To appear in *International Journal of Algebra and Computation*

CLASSIFYING FINITE MONOMIAL LINEAR GROUPS OF PRIME DEGREE IN CHARACTERISTIC ZERO

Z. BÁCSKAI, D. L. FLANNERY, AND E. A. O'BRIEN

In memory of L. G. Kovács

ABSTRACT. Let p be a prime and let $\mathbb{C}$ be the complex field. We explicitly classify the finite solvable irreducible monomial subgroups of $\mathrm{GL}(p, \mathbb{C})$ up to conjugacy. That is, we give a complete and irredundant list of $\mathrm{GL}(p, \mathbb{C})$-conjugacy class representatives as generating sets of monomial matrices. Copious structural information about non-solvable finite irreducible monomial subgroups of $\mathrm{GL}(p, \mathbb{C})$ is also proved, enabling a classification of all such groups bar one family. We explain the obstacles in that exceptional case. For $p \leq 3$, we classify all finite irreducible subgroups of $\mathrm{GL}(p, \mathbb{C})$. Our classifications are available publicly in MAGMA.

1. INTRODUCTION

Classifying finite subgroups of $\mathrm{GL}(n, \mathbb{F})$ for various fields $\mathbb{F}$ and degrees n is an enduring problem in linear group theory. Early results are due to Jordan, Klein, Maschke, and Schur. Subsequently contributions were made by Dickson, Blichfeldt, Brauer, and Feit, to name just a few.

Special degrees ('small', prime, product of two primes) have received the most attention. We focus on prime degree p, which eases the workload somewhat. For example, an irreducible subgroup of $\mathrm{GL}(p, \mathbb{F})$ can be imprimitive in only one way (monomial). Furthermore, classifications for prime degrees may be needed to classify groups of composite degree.

The term *classify* has disparate meanings in linear group theory. By *classification*, we mean a list of groups of the declared kind in $\mathrm{GL}(n, \mathbb{F})$ that contains every group of that kind exactly once up to $\mathrm{GL}(n, \mathbb{F})$-conjugacy; also, each listed group is given explicitly, as a generating set of matrices.

D. A. Suprunenko classified several kinds of linear groups over finite and infinite fields. In [36, Theorem 6, p. 167] and [36, §22.1], the maximal irreducible solvable linear groups of prime degree over finite fields and algebraically closed fields are listed up to conjugacy. This was extended to other classical groups by Detinko [11,

---

2010 *Mathematics Subject Classification.* 20H20, 20E99, 20-04.

12]. Many more classifications of finite linear groups have been published, some of which are surveyed in [18, §8], [37], and [38, §§4.5–4.7].

For our classifications, we take $\mathbb{F}$ to be the complex field $\mathbb{C}$. The list of groups in each degree is thus infinite. By contrast, the number of conjugacy classes of finite primitive subgroups of $\mathrm{SL}(n, \mathbb{C})$ is finite (hence the popularity of these restrictions in the literature). Each group in our lists has a unique label: an integer parameter string that specifies the non-zero entries of matrix generators.

In [8, 9] Conlon classified the non-abelian finite p-subgroups of classical groups of degree p over a field of characteristic not p. These papers set a benchmark of thoroughness, demonstrating that imprimitive groups in the full general linear group could be handled without too much difficulty.

L. G. Kovács initiated and guided a research program aimed at classifying finite linear groups to the standard of [8, 9]. Work within this program includes that by Bácskai [1], Flannery [20], Höfling [25], Short [34], and Sim [35]. Our paper is a development of [1]. We emphasize again the scale of all these classifications: they are complete and irredundant up to conjugacy in the relevant $\mathrm{GL}(n, \mathbb{F})$, with representatives given as generating sets of matrices.

One motivation for the Kovács program has origins in computational group theory. A certain maximal subgroups algorithm proposed by Kovács, Neubüser, and Newman requires lists of irreducible linear groups over finite fields, based on an equivalence with primitive permutation groups (see [34, pp. 2–4], and [10, 17] for later progress in this direction). Classifications of finite linear groups over $\mathbb{C}$ also serve as a resource for classifying linear groups over finite fields (see the use of [21] in [22]).

A comparable classification, of finite non-solvable irreducible monomial subgroups of $\mathrm{SL}(p, \mathbb{C})$, was achieved by Dixon and Zalesskii [16]. While our work inevitably has overlaps with [16], there are significant differences. First, a classification up to conjugacy in $\mathrm{GL}(p, \mathbb{C})$ is remote from an analogous classification in $\mathrm{SL}(p, \mathbb{C})$; the restriction to $\mathrm{SL}(p, \mathbb{C})$ affords various simplifications that are not applicable in the full general linear group. Moreover, we have completely classified the solvable finite irreducible monomial subgroups of $\mathrm{GL}(p, \mathbb{C})$ for all p—a notable accomplishment in its own right. The non-solvable case lacks a complete solution for arbitrary p, as we explain in Section 10.

