5). We fixed this as 2. But equally we could have fixed $\psi(\sqrt{-1})$ as 3, which amounts to replacing the original choice of maximal ideal of R defining $\mathbb{F}_p$ by its complex conjugate. Although we do not pursue the matter here, it is possible to show that this is an instance of a general phenomenon: if $t \in \mathbb{Z}$ has multiplicative order $p-1$ mod p then there is a maximal ideal I of R containing p such that $\omega_{p-1} - t \in I$, where ω_{p-1} is the primitive $(p-1)$th root of unity $\exp(2\pi\sqrt{-1}/p-1)$. Thus for our purposes $\psi(\omega_{p-1})$ may be chosen as any generator of $\mathrm{GF}(p)^\times$. However, the conjugacy class represented by an element of $\mathcal{L}_{n,q}$ may vary with I.

To end the section we give a proof of Proposition 3.9 by looking up groups in $\mathcal{L}_{4,\mathbb{C}}$. Confirmation of known results in this fashion is welcome, as evidence that a list is correct.

Proposition 4.8. *Let p be any odd prime. If G is an irreducible subgroup of* $\mathrm{M}(4,q)$ *such that $\pi G = S_4$, then G is absolutely irreducible.*

Proof. Set $H = \Theta(G)$ and suppose G is not absolutely irreducible. As in the proof of Proposition 3.9, we assume the diagonal subgroup of G is a scalar 2-group. Let $M \leq B$ be a finite normal nonscalar $\{2,3\}'$-subgroup of $\mathrm{M}(4,\mathbb{C})$. Then HM is an irreducible subgroup of $\mathrm{M}(4,\mathbb{C})$ by [12, Theorem 4.2], and $H^m M$ is in the list $\mathcal{S}$ of [12, Theorem 8.1] for some $m \in \mathrm{M}(4,\mathbb{C})$. By Schur–Zassenhaus, the possible H^m are then immediately visible. Actually, those groups that are irreducible cannot be conjugate to H, by Corollary 3.4. The other possibilities are $S_4 N$ and $\langle\, a, d, ex \,\rangle N$, where $N \leq X_2$ and $x \in X_2$, $N = \langle\, x^2 \,\rangle$. If H were $\mathrm{M}(4,\mathbb{C})$-conjugate to the first group then by Proposition 2.18, G would be $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to a split extension of S_4 by scalars in $\mathrm{M}(4,q)$, and thus would be reducible over $\mathrm{GF}(q)$. Suppose G is $\mathrm{M}(4,\mathbb{F}_p)$-conjugate to $\langle\, a, d, e\hat{x} \,\rangle$, $\hat{x} = \Psi(x)$. Since $\mathrm{tr}(e\hat{x}) \in \mathrm{GF}(q)$, so $\hat{x} \in \mathrm{D}(4,q)$. But then again G is reducible in $\mathrm{M}(4,q)$, as a subgroup of $S_4\langle\, \hat{x} \,\rangle$. □

5. Finite Absolutely Irreducible Linear Groups of Degree Two

In this section p is odd. An irreducible subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$ is primitive or monomial. We consider monomial groups first.

The finite nonabelian 2-subgroups of $\mathrm{M}(2,\mathbb{F}_p)$ are known by Conlon's classification in [5] of the finite irreducible 2-subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$. We need abelian groups as well, and these are obtained by Conlon's techniques. Then we proceed as in [12], taking semidirect products with groups of odd order diagonal matrices.

Inductively select primitive 2^{i+1}th roots of unity $\omega_i \in \mathbb{F}_p$ such that $\omega_{i+1}^2 = \omega_i$, $i \geq 0$. Define $z_i, w_i \in \mathrm{D}(2,\mathbb{F}_p)$ by

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

A Sylow 2-subgroup of $\mathrm{M}(2,\mathbb{F}_p)$, and of $\mathrm{GL}(2,\mathbb{F}_p)$, is

$$\varinjlim_{i,j\geq 0} \langle\, z_i,\, w_j \,\rangle \rtimes S_2 \cong C_{2^\infty} \text{ wr } S_2\,.$$

For integers $i, j \geq 0$ and $1 \leq k \leq 3$, define subgroups $H(i,j,k)$ of $\mathrm{M}(2,\mathbb{F}_p)$ by

$$H(i,j,1) = \langle\, a_1,\, z_i,\, w_j \,\rangle$$
$$H(i,j,2) = \langle\, a_1 z_{i+1},\, w_j \,\rangle$$
$$H(i,j,3) = \langle\, a_1,\, z_{i+1} w_{j+1},\, w_j \,\rangle$$

where a_1 is the permutation matrix generating S_2. Note that $H(i,j,k)$ is abelian if and only if $k = 1$ or 2 and $j = 0$. (Conlon labels only nonabelian groups. In his notation, $H(i-1,j-1,1)$ is $P_{j\,i\,0}$, $H(i-1,j-1,2)$ is $P_{j\,i\,2}$, and $H(i-1,j-2,3)$ is $P_{j\,i\,1}$, $i \geq 1$, $j \geq 2$.) We have $|H(i,j,1)| = |H(i,j,2)| = 2^{i+j+2}$, $|H(i,j,3)| = 2^{i+j+3}$, and $\mathsf{Z}(H(i,j,k)) = \langle\, z_i \,\rangle$, of order 2^{i+1}. Then $H(i,j,k) = H(i',j',k')$ implies $i = i'$, $j = j'$, and $k = k'$.

Theorem 5.1. *A finite irreducible subgroup H of $\mathrm{M}(2,\mathbb{F}_p)$ is $\mathrm{GL}(2,\mathbb{F}_p)$-conjugate to $H_{2'} \rtimes H_2$, where $H_{2'} := \mathsf{O}_{2'}(H)$ is a finite odd order $\mathbb{Z}S_2$-submodule of $\mathrm{D}(2,\mathbb{F}_p)$, and*

(i) *if $H_{2'}$ is scalar then H_2 is one of the $H(i,j,k)$, $i \geq 0$, $j \geq 1$, $1 \leq k \leq 3$;*
(ii) *if $H_{2'}$ is nonscalar then H_2 is $\langle\, a_1 \,\rangle$ or one of the $H(i,j,k)$, $i,j \geq 0$, $1 \leq k \leq 3$.*

Proof. $H_{2'} \leq \mathrm{D}(2,\mathbb{F}_p)$, $H_{2'} \trianglelefteq \mathrm{M}(2,\mathbb{F}_p)$, and H splits over $H_{2'}$ by a Sylow 2-subgroup H_2. We assume $H_2 \leq \lim_{\rightarrow}\langle\, z_i,\, w_j \,\rangle S_2$, replacing H by an $\mathrm{M}(2,\mathbb{F}_p)$-conjugate if necessary.

By [5, Proposition 1.8] or [11, pp. 9–10], if the diagonal subgroup N of H_2 is nontrivial then it is $\langle\, z_i,\, w_j \,\rangle$ or $\langle\, z_{i+1}w_{j+1},\, w_j \,\rangle$, for some $i,j \geq 0$. An element of $H_2\backslash N$ has the form $a_1 z w$, where z is scalar and $w \in \mathrm{D}(2,\mathbb{F}_p) \cap \mathrm{SL}(2,\mathbb{F}_p)$. Choose $\bar{w} \in \mathrm{SL}(2,\mathbb{F}_p)$ such that $\bar{w}^2 = w^{-1}$, and replace H, H_2 by $H^{\bar{w}}$, $H_2^{\bar{w}}$ respectively. Then $a_1 z \in H_2$ and $z^2 \in N$. Hence $z \in \langle\, z_{i+1} \,\rangle$. If $z_{i+1}w_{j+1} \in N$ (maybe $N = 1$, i and j taking the exceptional value -1) then $a_1 \in H_2$ or $a_1 \in H_2^{w_{j+2}}$. For the other N, $z \in N$ or $z \in z_{i+1}N$. We have proved that H_2 is $\mathrm{M}(2,\mathbb{F}_p)$-conjugate to $\langle\, a_1 \,\rangle$ or some $H(i,j,k)$.

If $H_{2'}$ is nonscalar then H is irreducible by Maschke's Theorem. Let $H = H(i,j,k)H_{2'}$ and suppose $H_{2'}$ is scalar. Then $H(i,j,k)$ must be nonabelian, so $j \geq 1$ if $k = 1$ or $k = 2$. Let h be the 2×2 Hadamard matrix in the proof of Theorem 4.5. Since $a_1^h = z_1 w_1^{-1}$ and $w_1^h = a_1 z_1^{-1}$, we get $H(i,0,3)^h = H(i,1,2)$ for $i \geq 1$ and $H(0,0,3)^{w_2 h} = H(0,1,1)$. Thus j can also be restricted to $j \geq 1$ if $k = 3$. □

Remark 5.2. For each odd prime $r \neq p$ and $i \geq -1$, define the scalar $z_{i,r}$ and the diagonal matrix $w_{i,r} \in \mathrm{SL}(2,\mathbb{F}_p)$ as z_i, w_i were defined for the prime 2, so that $|z_{i,r}| = |w_{i,r}| = r^{i+1}$. Then a finite $\mathbb{Z}S_2$-submodule of $\mathrm{D}(2,\mathbb{F}_p)$ of odd order is a direct product $\prod_r \langle\, z_{i_r,r},\, w_{j_r,r} \,\rangle$.

The next result extends [5, Proposition 4.2] in degree 2.