Classifications such as the ones in this paper are dense with intricacies that may increase the likelihood of error. To address this issue, we have made the classifications publicly available as part of the computer algebra system MAGMA [6]; they can be incorporated into other systems. Output is a list of groups over an algebraic number field prescribed by an input bound on group order. Measures to verify correctness are discussed in Section 12.

Initially we deal with solvable monomial subgroups of $\mathrm{GL}(p, \mathbb{C})$. The treatment is then widened to non-solvable groups, culminating in a classification of the finite irreducible monomial subgroups of $\mathrm{GL}(p, \mathbb{C})$ for $p \leq 11$. Additionally, for $p \leq 3$, we classify all finite irreducible subgroups of $\mathrm{GL}(p, \mathbb{C})$. To classify finite non-solvable primitive subgroups of $\mathrm{GL}(p, \mathbb{C})$ for $p > 3$, one might utilize the description in [15] of the finite primitive subgroups of $\mathrm{SL}(p, \mathbb{C})$ up to isomorphism.

As noted above, our development of the classification and its exposition follow [1]. Recently, the second and third authors revisited the topic, with a long-held aim of making these results accessible to the wider research community. We discovered errors in [1] which impact on the correctness of that work. Consequently, we prepared a new self-contained account that resolves these errors, and, for the first time, provides the classification in a format suitable for further computation.

2. Preliminaries

Unless stated otherwise, $\mathbb{F}$ denotes an arbitrary field. The group $\mathrm{M}(n, \mathbb{F})$ of all monomial matrices in $\mathrm{GL}(n, \mathbb{F})$ splits over the subgroup $\mathrm{D}(n, \mathbb{F})$ of diagonal matrices: $\mathrm{M}(n, \mathbb{F}) = \mathrm{D}(n, \mathbb{F}) \rtimes \mathrm{P}(n)$, where $\mathrm{P}(n)$ is the group of permutation matrices. We identify $\mathrm{P}(n)$ with $\mathrm{Sym}(n)$; say, under the isomorphism that maps $\alpha \in \mathrm{Sym}(n)$ to $[\delta_{i\alpha,j}]_{i,j} \in \mathrm{P}(n)$ where δ is the Kronecker delta. Each $G \leq \mathrm{M}(n, \mathbb{F})$ is an extension of its *diagonal subgroup* $G \cap \mathrm{D}(n, \mathbb{F})$ by its *permutation part* $\mathrm{D}(n, \mathbb{F})G \cap \mathrm{P}(n)$.

Definition 2.1. Let ϕ be the natural surjection $\mathrm{M}(n, \mathbb{F}) \to \mathrm{Sym}(n)$ defined by $\phi \colon dt \mapsto t$ for $d \in \mathrm{D}(n, \mathbb{F})$ and $t \in \mathrm{P}(n)$.

Note that G has permutation part $\phi(G)$. We speak of the diagonal subgroup $G \cap \ker \phi$ as a $\phi(G)$-*module*; $x \in \mathrm{M}(n, \mathbb{F})$ acts by conjugation on $\mathrm{D}(n, \mathbb{F})$ as $\phi(x)$ does, permuting diagonal entries as $\phi(x)$ permutes $\{1, \ldots, n\}$.

Lemma 2.2. *If $G \leq \mathrm{M}(n, \mathbb{F})$ is irreducible then $\phi(G)$ is transitive.*

So we must first solve a classification problem for permutation groups: classify the transitive groups of prime degree.

Notation 2.3. $\widetilde{\mathrm{M}}(n, \mathbb{F})$ denotes the group of all $n \times n$ monomial matrices over the roots of unity in $\mathbb{F}$.

Lemma 2.4. *If $G \leq \mathrm{M}(n, \mathbb{F})$ is finite and $\phi(G)$ is transitive then G is $\mathrm{M}(n, \mathbb{F})$-conjugate to a subgroup of $\widetilde{\mathrm{M}}(n, \mathbb{F})$.*

Proof. Let $e_k \in \mathbb{F}^n$ be the vector with 1 in position k and 0s elsewhere. The orbit Ge_1 contains a basis $\{b_1, \dots, b_n\}$ of $\mathbb{F}^n$. For each $g \in G$ and i, we have $gb_i = \lambda b_j$ for some j and $\lambda \in \mathbb{F}^{\times}$. Since $\lambda e_1 \in Ge_1$, the scalar λ has finite order. Thus, if $b \in \mathrm{M}(n, \mathbb{F})$ is the matrix with kth column b_k, then $G^b \leq \widetilde{\mathrm{M}}(n, \mathbb{F})$. □

In view of Lemma 2.4, we classify subgroups of $\widetilde{\mathrm{M}}(p, \mathbb{C})$. That is, listed groups will be given by generating sets of monomial matrices, and the non-zero entries of each generator are roots of unity.

The key steps in our approach are as follows.

(1) Classify the transitive $T \leq \mathrm{Sym}(p)$ up to conjugacy.
(2) For each permutation part T, list the candidate diagonal subgroups A, i.e., the finite T-submodules A of $\mathrm{D}(p, \mathbb{F})$.
(3) For pairs (T, A) drawn from (1) and (2), solve the extension problem in $\mathrm{M}(p, \mathbb{F})$ up to $\mathrm{GL}(p, \mathbb{F})$-conjugacy, ensuring that each retained extension of A by T is irreducible.
(4) Eliminate $\mathrm{GL}(p, \mathbb{F})$-conjugacy among all subgroups of $\mathrm{M}(p, \mathbb{F})$ found in (3).

These steps are carried out in Section 2.1; Section 3; Sections 2.3 and 4–9; and Sections 2.2 and 4–9, respectively.

The final lists are complete (every finite irreducible monomial subgroup of $\mathrm{GL}(p, \mathbb{F})$ is represented) and irredundant (no $\mathrm{GL}(p, \mathbb{F})$-conjugacy class is represented more than once). We justify completeness by proving that step (4) does not remove any conjugacy class. Most of the taxonomic complication arises in step (2), especially when T is solvable.

2.1. **Transitive subgroups of** $\mathrm{Sym}(p)$.

Permutation groups of prime degree have been studied from the time of Galois. We recap some of the essential theory.

A transitive group $T \leq \mathrm{Sym}(p)$ has a unique simple normal transitive subgroup U. The quotient $N_{\mathrm{Sym}(p)}(U)/U$ is cyclic of order dividing $p - 1$. Thus T is solvable if and only if U is solvable, i.e., $|U| = p$.

Notation 2.5. Throughout, $s = (1, 2, \dots, p) \in \mathrm{Sym}(p)$. Let $t \in \mathrm{Sym}(p)$ be defined by $i \mapsto iu \bmod p$ where u is the least primitive element modulo p in $\{1, \dots, p-1\}$. So $|s| = p$, $|t| = p - 1$, and $s^t = s^u$.

Since T contains a conjugate of s in $\mathrm{Sym}(p)$, we assume that $s \in T$ henceforth.

Lemma 2.6. *If T is solvable then $T \leq N_{\mathrm{Sym}(p)}(\langle s \rangle) = \langle s, t \rangle \cong C_p \rtimes C_{p-1}$.*

A solvable irreducible monomial subgroup of $\mathrm{GL}(p, \mathbb{F})$ is therefore conjugate to a subgroup of $\mathrm{M}(p, \mathbb{F})$ with permutation part $\langle s, t^a \rangle$ where $a \mid (p-1)$. On the other hand, $\langle s \rangle$ is not normal in non-solvable T.

Proposition 2.7. *A non-trivial normal subgroup of T is transitive. Hence the Fitting subgroup $\mathrm{Fit}(T)$ is non-trivial if and only if T is solvable, in which case $|\mathrm{Fit}(T)| = p$.*

Table 1 (extracted from [30, Table 1]; see also [16, § 1.1]) displays facts about all non-solvable U.

U	$N_{\mathrm{Sym}(p)}(U)$	Degree	# rep.s
$\mathrm{Alt}(p)$	$\mathrm{Sym}(p)$	$p \geq 7$	1
$\mathrm{SL}(d, q)$	$\Sigma\mathrm{L}(d, q)$	$p = \frac{q^d-1}{q-1}$	$1\,(d=2)$ $2\,(d \geq 3)$
M_p	M_p	$p = 11, 23$	1
$\mathrm{PSL}(2, 11)$	$\mathrm{PSL}(2, 11)$	$p = 11$	2

TABLE 1. Non-abelian simple transitive permutation groups of degree p

The fourth column states the number of inequivalent faithful representations of U in $\mathrm{Sym}(p)$; M_{11} and M_{23} are Mathieu groups; d is prime and $\gcd(d, q-1) = 1$, so $\mathrm{SL}(d, q) \cong \mathrm{PSL}(d, q)$. The normalizer $\Sigma\mathrm{L}(d, q)$ is $\mathrm{SL}(d, q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ where $\mathbb{F}_q$ denotes the field of size q. Of course, $\mathrm{Alt}(5)$ appears as U twice.