Theorem 5.3. *Let $H = H_{2'}H_2$ and $K = K_{2'}K_2$ be finite irreducible subgroups of $\mathrm{M}(2,\mathbb{F}_p)$ as in Theorem* 5.1. *If $H \cong K$ then $H = K$ (so two finite irreducible subgroups of $\mathrm{M}(2,\mathbb{F}_p)$ are $\mathrm{GL}(2,\mathbb{F}_p)$-conjugate if and only if they are isomorphic).*

Proof. Suppose $H(i,j,k) \cong H(i',j',k')$. These groups have the same centre, meaning $i = i'$. If $j, j' \geq 1$ then $j = j'$ and $k = k'$ by [5, Proposition 3.3]. If $j = j' = 0$ then $k = k' = 3$ or $k, k' \in \{1,2\}$, for the groups to have the same order; but $H(i,0,2)$ is cyclic whereas $H(i,0,1)$ is not, so $k = k'$. Let $j = 0$, $j' \geq 1$. By another order comparison, $k = 3$, $j' = 1$, and $k' = 1$ or 2. Indeed, $H(i,0,3)$ is isomorphic to $H(i,1,2)$ if $i \geq 1$ and to $H(i,1,1)$ if $i = 0$, as shown in the proof of Theorem 5.1. We conclude that these are the only isomorphisms between the $H(i,j,k)$.

Suppose $H \cong K$. Then H_2, K_2 are isomorphic, as Sylow 2-subgroups of H, K. For each odd prime r dividing $|H|$, $\mathsf{O}_r(H)$ and $\mathsf{O}_r(K)$ have the same order and the

same scalar subgroup. Thus (see Remark 5.2), $\mathsf{O}_r(H) = \mathsf{O}_r(K)$ and so $H_{2'} = K_{2'}$. By the previous paragraph and Theorem 5.1, if $H_2 \neq K_2$ then H_2' is nonscalar and either $H_2, K_2 \in \{H(0,0,3), H(0,1,1)\}$ or $H_2, K_2 \in \{H(i,0,3), H(i,1,2)\}$, $i \geq 1$. Any abelian subgroup A of index 2 in H contains $H_{2'}$, and if $H_{2'}$ is nonscalar then $A = \mathrm{D}(2,\mathbb{F}_p) \cap H$. In that event an isomorphism $H \to K$ restricts to an isomorphism $\mathrm{D}(2,\mathbb{F}_p) \cap H_2 \to \mathrm{D}(2,\mathbb{F}_p) \cap K_2$. However, the diagonal subgroups of the nominated H_2, K_2 have isomorphism types $C_2 \times C_2$, C_4, and $C_{2^{i+2}}$, $C_2 \times C_{2^{i+1}}$ for $i \geq 1$. Hence $H_2 = K_2$. □

Theorems 5.1 and 5.3 together with Remark 5.2 give a complete and irredundant list of the finite irreducible subgroups of $\mathrm{M}(2,\mathbb{F}_p)$. Section 2 is not needed because [5] applies to monomial groups over any field, like $\mathbb{F}_p$, that has elements of every 2-power order and whose characteristic is not 2.

Next, we list finite primitive subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ as required by Proposition 3.6(i).

Theorem 5.4. *Suppose $p \geq 5$. Let H be a finite primitive subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$ such that $H/\mathsf{Z}(H) \cong A_4$. Write $\mathsf{Z}(H) = Z = \langle\, z \,\rangle$. Let $\omega \in \mathbb{F}_p$ be a primitive fourth root of unity, and define*

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

Choose $\nu \in \mathbb{F}_p \backslash Z$ such that $\nu^3 = z$ (denoting a scalar matrix by its nonzero entry). Then $|Z|$ is even,

$$\langle\, (\omega, -\omega),\, s,\, z \,\rangle, \qquad \langle\, (\omega, -\omega),\, \nu s \,\rangle$$

are distinct primitive subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ with centre $\langle\, z \,\rangle$ and central quotient A_4, and H is conjugate to precisely one of them.

Proof. (Cf. [25, Sec. 5.3].) For each prime r dividing $|Z|$, denote the Sylow r-subgroup of Z by Z_r. If $Z_2 \neq 1$ then by the Universal Coefficient Theorem,

$$H^2(A_4, Z) = \mathrm{Ext}(A_4/A_4', Z_3) \times \mathrm{Hom}(H_2(A_4), Z_2) \cong \begin{cases} C_3 \times C_2 & Z_3 \neq 1 \\ C_2 & Z_3 = 1 \end{cases}.$$

The 2-cocycle classes in $H^2(A_4, Z)$ and presentations for corresponding extensions of Z by A_4 may be calculated by the algorithm in [13]. For example, if $[\xi] \in \mathrm{Ext}(A_4/A_4', Z_3)$ and E is a corresponding extension, then because ξ is trivial on $V_4 = A_4'$, E has an abelian normal subgroup N containing Z such that $N/Z \cong V_4$. Since an abelian normal subgroup of H is cyclic, $H \ncong E$. Thus the extension equivalence class of H cannot be in $\mathrm{Ext}(A_4/A_4', Z_3)$, so Z_2 cannot be trivial.

In the usual way $\mathrm{Aut}(A_4)$ acts on $H^2(A_4, Z)$, and 2-cocycle classes in the same $\mathrm{Aut}(A_4)$-orbit give rise to isomorphic extensions. The inner automorphism of S_4 that is conjugation by (12), restricted to A_4, inverts each element of $H^2(A_4, Z)$

of order 3 (if any exist). Hence there are at most two possible isomorphism types for H. The one corresponding to the nontrivial element of $\mathrm{Hom}(H_2(A_4), Z_2)$ has a subgroup K isomorphic to $\mathrm{SL}(2,3)$ (the unique nonsplit extension of C_2 by A_4) such that $K \cap Z = \langle\, (-1,-1) \,\rangle$, and thus $H = KZ$. The other type exists only if $Z_3 \neq 1$. It does not have a subgroup isomorphic to $\mathrm{SL}(2,3)$, since its Sylow 3-subgroups are cyclic of order $3|Z_3|$, and so its elements of order 3 are central.

Since p does not divide $|\mathrm{SL}(2,3)|$, we see from its character table that $\mathrm{SL}(2,3)$ has exactly three inequivalent faithful irreducible representations in $\mathrm{GL}(2,\mathbb{F}_p)$. Two of these are related by an outer automorphism of $\mathrm{SL}(2,3)$, so there are at most two non-conjugate irreducible subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$ isomorphic to $\mathrm{SL}(2,3)$. Indeed, if $\mu \in \mathbb{F}_p$ is a primitive cube root of unity then

$$K_1 = \langle\, (\omega, -\omega),\, s \,\rangle\,, \qquad K_2 = \langle\, (\omega, -\omega),\, \mu s \,\rangle$$

are both isomorphic to $\mathrm{SL}(2,3)$, and are therefore irreducible by Maschke's Theorem. Each K_i is primitive because it does not have an abelian subgroup of index 2. K_1 but not K_2 is in $\mathrm{SL}(2,\mathbb{F}_p)$, so K_1 and K_2 are not conjugate.

If H has a subgroup isomorphic to $\mathrm{SL}(2,3)$ then H is conjugate to K_1Z or K_2Z. Now suppose H does not have a subgroup isomorphic to $\mathrm{SL}(2,3)$. Choose $h \in H \backslash Z$ and a scalar ν not in Z such that $h^3 = z$ and $\nu^3 = z$ (as $p > 3$, such a ν surely exists). Then $\langle\, H,\, \nu \,\rangle$ has a subgroup $K \cong \mathrm{SL}(2,3)$, generated by $\nu^{-1}h$ and a nonsplit extension of $\langle\, (-1,-1) \,\rangle$ by V_4. For some $x \in \mathrm{GL}(2,\mathbb{F}_p)$, we have $K^x = K_j$, $j = 1$ or 2, so $H^x/Z \cong A_4$ is a subgroup of $\langle\, K_jZ,\, \nu \,\rangle/Z \cong A_4 \times C_3$. Here $\mu \in Z_3$, so $K_1Z = K_2Z$. There are three subgroups of $\langle\, K_1Z,\, \nu \,\rangle$ whose quotient modulo Z is isomorphic to A_4, namely

$$K_1Z\,, \qquad \langle\, (\omega, -\omega),\, \nu s \,\rangle\,, \qquad \langle\, (\omega, -\omega),\, \nu^2 s,\, z \,\rangle\,.$$

The second and third groups are conjugate by (α, α^{-1}), where $\alpha \in \mathbb{F}_p$ is a square root of ω.

So far we have proved that H is conjugate to one of

$$\langle\, (\omega, -\omega),\, s,\, z \,\rangle \qquad \langle\, (\omega, -\omega),\, \mu s,\, z \,\rangle \qquad \langle\, (\omega, -\omega),\, \nu s \,\rangle\,.$$

As noted above, if $Z_3 \neq 1$ then the first and second groups are equal. If $Z_3 = 1$ then we may choose $\nu \in \mu Z$, and the second and third groups coincide. □

Remark 5.5. Let $G \leq \mathrm{GL}(n,\mathbb{F}_p)$ be primitive, p any prime. It seems to be reasonably well-known that $\mathrm{Fit}(G)/\mathsf{Z}(G)$ is a finite p'-group. Thus if $G/\mathsf{Z}(G) \cong A_4$ or S_4 then $p \neq 2$.

Remark 5.6. The generators for the primitive absolutely irreducible linear groups in Theorem 5.4 were chosen with classical results of Klein and Jordan in mind ([3, Chap. 3]). These results amount to a complete and irredundant list of the finite subgroups of $\mathrm{SL}(2,\mathbb{C})$. A finite primitive p'-subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$ has the same collineation group as some primitive subgroup of $\mathrm{SL}(2,\mathbb{C})$.

6. Solution of the Main Listing Problem

Again p is odd throughout. Recall the definitions of ω_i, z_i, w_i, $w_{i,r}$ and $H(i,j,k)$ made in Sec. 5.

Proposition 6.1. *Let G be an irreducible but not absolutely irreducible nonabelian subgroup of $\mathrm{M}(4,q)$ with πG a 2-group. Then G is conjugate to $G_2G_{2'}$, where*

$$G_2 = \{(h,h^\sigma)\,|\,h \in H_2\}\,, \qquad G_{2'} = \{(h,h^\sigma)\,|\,h \in H_{2'}\}$$

for some irreducible subgroup $H_2H_{2'}$ of $\mathrm{M}(2,\mathbb{F}_p)$ as stated in Theorem 5.1. Furthermore

(i) *$H_{2'} \leq \mathrm{D}(2,q)$ and $G_{2'} \leq \mathrm{D}(4,q)$.*

(ii) *If $q \equiv 1 \bmod 4$ and the Sylow 2-subgroup of $\mathrm{GF}(q^2)^\times$ has order 2^{t+1} then $H_2 = H(i,j,k)$, where $0 \leq i,j \leq t$, $j \geq 1$ if $H_{2'}$ is scalar, and*

$$\begin{gathered} i = t \text{ or } j = t\,, \qquad 1 \leq k \leq 2 \\ \left.\begin{aligned} &i = j = t \\ &i = t-1,\ j \leq t-2 \\ &i \leq t-2,\ j = t-1 \end{aligned}\right\}\ k = 3. \end{gathered}$$

(iii) *If $q \equiv 3 \bmod 4$ then H_2 is one of*

$$\begin{aligned} &H(0,2,1), \quad q \equiv 3 \bmod 8 \text{ only} \\ &H(1,j,k), \quad 0 \leq j \leq 1, \quad 1 \leq k \leq 2 \\ &H(0,1,k), \quad 1 \leq k \leq 2 \\ &H(0,1,3), \quad q \equiv 7 \bmod 8 \text{ only} \\ &H(1,1,3)\,, \end{aligned}$$

where $H_2 \neq H(1,0,k)$, $H(0,1,k)$ if $H_{2'}$ is scalar, and $H_{2'}$ is scalar if $H_2 = H(0,2,1)$ or $H(0,1,3)$.

(iv) *Conversely, if $H_2 \leq \mathrm{M}(2,\mathbb{F}_p)$ is conjugate to $H(i,j,k)$ for any i,j,k as stipulated in* (ii) *or* (iii) *then $G_2G_{2'}$ is conjugate to an irreducible but not absolutely irreducible subgroup of $\mathrm{GL}(4,q)$.*

Proof. By Proposition 3.6, G is conjugate to $\tilde{G} = \{(h,h^\sigma)\,|\,h \in H\}$, where H is an absolutely irreducible subgroup of $\mathrm{M}(2,q^2)$ such that $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$. By Theorem 5.1, $H^x = H_2H_{2'}$ for some $x \in \mathrm{GL}(2,\mathbb{F}_p)$ and H_2H_2' as in the theorem. Then $\tilde{G}^{(x,x^\sigma)} = G_2G_{2'}$.

(i) $G_{2'} \leq \mathrm{D}(4,q)$ by Lemma 4.3(i) and (ii), so clearly $H_{2'} \leq \mathrm{D}(2,q)$.

(ii) The Sylow 2-subgroup of $\mathrm{GF}(q)^\times$ has order 2^t. From (i), $\mathrm{tr}(H_2) \subseteq \mathrm{GF}(q^2)$ yet $\mathrm{tr}(H_2) \not\subseteq \mathrm{GF}(q)$. Thus $H_2 = H(i,j,k)$ for some $i,j \geq 0$. Evaluating $\mathrm{tr}(z_i)$ and $\mathrm{tr}(w_j)$, we infer that $i \leq t$, and $j \leq t$ by Lemma 4.2.

Suppose $k = 1$ or 2. If i and j are both less than t then $\mathrm{tr}(H_2) \subseteq \mathrm{GF}(q)$. Hence $i = t$ or $j = t$. Now suppose $k = 3$. If $i = t$ then $j = t$: otherwise, $\mathrm{tr}(z_{t+1}w_{j+1}w_{k,r}) \in \mathrm{GF}(q^2)$, r an odd prime dividing $q-1$, forces $\omega_{t+1} \in \mathrm{GF}(q^2)$ (we only need to choose $w_{k,r} \neq 1$ when $j = 0$ and H_2' is nonscalar). If $i = t-1$ then similarly $j \neq t$ by Lemma 4.2; nor can we have $j = t-1$, to ensure that $H_2 \not\leq \mathrm{M}(2,q)$. For the same reason $j \geq t-1$ if $i \leq t-2$, in which case $j \neq t$ by Lemma 4.2.

(iii) Here a Sylow 2-subgroup of $\mathrm{M}(4,q)$ has exponent 8, which is therefore an upper bound on the exponent of G_2. An element of $\mathrm{M}(4,q)$ of order 8 projects on to a 4-cycle in S_4 and thus has zero trace.

Since $N := \mathsf{O}_2(\mathrm{D}(4,q) \cap G)$ is elementary abelian, if $|N| \geq 8$ then G acts faithfully on N and G is absolutely irreducible. Hence $|N| \leq 4$ and $|H_2| = |G_2| \leq 32$. Trace calculations show that $|H_2| > 4$.

Let $H_2 = H(i,j,k)$; then $i \leq 2$, because $|\mathsf{Z}(H(i,j,k))| = 2^{i+1}$. If $i = 2$ then G has an element of order 8, conjugate to $(\omega_2, \omega_2, \omega_2^q, \omega_2^q)$. However $\omega_2 + \omega_2^q \neq 0$.

For $k = 1$ or 2, $1 \leq i + j \leq 3$. Since $i \leq 1$, $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$, and no element of H_2 can have order greater than 8, we see that $(i,j) \in \{(0,2),(1,0),(1,1),(1,2)\}$, or $(i,j) = (0,1)$ and $H_{2'}$ is nonscalar. On the other hand $(i,j) \in \{(0,1),(1,0),(1,1)\}$ if $k = 3$.

We have $\omega_2^q = \omega_2\omega_1^{(q-1)/2}$ and $\omega_2^{-q} = \omega_2\omega_1^{(q+1)/2}$. If $H_2 = H(i,2,k)$ then the element $(\omega_2, \omega_2^{-1}, \omega_2^q, \omega_2^{-q})$ of G_2 has order 8, and for this matrix to have zero trace, $q \equiv 3 \bmod 8$. Similarly q must be congruent to 7 mod 8 when $H_2 = H(0,1,3)$.

Suppose $H_2 = H(1,2,k)$, so that $K := \langle\, z_1,\, w_2 \,\rangle \leq H_2$. If $\{(h, h^\sigma) \mid h \in K\}$ were conjugate to a subgroup of $\mathrm{M}(4,q)$ then that subgroup would have projection C_4 in S_4, and would therefore contain four different scalars. But a Sylow 2-subgroup of $\mathrm{M}(4,q)$ has just two scalars. There is a unique involution in $H(0,2,2) \cong Q_{16}$, whereas a subgroup of $\mathrm{M}(4,q)$ conjugate to $\{(h, h^\sigma) \mid h \in H(0,2,2)\}$ could only be an extension of $\langle\, (-1,-1,-1,-1) \,\rangle$ by D, with nonscalar involutions. We have proved that H_2 is not $H(1,2,1)$ nor $H(1,2,2)$ nor $H(0,2,2)$.

If H_2 has a diagonal element of order 8 then there exists an abelian index 2 subgroup of G with projection C_4 in S_4. As this subgroup contains $\mathsf{O}_{2'}(G)$, the latter is central in G, so $H_{2'}$ is central in $H_2H_{2'}$. Hence $H_{2'}$ is scalar if $H_2 = H(0,2,1)$ or $H(0,1,3)$ ($z_2w_1 \in H(1,0,3)$ and $|z_2w_1| = 8$, but $H_2 \neq H(1,0,3)$ by Theorem 5.1(i) if $H_{2'}$ is scalar).

(iv) This follows from Corollary 3.5, as $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$ for the stipulated values of i,j,k. □

Lemma 6.2. *Define*

$$m = \begin{pmatrix} \omega_t & \omega_{t-1} \\ -1 & \omega_t \end{pmatrix} \otimes I_2 \in \mathrm{GL}(4,q^2)$$

where 2^t *is the order of the Sylow* 2*-subgroup of* $\mathrm{GF}(q)^\times$.

(i) *If* $h \in \mathrm{GL}(2,q)$ *then* $(h,h^\sigma)^m = (h,h)$.

(ii) *If* h *is* $(\omega_t, 1)$, $(1, \omega_t)$, z_t, *or* w_t *then* $(h, h^\sigma)^m$ *is* $ac(1, 1, \omega_{t-1}, 1)$, $ac^{-1}(1, 1, 1, \omega_{t-1})$, $b(1, 1, \omega_{t-1}, \omega_{t-1})$, *or* $b(1, \omega_{t-1}^{-1}, \omega_{t-1}, 1)$, *respectively.*

Definition 6.3. For each odd prime r dividing $q-1$, choose a generator α_r of the Sylow r-subgroup of $\mathrm{GF}(q)^\times$. Define $\mathcal{G}_{2'}$ to be the list of all direct products

$$\prod_{r\in\triangle} \langle\, (\alpha_r, \alpha_r, \alpha_r, \alpha_r)^{r^{k_r}},\, (\alpha_r, \alpha_r^{-1}, \alpha_r, \alpha_r^{-1})^{r^{l_r}} \,\rangle$$

as $\triangle$ ranges over subsets of the set of odd prime divisors of $q-1$, and $0 \le k_r, l_r \le \log_r |\alpha_r|$. If $G_{2'}$ is a subgroup of $\mathrm{D}(4, q)$ arising from an odd order $\mathbb{Z}S_2$-submodule $H_{2'}$ of $\mathrm{D}(2, q)$ as in Proposition 6.1, then $G_{2'} \in \mathcal{G}_{2'}$ by Remark 5.2.