Observe that $\mathrm{Sym}(p)$ always has transitive subgroups of the following kinds: the solvable ones, $\mathrm{Alt}(p)$, and $\mathrm{Sym}(p)$; these we call *compulsory*. All but three non-compulsory transitive permutation groups of degree p belong to the 'projective' family (i.e., with U as in row 2 of Table 1). Bateman and Stemmler [2, Theorem 4] show that for large n there are at most $50\sqrt{n}/(\log n)^2$ primes of this form not exceeding n. So there are infinitely many 'non-projective' primes.

The next fact does not seem to be widely known.

Theorem 2.8. *Transitive subgroups of $\mathrm{Sym}(p)$ are conjugate if and only if they are isomorphic.*

Proof. If U is C_p, $\mathrm{Alt}(p)$, $\mathrm{SL}(2, q)$, or M_p, then there is only one faithful permutation representation of U of degree p up to equivalence, and hence a single conjugacy class of groups in $\mathrm{Sym}(p)$ isomorphic to U.

Suppose that $U \cong \mathrm{PSL}(2, 11)$ and θ is a transitive embedding of U in $\mathrm{Sym}(p)$ inequivalent to id_U. If $\alpha \in \mathrm{Aut}(U)$ and $\theta\alpha(u)^a = \theta(u)$ for some $a \in \mathrm{Sym}(p)$ and all

$u \in U$, then $a \in \theta(U)$ because $\theta(U)$ is self-normalizing. Since $\mathrm{Out}(U) \neq 1$, there will be an α such that id_U and $\theta\alpha$ are equivalent; whence U is conjugate to $\theta(U)$.

If $U \cong \mathrm{SL}(d,q)$ for $d \geq 3$ then the graph (inverse transpose) automorphism of U swaps the two inequivalent transitive representations of U in $\mathrm{Sym}(p)$ [30, p. 523].

Now let S and $\hat{S}$ be isomorphic transitive subgroups of $\mathrm{Sym}(p)$, with simple normal transitive subgroups U, $\hat{U}$ respectively. By the above, $U^w = \hat{U}$ for some $w \in \mathrm{Sym}(p)$. Thus S^w normalizes $\hat{U}$. Since $N_{\mathrm{Sym}(p)}(\hat{U})/\hat{U}$ is cyclic, $S^w = \hat{S}$. □

2.2. **Conjugacy.** Already we witness a division of the classification into mutually disjoint families: groups with permutation parts that are not conjugate in $\mathrm{Sym}(p)$ are not $\mathrm{M}(p,\mathbb{F})$-conjugate. Such groups cannot even be isomorphic.

Theorem 2.9. *Suppose that $G, H \leq \mathrm{M}(p,\mathbb{F})$ are isomorphic, with $\phi(G)$ and $\phi(H)$ transitive. Then $\phi(G)$ and $\phi(H)$ are $\mathrm{Sym}(p)$-conjugate. If G is non-solvable, then $\mathrm{D}(p,\mathbb{F}) \cap G$ maps onto $\mathrm{D}(p,\mathbb{F}) \cap H$ under any isomorphism $G \to H$.*

Proof. The theorem follows (with a little effort) from Lemma 2.6, Proposition 2.7, and Theorem 2.8. □

Theorem 2.9 is vital in our solution of the conjugacy problem: groups with different permutation parts are not conjugate, and conjugacy that does not respect diagonal subgroups can only occur between (irreducible) solvable groups.

Theorem 2.10. *Let G be an irreducible subgroup of $\widetilde{\mathrm{M}}(p,\mathbb{F})$ with non-scalar diagonal subgroup A. Suppose that $G^w \leq \widetilde{\mathrm{M}}(p,\mathbb{F})$ and $A^w \leq \mathrm{D}(p,\mathbb{F})$ for some $w \in \mathrm{GL}(p,\mathbb{F})$. Then w is monomial; furthermore, $w \in \widetilde{\mathrm{M}}(p,\mathbb{F})$ up to scalars if $\mathbb{F}$ is algebraically closed.*