Theorem 6.4. *Suppose* $q \equiv 1 \bmod 4$ *and let* 2^t *be the order of the Sylow* 2*-subgroup of* $\mathrm{GF}(q)^\times$. *Define lists* $\mathcal{G}_{2,1}$ *and* $\mathcal{G}_{2,2}$ *of* 2*-subgroups of* $\mathrm{M}(4, q)$ *as follows*:

$$\begin{aligned}
\mathcal{G}_{2,1} : &\langle\, a,\, b(1, 1, \omega_{t-1}, \omega_{t-1}),\, (\omega_{t-1}, 1, \omega_{t-1}, 1) \,\rangle \\
&\langle\, c(1, 1, \omega_{t-1}, 1),\, (\omega_{t-1}, 1, \omega_{t-1}, 1) \,\rangle \\
&\langle\, a,\, c(1, 1, \omega_{t-1}, 1),\, (\omega_{t-1}, 1, \omega_{t-1}, 1) \,\rangle \\
&\langle\, a,\, b(1, \omega_{t-1}^{-1}, \omega_{t-1}, 1),\, (\omega_i, \omega_i, \omega_i, \omega_i) \,\rangle \qquad 0 \le i \le t-1
\end{aligned}$$

$$\begin{aligned}
&\langle\, a(\omega_i, 1, \omega_i, 1),\, b(1, \omega_{t-1}^{-1}, \omega_{t-1}, 1) \,\rangle && 0 \le i \le t-1 \\
&\langle\, a,\, b(\omega_{i+1}, \omega_{i+1}\omega_{t-1}^{-1}, \omega_{i+1}\omega_{t-1}, \omega_{i+1}),\, (\omega_{t-1}, \omega_{t-1}^{-1}, \omega_{t-1}, \omega_{t-1}^{-1}) \,\rangle && 0 \le i \le t-2 \\
&\langle\, a,\, b(1, 1, \omega_{t-1}, \omega_{t-1}),\, (\omega_i, \omega_i^{-1}, \omega_i, \omega_i^{-1}) \,\rangle && 1 \le i \le t-1 \\
&\langle\, c(1, 1, \omega_{t-1}, 1),\, (\omega_i, \omega_i^{-1}, \omega_i, \omega_i^{-1}) \,\rangle && 1 \le i \le t-1 \\
&\langle\, a,\, b(\omega_{i+1}, \omega_{i+1}^{-1}, \omega_{i+1}\omega_{t-1}, \omega_{i+1}^{-1}\omega_{t-1}),\, (\omega_i, \omega_i^{-1}, \omega_i, \omega_i^{-1}) \,\rangle && 1 \le i \le t-2\,.
\end{aligned}$$

$$\begin{aligned}
\mathcal{G}_{2,2} : &\langle\, a,\, b(1, 1, \omega_{t-1}, \omega_{t-1}) \,\rangle\,, \\
&\langle\, c(1, 1, \omega_{t-1}, 1) \,\rangle\,, \\
&\langle\, a,\, b(\omega_1, -\omega_1, \omega_{t-1}\omega_1, -\omega_{t-1}\omega_1) \,\rangle\,.
\end{aligned}$$

The list $\mathcal{G}$ *consisting of all groups* $G_2 G_{2'}$, $G_{2'} \in \mathcal{G}_{2'}$ (*see Definition* 6.3), *and* $G_2 \in \mathcal{G}_{2,1}$ *or* $G_2 \in \mathcal{G}_{2,1} \cup \mathcal{G}_{2,2}$ *if* $G_{2'}$ *is scalar or nonscalar, respectively, is a complete and irredundant list of the nonabelian irreducible but not absolutely irreducible subgroups* G *of* $\mathrm{M}(4, q)$ *with* πG *a* 2*-group.*

Proof. A group in $\mathcal{G}$ has the form $\{(h, h^\sigma) \,|\, h \in H\}^m$ where m is the matrix of Lemma 6.2 (which centralizes every element of $\mathcal{G}_{2'}$ by Lemma 6.2(i)) and H is an irreducible subgroup $H_2 H_{2'}$ of $\mathrm{M}(2, \mathbb{F}_p)$ as specified in Proposition 6.1(ii), except when $H_2 = H(t, j, 2)$, $0 \le j \le t$ (then $H = H(t, j, 2)^{w_{t+2}} H_{2'}$), or when $H_2 = H(i, t, 2)$, $0 \le i \le t-1$ (then $H = H(i, t, 2)^{w_{i+2}} H_{2'}$). This claim summarizes the routine compilation of $\mathcal{G}$, details of which are omitted. Note that if $H_{2'}$ is nonscalar

then $G_{2'}$ is nonscalar (and vice versa) and H_2 could be $H(t,0,1)$, $H(t,0,2)$, or $H(t-1,0,3)$; these give rise to the groups in $\mathcal{G}_{2,2}$.

Every group in $\mathcal{G}$ is irreducible by Proposition 6.1(ii). Also by Proposition 6.1 and the Deuring–Noether Theorem, $\mathcal{G}$ is complete. Suppose $G, \bar{G} \in \mathcal{G}$ are isomorphic and arise from (isomorphic) subgroups H, $\bar{H}$ of $\mathrm{M}(2,\mathbb{F}_p)$. If H, $\bar{H}$ are listed in Theorem 5.1 then $H = \bar{H}$ by Theorem 5.3, and thus $G = \bar{G}$. Otherwise H and $\bar{H}$ both have Sylow 2-subgroup $H(t,j,2)^{w_{t+2}}$ or $H(i,t,2)^{w_{i+2}}$. Since H^w and $\bar{H}^w$ are then listed in Theorem 5.1 for some $w \in \mathrm{D}(2,\mathbb{F}_p)$, one more appeal to Theorem 5.3 finishes the proof that $\mathcal{G}$ is irredundant. □

Theorem 6.5. *Suppose* $q \equiv 3 \bmod 4$ *and define lists* $\mathcal{G}_{2,1}$, $\mathcal{G}_{2,2}$, *and* $\mathcal{G}_{2,3}$ *of* 2*-subgroups of* $\mathrm{M}(4,q)$ *as follows*:

$$\begin{aligned}
\mathcal{G}_{2,1} &: \langle\, a(1,1,-1,-1),\, c(1,1,-1,1)\,\rangle \qquad q \equiv 3 \bmod 8 \text{ only}\\
&\quad \langle\, a(1,-1,-1,1),\, c(1,1,-1,1)\,\rangle \qquad q \equiv 7 \bmod 8 \text{ only}.\\
\mathcal{G}_{2,2} &: \langle\, a,\, b(1,1,-1,-1)\,\rangle\\
&\quad \langle\, a,\, b(1,-1,-1,1)\,\rangle\\
&\quad \langle\, c(1,1,-1,1)\,\rangle\\
&\quad \langle\, a(1,-1,1,-1),\, b(1,-1,-1,1)\,\rangle.\\
\mathcal{G}_{2,3} &: \langle\, a,\, b(1,1,-1,-1),\, (1,-1,1,-1)\,\rangle\\
&\quad \langle\, c(1,1,-1,1),\, (1,-1,1,-1)\,\rangle\\
&\quad \langle\, a,\, c(1,1,-1,1),\, (1,-1,1,-1)\,\rangle.
\end{aligned}$$

The list consisting of all groups $G_2G_{2'}$, *where* $G_{2'} \in \mathcal{G}_{2'}$ (*see Definition* 6.3), *and* $G_2 \in \mathcal{G}_{2,1} \cup \mathcal{G}_{2,3}$ *or* $G_2 \in \mathcal{G}_{2,2} \cup \mathcal{G}_{2,3}$ *if* $G_{2'}$ *is scalar or nonscalar, respectively, is a complete and irredundant list of the nonabelian irreducible but not absolutely irreducible subgroups* G *of* $\mathrm{M}(4,q)$ *with* πG *a* 2*-group.*

Proof. Let $H_2H_{2'}$ be as in Proposition 6.1(iii). If H_2 contains no diagonal element of order 8 then we can get a conjugate of $\{(h,h^\sigma) \mid h \in H_2H_{2'}\}$ in $\mathrm{M}(4,q)$ by Lemma 6.2. That leaves us with the (more onerous) conjugacy problem for $H_2H_{2'}$ where $H_2 = H(0,2,1)$ or $H_2 = H(0,1,3)$ and $H_{2'}$ is scalar. Let

$$m = \begin{pmatrix} -\omega_2\omega_1 & 1 & -\omega_2 & -\omega_1 \\ \omega_2 & 1 & \omega_2\omega_1 & \omega_1 \\ -\omega_2 & 1 & -\omega_2\omega_1 & \omega_1 \\ \omega_2\omega_1 & 1 & \omega_2 & -\omega_1 \end{pmatrix}.$$

Row reduction shows that $m \in \mathrm{GL}(4,\mathbb{F}_p)$. Also

$$(a(\omega_2, -\omega_2\omega_1, \omega_2\omega_1, -\omega_2))^m = a(1,1,-1,-1)$$

and

$$(\omega_2, -\omega_2\omega_1, \omega_2\omega_1, -\omega_2)^m = c^{-1}(1,-1,1,1)\,;$$

hence the group listed first in $\mathcal{G}_{2,1}$. The second group results from similar manipulations. For all other statements, cf. the proof of Theorem 6.4. □

Proposition 6.6. *Suppose $p \geq 5$. Then $\mathrm{M}(4,q)$ has an irreducible but not absolutely irreducible subgroup G such that $\pi G = A_4$ if and only if $q-1$ is not divisible by 3. If $q-1$ is not divisible by 3 then $|\mathsf{Z}(G)|$ is even and G is $\mathrm{GL}(4,q)$-conjugate to*

$$\langle\, a(1,-1,-1,1),\, d,\, \mathsf{Z}(G) \,\rangle\,.$$

Proof. Suppose G exists. By Proposition 3.6 and Theorem 5.4, G is conjugate to $\{(h,h^\sigma)\,|\,h\in H\}$, where H is $\langle\,(\omega,-\omega),\, s,\, z\,\rangle$ or $\langle\,(\omega,-\omega),\, \nu s,\, z\,\rangle$, $\mathsf{Z}(H) = \langle\, z\,\rangle$, and $\mathrm{tr}(H) \subseteq \mathrm{GF}(q^2)$ yet $\mathrm{tr}(H) \not\subseteq \mathrm{GF}(q)$. Additionally $\mathsf{Z}(G) = \langle\,(z,z^\sigma)\,\rangle$ is scalar, so that $z \in \mathrm{GF}(q)$.

Since each element of $\langle\,(\omega,-\omega),\, s\,\rangle \cong \mathrm{SL}(2,3)$ has trace in $\{0,\pm1,\pm2\} \subseteq \mathrm{GF}(q)$, H cannot be $\langle\,(\omega,-\omega),\, s,\, z\,\rangle$. If 3 divides $q-1$ then $\mathrm{GF}(q^2)^\times$, $\mathrm{GF}(q)^\times$ have the same Sylow 3-subgroup, which contains some element of $\nu\mathsf{Z}(H)$, and we exhaust all choices for H.

Henceforth in the proof, 3 does not divide $q-1$. There is an element of $\nu\mathsf{Z}(H)$ with trivial cube, so we assume $\nu^3 = 1$, and thus $\nu \in \mathrm{GF}(q^2)\backslash\mathrm{GF}(q)$. Define $m \in \mathrm{GL}(4,\mathbb{F}_p)$ by

$$m = \begin{pmatrix} m_1 & m_2 \\ m_1' & m_2' \end{pmatrix},$$

where

$$m_1 = \begin{pmatrix} 1 & \nu(\omega-\nu) \\ -\omega & -\nu(\nu\omega+1) \end{pmatrix}, \qquad m_2 = \begin{pmatrix} 1 & \nu(\nu\omega-1) \\ -\omega & -\nu(\omega+\nu) \end{pmatrix}$$

and $m_i' = m_i(-1,1)a_1$, $i = 1, 2$.

Let $q \equiv 1 \bmod 4$. Then (h,h^σ) is $(\omega,-\omega,\omega,-\omega)$ if $h = (\omega,-\omega)$, and $\nu(s,\nu s)$ if $h = \nu s$. We check that

$$(\omega,-\omega,\omega,-\omega) = (a(1,-1,-1,1))^m\,, \qquad \nu(s,\nu s) = d^m\,.$$

Thus G is conjugate to the subgroup $\langle\, a(1,-1,-1,1),\, d,\, \mathsf{Z}(G)\,\rangle$ of $\mathrm{GL}(4,q)$, which is irreducible by Corollary 3.5. The proof in this case is then complete.

Suppose now that $q \equiv 3 \bmod 4$. Then (h,h^σ) is $(\omega,-\omega,-\omega,\omega)$ if $h = (\omega,-\omega)$, and $\nu(s,\nu s^{(12)(1,-1)})$ if $h = \nu s$. Since

$$(\omega,-\omega,-\omega,\omega) = (\omega,-\omega,\omega,-\omega)^{ae(1,1,1,-1)} = (a(1,-1,-1,1))^{mae(1,1,1,-1)}$$

and

$$\nu(s,\nu s^{(12)(1,-1)}) = \nu(s,\nu s)^{ae(1,1,1,-1)} = d^{mae(1,1,1,-1)}\,,$$

we are done. □

Theorem 6.7. *The following are irreducible but not absolutely irreducible subgroups of* $\mathrm{M}(4,5)$:

$$\langle\, a,\ b(1,1,2,2),\ (2,1,2,1)\,\rangle$$
$$\langle\, c(1,1,2,1),\ (2,1,2,1)\,\rangle$$
$$\langle\, a,\ c(1,1,2,1),\ (2,1,2,1)\,\rangle$$
$$\langle\, a,\ b(1,3,2,1),\ (4,4,4,4)\,\rangle$$
$$\langle\, a,\ b(1,3,2,1),\ (2,2,2,2)\,\rangle$$
$$\langle\, a(4,1,4,1),\ b(1,3,2,1)\,\rangle$$
$$\langle\, a(2,1,2,1),\ b(1,3,2,1)\,\rangle$$
$$\langle\, a,\ b(2,1,4,2),\ (2,3,2,3)\,\rangle$$
$$\langle\, a,\ b(1,1,2,2),\ (2,3,2,3)\,\rangle$$
$$\langle\, c(1,1,2,1),\ (2,3,2,3)\,\rangle$$
$$\langle\, a(1,4,4,1),\ d,\ (4,4,4,4)\,\rangle$$
$$\langle\, a(1,4,4,1),\ d,\ (2,2,2,2)\,\rangle$$
$$\langle\, c(2,1,1,1)\,\rangle\,.$$

The union of this list and the one in Theorem 4.5 *is a complete and irredundant list of the irreducible subgroups of* $\mathrm{M}(4,5)$.

Proof. We combine Theorem 6.4 and Propositions 3.12 and 6.6, for $q = 5$. The union is complete and irredundant by these results, Propositions 3.6 and 3.9, and Theorem 4.5. □

7. Computing Lists of Irreducible Monomial Linear Groups

Many of the basic computational problems for finite degree permutation groups have been solved. This contrasts markedly with the current situation for linear groups over finite fields. To list the irreducible subgroups of $\mathrm{M}(n,q)$ by computer we therefore work in a permutation group setting. (Alternatively, if $n \leq 4$ then $\mathrm{M}(n,q)$ is soluble and we may work with a polycyclic presentation of $\mathrm{M}(n,q)$.) We begin by representing $\mathrm{M}(n,q)$ faithfully as a permutation group $\mathrm{P}(n,q)$ via its action on the set

$$\{(\omega^{i_1},0,\ldots,0),(0,\omega^{i_2},0,\ldots,0),\ldots,(0,\ldots,0,\omega^{i_n})\,|\,0\leq i_1,i_2,\ldots,i_n\leq q-2\}$$

of $nq-n$ vectors in $\mathrm{GF}(q)^{(n)}$, where $\mathrm{GF}(q)^\times = \langle\,\omega\,\rangle$. Then we compute the subgroup lattice of $\mathrm{P}(n,q)$, which is returned as a list $\mathcal{S}$ of subgroups of $\mathrm{Sym}(nq-n)$. With the elements of $\mathcal{S}$ represented in $\mathrm{M}(n,q)$, the reducible ones are eliminated, producing a list $\mathcal{M}$. An irreducible subgroup of $\mathrm{M}(n,q)$ is $\mathrm{M}(n,q)$-conjugate to a single element

of $\mathcal{M}$. We use the faithful permutation representation of $\mathrm{GL}(n,q)$ in $\mathrm{Sym}(q^n)$ arising from the natural action on $\mathrm{GF}(q)^{(n)}$ to refine $\mathcal{M}$ to a list whose elements are not $\mathrm{GL}(n,q)$-conjugate.

For $n = 4$ and $q = 5$ we compute that $\mathcal{M}$ has 216 elements, and these fuse into 155 $\mathrm{GL}(4,5)$-conjugacy classes — just as predicted by Theorems 4.5 and 6.7. We may check by computer that the groups listed in Theorems 4.5 and 6.7 are all irreducible, and that distinct groups are not $\mathrm{GL}(4,5)$-conjugate. Thus we verify our list is correct. (Other tests are possible.)

The naive approach to computing irreducible subgroups of $\mathrm{M}(n,q)$, above, is limited by the sorting of groups into $\mathrm{GL}(n,q)$-conjugacy classes, since that employs a permutation representation of degree q^n. To overcome the limitation, we propose listing algorithms modeled on ideas in this paper. Combined output from these algorithms is a complete and irredundant list of the irreducible monomial subgroups of $\mathrm{GL}(n,q)$, where $n < 31$ is a prime or 4, and q is a power of a prime $p > n$. Each group is returned as a generating set of monomial matrices. We recap the principal ideas below.

One algorithm deals with the non-absolutely irreducible groups. Its input is just n and q, and it is wholly deterministic: if $n = 4$, the algorithm would be an implementation of Proposition 3.12 and Sec. 6; if n is (any) prime then there are only cyclic groups to worry about, and it is not difficult to formulate a thorough description of those groups (cf. Proposition 3.12) for implementation.

As well as n, q, input to the algorithm for listing the absolutely irreducible subgroups of $\mathrm{M}(n,q)$ is a finite sublist $\mathcal{L}$ of a list $\mathcal{L}_{n,\mathbb{C}}$ of the finite irreducible subgroups of $\mathrm{M}(n,\mathbb{C})$. Like all existing lists, $\mathcal{L}_{n,\mathbb{C}}$ has a prescribed format, suited to our objective. Groups are given by parametrized generating sets of monomial matrices. Nonzero entries of generators for p'-groups are p'-roots of unity (see the second last paragraph before Proposition 2.12 for an explanation of why matrix entries can always be chosen this way). The diagonal matrices in each generating set generate the diagonal subgroup of the group, and by this fact one gets a pre-defined order function for each listed group (a function of integer parameters labeling the group). Given N, we can then find the finitely many groups in $\mathcal{L}_{n,\mathbb{C}}$ of order N. Hence we can find the finite sublist $\mathcal{L}$ of $\mathcal{L}_{n,\mathbb{C}}$ whose elements have orders dividing $n!(q-1)^n$. Further cut downs of $\mathcal{L}$ come from analyzing diagonal subgroups; for $n = 4$, cf. Lemmas 4.3 and 4.4. We emphasize that all of these considerations are purely theoretical ones, to be settled in advance. They are not part of the algorithm proper.

Reduction mod p of the generating sets for the groups in $\mathcal{L}$ produces a list $\Psi(\mathcal{L})$ of finite irreducible p'-subgroups of $\mathrm{M}(n,\mathbb{F}_p)$ that is complete (by Theorems 2.17 and 4.1) and irredundant (by Proposition 2.7). Say all nonzero entries of generators of groups in $\mathcal{L}$ belong to $\langle\,\omega\,\rangle \leq \mathbb{C}^\times$, and let $\zeta \in \mathbb{F}_p$ be a primitive $|\omega|$th root of unity. Then the mod p reduction of $\mathcal{L}$ is simply putting ζ^i for ω^i everywhere in generating sets of groups in $\mathcal{L}$.

The reduced list $\Psi(\mathcal{L})$ contains, up to conjugacy, a list of the absolutely irreducible subgroups of $\mathrm{M}(n,q)$. Conjugacy classes of each group in $\Psi(\mathcal{L})$ are computed, and a group is deleted from $\Psi(\mathcal{L})$ if some conjugacy class representative fails to have trace in $\mathrm{GF}(q)$.

The final stage is rewriting in $\mathrm{M}(n,q)$ the remaining groups $G \in \Psi(\mathcal{L})$ that are $\mathrm{GF}(q)$-monomial, a randomized process discussed after Corollary 2.21. A conjugate G^* of G in $\mathrm{GL}(n,q)$ is found by the algorithm of [14], and then the orbits of G^* on the lines of $\mathrm{GF}(q)^{(n)}$ are computed. If there is not a length n orbit o whose elements sum to $\mathrm{GF}(q)^{(n)}$ then G is deleted. Otherwise, o is used to rewrite G^* in $\mathrm{M}(n,q)$.

We remark that variations of the above algorithms may be viable for other degrees n, provided one has the necessary lists of irreducible linear groups of degrees dividing n, and also the necessary analogues of Theorems 2.17 and 4.1.

8. Isomorphism and Associated Primitive Permutation Groups

One may associate a primitive permutation group of finite degree to an irreducible linear group over a finite field, and vice versa. This classical equivalence goes back to Jordan and Galois, and is one of the original motivations for listing irreducible linear groups, especially soluble ones, over finite fields; cf. [25, Theorem 2.1.6] and [7, Sec. 4.7]. The topic of this section is isomorphism between linear groups and its relation to isomorphism between associated permutation groups under the equivalence. Our goal is to show how the automorphism groups of certain primitive permutation groups with abelian socle can be constructed from irreducible monomial linear groups. The determination of these automorphism groups is required in the specific context of [25, Theorem 1.1.1], for example.

Theorem 8.1. *Let G and H be groups acting on an additive abelian group V, and write the semidirect products $G \ltimes V$, $H \ltimes V$ with respect to these actions as GV, HV. A map $\alpha: GV \to HV$ is an isomorphism such that $\alpha(V) = V$ if and only if there exist*

(i) *an isomorphism $\beta: G \to H$,*
(ii) *a $\mathbb{Z}G$-isomorphism γ from V to V_β, where V_β has the same elements as V and G acts by $vg = v\beta(g)$,*
(iii) *a derivation $\delta: G \to V_\beta$,*

such that $\alpha(g,v) = (\beta(g), \gamma(v) + \delta(g))$ for all $g \in G$, $v \in V$.

Now we take V to be the n-dimensional vector space over some field $\mathbb{E}$.

Corollary 8.2. *Let G and H be irreducible subgroups of* $\mathrm{GL}(n,\mathbb{E})$, *acting naturally on V.*

(i) *If G and H are conjugate then $GV \cong HV$.*
(ii) *When $\mathbb{E} = \mathrm{GF}(p)$, $GV \cong HV$ if and only if G and H are conjugate.*

Proof. (i) Suppose $G^x = H$ for some $x \in \mathrm{GL}(n, \mathbb{E})$. Then in Theorem 8.1, set $\delta = 0$ and define β, γ by $\beta(g) = g^x$, $\gamma(v) = vx$.

(ii) We have $\mathrm{soc}(GV) = \mathrm{soc}(HV) = V$ (by [18, Theorem 1.16(d), p. 18], this much is true when $\mathbb{E}$ is any finite subfield of $\mathbb{F}_p$). Therefore, if $\alpha\colon GV \to HV$ is an isomorphism then $\alpha(V) = V$, so let β, γ be as in Theorem 8.1. Now γ acts as some $x \in \mathrm{GL}(n, p)$, and thus $\beta(g) = g^x$ because $\gamma(vg) = \gamma(v)\beta(g)$ for all $v \in V$. □

Let $\mathcal{L}$ be a complete and irredundant list of the irreducible subgroups of $\mathrm{GL}(n, p)$. If $G \in \mathcal{L}$ then the image of GV under the faithful permutation representation mapping (g, v) to the affine transformation of V defined by $u \mapsto ug + v$ is a primitive subgroup of $\mathrm{Sym}(V) \cong S_{p^n}$. Thus we may obtain a list $\mathcal{P}$ of primitive permutation groups of degree p^n with abelian socle directly from $\mathcal{L}$. By Corollary 8.2(ii), distinct elements of $\mathcal{P}$ are not isomorphic. In fact $\mathcal{P}$ is also complete with respect to permutational isomorphism, which is the other half of the equivalence mentioned at the beginning of this section. So Corollary 8.2(ii) says that two primitive subgroups of S_{p^n} with abelian socle are isomorphic if and only if they are conjugate in S_{p^n}.

Now we consider the problem of finding the automorphism group of each element of $\mathcal{P}$. Since V is regular, if $G \in \mathcal{L}$ then $\mathsf{N}_{S_{p^n}}(GV)$ is embedded in $\mathrm{GL}(n, p)V$ by [7, Corollary 4.2B, p. 110]. Since G is irreducible, GV has trivial centralizer in $\mathrm{GL}(n, p)V$. Thus $\mathsf{N}_{S_{p^n}}(GV) = \mathsf{N}_{\mathrm{GL}(n,p)V}(GV)$ is embedded in $\mathrm{Aut}(GV)$. We next give a criterion for these two groups to coincide. If this happens then $\mathrm{Aut}(GV)$ splits over V, with a complement that is conjugate to an element of $\mathcal{L}$.

Proposition 8.3. *Let G be an irreducible subgroup of $\mathrm{GL}(n, p)$. Then $\mathrm{Aut}(GV)$ is the group $\mathsf{N}_{\mathrm{GL}(n,p)}(G)V$, acting by conjugation, if and only if $H^1(G, V) = 0$.*

Proof. Let $\alpha \in \mathrm{Aut}(GV)$, with $\beta \in \mathrm{Aut}(G)$ induced from α as usual. Suppose $H^1(G, V) = 0$, so that $H^1(G, V_\beta) = 0$. By Theorem 8.1 and the proof of Corollary 8.2, for all $g \in G$ and $v \in V$ we have $\alpha(g, v) = (g^x, vx + \delta(g))$ for some $x \in \mathsf{N}_{\mathrm{GL}(n,p)}(G)$ and inner derivation $\delta\colon G \to V_\beta$; say $\delta(g) = u(1 - g^x)$, $u \in V$. Hence $\alpha(g, v) = (g, v)^{(x,u)}$. The other direction is equally easy. □

Remark 8.4. $\mathrm{Aut}(GV) = \mathsf{N}_{\mathrm{GL}(n,p)}(G)V$ if and only if $\mathrm{Out}(GV) \cong \mathsf{N}_{\mathrm{GL}(n,p)}(G)/G$. Thus Proposition 8.3 also follows from [24, (4.5)].

Corollary 8.5. *Let G be an irreducible subgroup of $\mathrm{GL}(n, p)$. If $\mathsf{O}_{p'}(G) \neq 1$ then $\mathrm{Aut}(GV) = \mathsf{N}_{\mathrm{GL}(n,p)}(G)V$.*

Proof. $H^1(G, V) = 0$ by [15, Theorem 1]. □

The hypothesis $\mathsf{O}_{p'}(G) \neq 1$ holds if G is soluble, and it obviously holds in our favorite situation $G \leq \mathrm{M}(n,p)$, $p > n$. So in the sequel we concentrate on normalizers of monomial linear groups.

Let us revert to general $\mathbb{E}$. Denote the normalizer in $\mathrm{GL}(n,\mathbb{E})$ of a subgroup G as $\mathsf{N}(G)$. When G is monomial, we show that in some circumstances $\mathsf{N}(G)$ is also monomial, so that if $\mathbb{E} = \mathrm{GF}(p)$ and G is irreducible, finding the automorphism group of the associated primitive permutation group GV boils down to finding the irreducible subgroup $\mathsf{N}(G) = \mathsf{N}_{\mathrm{M}(n,p)}(G)$ of $\mathrm{M}(n,p)$. If a list of such groups exists then we might try to recognize $\mathsf{N}(G)$ in the list. However, we cannot as yet offer a general recognition method. But when $\mathbb{E}$ is finite, knowing that $\mathsf{N}(G)$ is monomial is at least helpful computationally. For then the computation of $\mathsf{N}(G)$ can take place entirely in $\mathrm{M}(n,p)$, which has a smaller degree permutation representation than $\mathrm{GL}(n,p)$ does; even better, $\mathrm{M}(n,p)$ has a polycyclic presentation if $n \leq 4$ (cf. Sec. 7).

Below, $G \leq \mathrm{M}(n,\mathbb{E})$, $\mathrm{D}(n,\mathbb{E}) \cap G := A$, and α_i is the linear $\mathbb{E}$-representation of A that maps an element to its ith diagonal entry.

Lemma 8.6. *If the α_is are distinct on A then $\mathsf{N}(A) \leq \mathrm{M}(n,\mathbb{E})$.*

Proof. Cf. [11, proof of Proposition 1.3.7]. □

Proposition 8.7. *Suppose $\mathsf{C}_G(A) = A$ and πG has an abelian transitive subgroup T. Then $\mathsf{N}(A) \leq \mathrm{M}(n,\mathbb{E})$.*

Proof. Suppose at least two of the α_is are equal. Then T acts imprimitively on the set $\{\alpha_1,\ldots,\alpha_n\}$, where each block of imprimitivity consists of equal characters. Say the number of blocks is m, so $m < n$, and a factor of T is isomorphic to a regular subgroup of S_m. That factor is not T, because T is also regular in degree n. Hence some nontrivial subgroup of T acts trivially on $\{\alpha_1,\ldots,\alpha_n\}$, which contradicts $\mathsf{C}_G(A) = A$. The result follows from Lemma 8.6. □

Corollary 8.8. *Let n be prime. If A is nonscalar and πG is transitive then $\mathsf{N}(A) \leq \mathrm{M}(n,\mathbb{E})$.*

Proof. πG is a primitive permutation group. If $\mathsf{C}_G(A) \neq A$ then $\pi\mathsf{C}_G(A)$ is a nontrivial normal subgroup of πG, and as such is transitive. But then A is scalar. Since πG contains an n-cycle, we get the result by Proposition 8.7. □

Proposition 8.9. *Suppose G is irreducible, $\mathsf{C}_G(A) = A$, and $n = qr$, where q and r are primes. If*

(i) *$r = q$, or*
(ii) *$r > q$, and either r^2 divides $|\pi G|$, or q^2 divides $|\pi G|$ and $q > r/2$,*

then $\mathsf{N}(A) \leq \mathrm{M}(n,\mathbb{E})$.

Proof. Remember that πG is transitive, so n divides $|\pi G|$.

(i) By Clifford's Theorem, V_A has q homogeneous components all of dimension q, or q^2 components all of dimension 1. The permutation representation of πG arising from its action on the set of components has kernel that centralizes A, so is trivial. Then since q^2 divides $|\pi G|$, there must be q^2 components. The corresponding $\mathbb{E}$-characters α_i are pairwise distinct.

(ii) As in (i), it may be seen that V_A cannot have r homogeneous components of dimension q, nor vice versa. □

Theorem 8.10. *Let G be irreducible. In each of the following cases, $\mathsf{N}(G)$ is an irreducible subgroup of $\mathrm{M}(n, \mathbb{E})$.*

(i) *n is prime, A is nonscalar (so $\mathsf{Z}(G)$ is scalar), and either $|A : \mathsf{Z}(G)| \neq n$ or πG is insoluble.*
(ii) *$n = 4$, $\mathsf{C}_G(A) = A$, and A is characteristic in G.*
(iii) *$n = 6$, $\mathsf{C}_G(A) = A$, A is characteristic in G, and either* (a) *$\pi G \ncong S_3$, or* (b) *$\pi G \cong S_3$ and A is not centralized by any element of $\mathsf{C}_{S_6}(\pi G)$ (which is conjugate to πG).*
(iv) *$G = H$ wr S_n, where H is any subgroup of $\mathbb{E}^\times$ if $n > 2$, and any subgroup of $\mathbb{E}^\times$ that is not "special dihedral" if $n = 2$ (for finite $\mathbb{E}$, this means $|\mathbb{E}| \geq 4$).*

Proof. (i) Let $x \in \mathsf{N}(G)$. Since πA^x is a normal subgroup of πG, it is transitive. If πA^x is nontrivial then it is regular, and is therefore the unique Sylow n-subgroup of πG. An insoluble transitive permutation group of prime degree n has more than one Sylow n-subgroup (see [7, Exercise 3.5.1, p. 91]). So if πG is insoluble then $\pi A^x = 1$; that is, $x \in \mathsf{N}(A)$. This establishes part of the claim by Corollary 8.8.

If $\pi\mathsf{Z}(G)$ were nontrivial then it would be transitive on A, so A would be scalar. Thus $\mathsf{Z}(G) \leq A$. If $x \notin \mathsf{N}(A)$ then $A \cap A^x \leq \mathsf{Z}(G)$ and $|A : A \cap A^x| = n$, since πA^x is regular. Therefore $\mathsf{Z}(G) = A \cap A^x$.

(ii) Here $\mathsf{N}(G) \leq \mathsf{N}(A)$, and then Proposition 8.9(i) applies.

(iii) By [7, Table 2.1, p. 60], a transitive subgroup of S_6 is cyclic, or has order divisible by 4 or 9, or is isomorphic to S_3 (there is an error in the "Generators" column at line T6.2 of the table, which can be rectified by replacing the second stated generator with (153)(246)). Then (a) follows from Proposition 8.7 and Proposition 8.9(ii). Suppose $\pi G \cong S_3$, and $\{\alpha_1, \ldots, \alpha_6\}$ splits into three blocks of two equal characters each; say $s = (s_1 s_2)(s_3 s_4)(s_5 s_6) \in S_6 \backslash \pi G$ centralizes A. Since s^t centralizes A for all $t \in \pi G$, $\langle\, s,\, s^t \,\rangle$ is a transitive subgroup of S_6 if $s^t \neq s$ for some t. But then A is scalar. Thus $s \in \mathsf{C}_{S_6}(\pi G)$.

(iv) By [23, Theorem 9.12], the base group of G is a characteristic subgroup. Its normalizer is monomial by Lemma 8.6. □

Remark 8.11. In Theorem 8.10(ii), let $\mathbb{E} = \mathbb{F}_p$ and G be finite; then $\mathsf{C}_G(A) = A$ up to conjugacy except perhaps when $\pi G = S_4$ and A is scalar. If G is a p'-group then this is a consequence of [12, Theorem 4.2] and reasoning like that in the proof

of Theorem 2.17(iii). Still with G a p'-group, we comment on the other requirement in Theorem 8.10(ii), namely that A be a characteristic subgroup of G. This is a stronger hypothesis than is necessary, but it has the benefit of allowing us again to transfer from $\mathbb{E} = \mathbb{F}_p$ to $\mathbb{E} = \mathbb{C}$. If $\pi G \geq A_4$ and A is a characteristic subgroup of the inverse image $\pi^{-1}V_4$ of V_4 in G then A is characteristic in G, because $\pi^{-1}V_4$ is characteristic in G. Hence suppose first that $\pi G = V_4$. If A is not characteristic in G then A contains a normal subgroup N of G such that $\mathsf{O}_{2'}(A) \leq N$ and either $|\mathsf{O}_2(A) : \mathsf{O}_2(A) \cap N| = |\pi \mathsf{C}_G(N)| = 2$, or $|\mathsf{O}_2(A) : \mathsf{O}_2(A) \cap N| = 4$ and N is scalar. In both cases, if $\mathsf{O}_2(A)$ is noncyclic then $\mathsf{O}_2(A)$ has a nonscalar subgroup of index 2 centralized by an involution of V_4. The possible $\mathsf{O}_2(A)$ can then be identified (up to conjugacy) from [11, Example 3.1.11]. Similar deliberations are possible when $\pi G = C$ or D; see the discussion after [11, Lemma 4.5] and [11, Proposition 5.11].

Remark 8.12. $\mathrm{M}(n, \mathbb{E})$ is not normalized by $\mathrm{GL}(n, \mathbb{E})$, so Theorem 8.10(iv) for $H = \mathbb{E}^\times$ may also be deduced from the main theorem in [22].

Corollary 8.13. *If $p > n$ and $n > 2$, or $p \geq 5$ and $n = 2$, then* $\mathrm{Aut}(\mathrm{M}(n,p)V) = \mathrm{Inn}(\mathrm{M}(n,p)V) \cong \mathrm{M}(n,p)V$.

Remark 8.14. $|\mathrm{Out}(\mathrm{M}(2,3)V)| = 2$.

Let G be a nonabelian irreducible but not absolutely irreducible subgroup of $\mathrm{M}(r^2, q)$, r prime. If $\mathsf{N}_{\mathrm{GL}(r^2,q)}(G)$ is not absolutely irreducible then it is determined by $\mathsf{N}_{\mathrm{GL}(r,q^r)}(H)$ for some absolutely irreducible subgroup H of $\mathrm{GL}(r, q^r)$. Suppose, then, that n is prime, G is an absolutely irreducible subgroup of $\mathrm{M}(n, q)$, and $\mathbb{E} = \mathbb{F}_p$. Of course $\mathsf{N}_{\mathrm{GL}(n,q)}(G) = \mathsf{N}(G) \cap \mathrm{GL}(n, q)$. Assume πG is soluble, so that G has a normal subgroup Q containing A such that $|Q : A| = n$. If $|A : \mathsf{Z}(G)| \neq n$ then A and thus Q is characteristic in G; that is, $\mathsf{N}(G) \leq \mathsf{N}(Q)$. Hence the problem of finding $\mathsf{N}(G)$ for soluble G mostly reduces to the case $|\pi G| = n$. In [5, Sec. 6], $\mathsf{N}(G)$ is described for some n-groups G. We solve the easiest version of the more general problem, taking G to be a finite irreducible subgroup of $\mathrm{M}(2, \mathbb{F}_p)$, p odd.

By Theorem 5.1, let $G = HG_{2'}$, where H is $H(i, j, k)$ or $\langle\, a_1 \,\rangle$ and $G_{2'} = \mathsf{O}_{2'}(G)$. Either $G_{2'}$ is scalar, or $\mathsf{N}(G_{2'})$ and thus $\mathsf{N}(G)$ is monomial (apply Corollary 8.8 to $\langle\, a_1, G_{2'} \,\rangle$). In the former case $\mathsf{N}(G) = \mathsf{N}(H)$. In the latter, $\mathsf{N}(G) = \mathsf{M}(H)G_{2'}$, where $\mathsf{M}(H) := \mathsf{N}(H) \cap \mathrm{M}(2, \mathbb{E})$, by the Frattini argument. $\mathsf{M}(H)$ is stated in Theorem 8.15 below. By Theorem 8.10(i) and Theorem 5.1, it remains to find $\mathsf{N}(H)$ when $H = H(i, j, k)$, $1 \leq k \leq 2$ and $j = 1$. We do so next.

Let $x \in \mathsf{N}(H)$. If a_1^x is diagonal then $a_1^x = z_1^{\pm 1} w_1$, which implies $x = hm$ for some monomial matrix m and h the Hadamard matrix in the proof of Theorem 4.5. Recall that $a_1^h = z_1 w_1^{-1}$ and $w_1^h = a_1 z_1^{-1}$. If a_1^x is not diagonal then $a_1^{xw} = a_1$ for some $w \in \mathrm{SL}(2, \mathbb{F}_p) \cap \mathrm{D}(2, \mathbb{F}_p)$. Therefore xw is symmetric and has constant diagonal. Since w_1^{xw} is monomial, $(xw)_{11} = \pm(xw)_{12}\, \omega_1$ if xw is not monomial, and then xw is a scalar multiple of

$$g := \begin{pmatrix} \omega_1 & 1 \\ 1 & \omega_1 \end{pmatrix}$$

or g^{-1}. Note that $w_1^g = a_1 z_1 w_1$. Thus x is one of m, hm, or $g^{\pm 1}m$, for some $m \in \mathrm{M}(2, \mathbb{F}_p)$.

Let $H = H(i, 1, 1)$. We see that $H^h = H^g = H$ if $i \geq 1$. If $i = 0$ then H^h, H^g, and $H^{g^{-1}}$ (yet definitely not H) are $\mathrm{M}(2, \mathbb{F}_p)$-conjugate to $H(0, 0, 3)$, whence x must be monomial. We have proved that

$$\mathsf{N}(H) = \begin{cases} \mathsf{M}(H) & i = 0 \\ \langle\, \mathsf{M}(H),\, h,\, g \,\rangle & i \geq 1\,. \end{cases} \tag{I}$$

Let $H = H(i, 1, 2)$. If $i = 0$ then $H^h = H^g = H$. If $i \geq 1$ then H^h, H^g, $H^{g^{-1}}$ are $\mathrm{M}(2, \mathbb{F}_p)$-conjugate to $H(i, 0, 3)$. Therefore

$$\mathsf{N}(H) = \begin{cases} \langle\, \mathsf{M}(H),\, h,\, g \,\rangle & i = 0 \\ \mathsf{M}(H) & i \geq 1\,. \end{cases} \tag{II}$$

Theorem 8.15 (Cf. Theorem 8.10(i)).

(i) *Suppose* $G_{2'}$ *is nonscalar. Then* $\mathsf{N}(G) = \mathsf{M}(H)G_{2'}$, *where* $\mathsf{M}(H) = \langle\, a_1,\, Z \,\rangle$ *if* $H = \langle\, a_1 \,\rangle$ *and* $\mathsf{M}(H) = \langle\, a_1,\, w_{j+1},\, Z \,\rangle$ *if* $H = H(i, j, k)$, $i, j \geq 0$, *where* Z *is the group of all scalars in* $\mathrm{GL}(2, \mathbb{F}_p)$.

(ii) *Suppose* $G_{2'}$ *is scalar. Then* $H = H(i, j, k)$, $i \geq 0$, $j \geq 1$, *and* $\mathsf{N}(G) = \mathsf{M}(H)$ *as in* (i), *unless* $1 \leq k \leq 2$ *and* $j = 1$. $\mathsf{N}(G) = \mathsf{N}(H)$ *is given by* (I) *if* $k = 1$, $j = 1$, *and by* (II) *if* $k = 2$, $j = 1$.

Acknowledgments

I am very much indebted to Dr. B. Höfling, who carefully read drafts of this paper and suggested many improvements, and who discussed some computational issues with me. I am also grateful for the assistance of Professor E. A. O'Brien (particularly with the computing) and Dr L. G. Kovács.

This paper was written during a sabbatical year at the Centre for Mathematics and its Applications, Australian National University. I thank the CMA staff for their hospitality.

Appendix

The first set of errata, E.1, pertains to [11]. The construction in [12] relies on [11] and so we have to make corrections there that follow from E.1; this is done in parts (a) and (b) of the second set of errata, E.2. Part (c) of E.2 pertains solely to [12].

E.1. Amend the list in [11, Theorem 6.1.1] by adding $\langle\, ax_2u_2,\, c,\, C(1,1,1,0,1)\,\rangle$ and the groups

$$\left.\begin{array}{l}\langle\, ay_{j+1},\, bu_{j+1},\, F(i,j,j,j,0,0)\,\rangle\\ \langle\, a,\, b,\, F(i,j,0,0,1,1,2,1)\,\rangle\\ \langle\, a,\, b,\, F(i,j,0,0,1,1,2,-1)\,\rangle\end{array}\right\}\ i,j\geq 1 \qquad (\sharp)$$

and (also noted in [12, Sec. 6.1]) deleting the reducible groups

$$\begin{array}{ll}\langle\, ax_{i+1}^{\varepsilon}y_{j+1}^{\eta},\, bx_{i+1}^{\mu(1-\varepsilon)},\, F(i,j,0,0,0,1)\,\rangle & i,j\geq 1\\ \langle\, ax_{i+1}^{\varepsilon},\, b,\, F(i,j,0,0,1,1)\,\rangle & i,j\geq 1 \text{ or } i=j=0\,,\end{array}$$

ε,η,μ ranging freely over $\{0,1\}$.

E.2. Amend the lists $\mathcal{D}$ and $\mathcal{F}$ of [12] as follows.

(a) To $\mathcal{D}_1$ and $\mathcal{D}_2$ as defined before [12, Theorem 6.3.3] add the groups

$$\langle\, ax_2u_2,\, c,\, C(1,1,1,0,1)\,\rangle N\,.$$

(b) To $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_3$, and $\mathcal{F}_3'$ as defined around [12, Remark 6.1.3], add all groups G_2N, where G_2 is a group at $(\sharp)$.

(c) Further add to $\mathcal{F}$ all groups G_2N, where

for any finite nonscalar V_4-submodule N of $X_{2'}U_{2'}$, G_2 is one of

$$\begin{array}{ll}\langle\, ax_{i+1,2}^{\varepsilon}y_{j+1,2}^{\eta},\, bx_{i+1,2}^{\mu(1-\varepsilon)},\, F(i,j,0,0,0,1)\,\rangle & i,j\geq 1\\ \langle\, ax_{i+1,2}^{\varepsilon},\, b,\, F(i,j,0,0,1,1)\,\rangle & i=j=0 \text{ or } i,j\geq 1\\ \langle\, ax_{1,2}^{\varepsilon}y_{i+1,2}^{\eta},\, bx_{1,2}^{\mu(1-\varepsilon)},\, M(-1,i,-1,-1)\,\rangle & i\geq 2\\ \langle\, ax_{1,2}^{\varepsilon}y_{2,2},\, bx_{1,2}^{\mu(1-\varepsilon)},\, M(-1,1,-1,-1)\,\rangle & \\ \langle\, a,\, bx_{1,2},\, M(-1,1,-1,-1)\,\rangle & \\ \langle\, ax_{1,2}^{\varepsilon},\, b,\, M(1,i+1,-1,-1)\,\rangle & i\geq 1\,,\end{array}$$

and for any finite nonscalar V_4-submodule N of $X_{2'}V_{2'}$, G_2 is one of

$$\begin{array}{ll}\langle\, ax_{i+1,2}y_{j+1,2}^{\eta},\, b,\, F(i,j,0,0,0,1)\,\rangle & i,j\geq 1\\ \langle\, ax_{1,2}y_{i+1,2}^{\eta},\, b,\, M(-1,i,-1,-1)\,\rangle & i\geq 1\,,\end{array}$$

ε,η,μ ranging freely over $\{0,1\}$.

References

[1] J. L. Alperin and R. B. Bell, *Groups and Representations* (Springer-Verlag, 1995).
[2] Z. Bácskai, Finite irreducible monomial groups of small prime degree, Ph.D. thesis, Australian National University (1999).
[3] H. F. Blichfeldt, *Finite Collineation Groups* (University of Chicago Press, 1917).
[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24**(3–4) (1997) 235–265.

[5] S. B. Conlon, p-groups with an abelian maximal subgroup and cyclic center, *J. Austral. Math. Soc. Ser. A* **22**(2) (1976) 221–233.
[6] J. D. Dixon, *The Structure of Linear Groups* (Van Nostrand Reinhold, 1971).
[7] J. D. Dixon and B. Mortimer, *Permutation Groups* (Springer-Verlag, 1996).
[8] J. D. Dixon and A. E. Zalesskii, Finite primitive linear groups of prime degree, *J. London Math. Soc.* (2) **57**(1) (1998) 126–134.
[9] L. Dornhoff, *Group Representation Theory, Part B* (Marcel Dekker, 1972).
[10] W. Feit, The current situation in the theory of finite simple groups, in *Actes du Congrès International des Mathématiciens*, Nice, 1970, Tome 1 (Gauthier-Villars, 1971), pp. 55–93.
[11] D. L. Flannery, The finite irreducible linear 2-groups of degree 4, *Mem. Amer. Math. Soc.* **129**(613), American Mathematical Society, 1997.
[12] D. L. Flannery, The finite irreducible monomial linear groups of degree 4, *J. Algebra* **218**(2) (1999) 436–469.
[13] D. L. Flannery and E. A. O'Brien, Computing 2-cocycles for central extensions and relative difference sets, *Comm. Algebra* **28**(4) (2000) 1939–1955.
[14] S. P. Glasby and R. B. Howlett, Writing representations over minimal fields, *Comm. Algebra* **25**(6) (1997) 1703–1711.
[15] G. Higman, Complementation of abelian normal subgroups, *Publ. Math. Debrecen* **4** (1956) 455–458.
[16] B. Höfling, Finite irreducible imprimitive nonmonomial complex linear groups of degree 4, *J. Algebra* **236**(2) (2001) 419–470.
[17] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, 1967).
[18] B. Huppert and N. Blackburn, *Finite groups II* (Springer-Verlag, 1982).
[19] I. M. Isaacs, *Character Theory of Finite Groups* (Dover, 1994).
[20] A. S. Kondratiev, Finite linear groups of small degree, in *The Atlas of Finite Groups: Ten Years On*, London Math. Soc. Lecture Note Ser. **249** (Cambridge University Press, 1998), pp. 139–148.
[21] C. R. Leedham-Green and W. Plesken, Some remarks on Sylow subgroups of general linear groups, *Math. Z.* **191**(4) (1986) 529–535.
[22] S. Li, The maximality of monomial subgroups of linear groups over division rings, *J. Algebra* **127**(1) (1989) 22–39.
[23] P. M. Neumann, On the structure of standard wreath products of groups, *Math. Z.* **84** (1964) 343–373.
[24] D. J. Robinson, *Applications of cohomology to the theory of groups*, in *Groups—St Andrews 1981*, London Math. Soc. Lecture Note Ser. **71** (Cambridge University Press, 1982), pp. 46–80.
[25] M. W. Short, *The Primitive Soluble Permutation Groups of Degree Less than* 256, Lect. Notes in Math. **1519** (Springer-Verlag, 1992).
[26] Pham Huu Tiep and A. E. Zalesskii, Some aspects of finite linear groups: a survey, *J. Math. Sci.* (New York) **100**(1) (2000) 1893–1914.
[27] A. E. Zalesskii, *Linear Groups*, *Russian Math. Surveys* **36**(5) (1981) 63–128.