Proof. By Clifford's Theorem, the A-submodules of $\mathbb{F}^n$ are exactly the 1-dimensional subspaces $\mathbb{F}e_i$. Then $we_i \in \mathbb{F}e_j$ for some j, because $A^w e_i \subseteq \mathbb{F}e_i$. Hence w is monomial. We may assume that w is diagonal. Fix $g \in G$; the map defined by $b \mapsto [b,g]$ is an endomorphism of $\mathrm{D}(p,\mathbb{F})$. Since $[w,g] \in \widetilde{\mathrm{M}}(p,\mathbb{F})$, we have $[w^n,g] = [w,g]^n = 1$ for some n and all g. By Schur's Lemma, w^n is scalar. Taking nth roots, we see that a scalar multiple of w has finite order. □

In other words, $\mathrm{GL}(p,\mathbb{C})$-conjugacy that respects (non-scalar) diagonal subgroups is effected by a monomial matrix. So our priority is to sort out the conjugacy classes of $\widetilde{\mathrm{M}}(p,\mathbb{C})$. Moreover, Theorems 2.9 and 2.10 are frequently used to show that $\mathrm{GL}(p,\mathbb{C})$-conjugacy among non-solvable groups is the same as $\widetilde{\mathrm{M}}(p,\mathbb{C})$-conjugacy.

Remark 2.11. The *isomorphism question* for a set $\mathcal{S}$ of subgroups of $\mathrm{GL}(n,\mathbb{F})$ asks: if G, $H \in \mathcal{S}$ are (abstractly) isomorphic, are G and H linearly isomorphic ($\mathrm{GL}(n,\mathbb{F})$-conjugate)? The answer is "yes" for non-abelian finite p-subgroups of $\mathrm{GL}(p,\mathbb{C})$ by [8, Proposition 4.2], but "no" more generally for finite irreducible subgroups of $\mathrm{M}(p,\mathbb{C})$. Cf. Theorem 2.8. Corollary 11.2 gives another answer to the isomorphism question.

2.3. **Irreducibility.** We prove the next theorem using Ito's result that the irreducible ordinary character degrees of a finite group divide the index of each abelian normal subgroup.

Theorem 2.12. *Let G be a finite subgroup of $\mathrm{M}(p,\mathbb{C})$ such that $\phi(G)$ is transitive. If $\mathrm{D}(p,\mathbb{C}) \cap G$ is non-scalar, then G is irreducible. Conversely, if G is solvable irreducible, then $\mathrm{D}(p,\mathbb{C}) \cap G$ is non-scalar.*

Corollary 2.13. *If G is a finite irreducible subgroup of $\mathrm{M}(p,\mathbb{C})$ then $\mathrm{D}(p,\mathbb{C}) \cap G$ is a maximal abelian normal subgroup of G.*

Remark 2.14. Let $G = A \rtimes T$ for scalar $A \leq \mathrm{D}(n,\mathbb{F})$ and $T \leq \mathrm{Sym}(n)$. Then G fixes the all 1s vector, so is reducible.

Remark 2.15. The general converse of the first claim in Theorem 2.12 is false: $\mathrm{M}(5,\mathbb{C})$ has irreducible subgroups isomorphic to $\mathrm{Alt}(5)$.

3. Diagonal subgroups

Let $T \leq \mathrm{Sym}(p)$. A finite T-submodule of $\mathrm{D}(p,\mathbb{C})$ is the direct product of its Sylow p-subgroup and its Hall p'-subgroup, which are also T-modules. The submodule listing problem bifurcates accordingly.

3.1. $\langle s\rangle$-modules.

3.1.1. *The modules of p-power order.* Our paradigm for listing the $\langle s\rangle$-submodules of $\mathrm{D}(p,\mathbb{C})$ of p-power order is [8, § 1].

Note that $\mathrm{D}(p,\mathbb{C})$ is a central product XZ amalgamating the scalar subgroup of order p, where Z is the group of all scalars and $X = \mathrm{SL}(p,\mathbb{C}) \cap \mathrm{D}(p,\mathbb{C})$. We define endomorphisms γ and χ of $\mathrm{D}(p,\mathbb{C})$ by

$$\gamma(d) = d^{1-s}, \qquad \chi(d) = d^{1+s+\cdots+s^{p-1}}.$$

Then $Z = \chi(Z) = \chi(\mathrm{D}(p,\mathbb{C})) = \ker\,\gamma$ and $X = \gamma(X) = \gamma(\mathrm{D}(p,\mathbb{C})) = \ker\,\chi$. For $\mathrm{i} = \sqrt{-1}$, let

$$b_m = \mathrm{diag}(e^{2\pi \mathrm{i}/m}, e^{-2\pi \mathrm{i}/m}, 1, \ldots, 1), \qquad z_m = \mathrm{diag}(e^{2\pi \mathrm{i}/m}, \ldots, e^{2\pi \mathrm{i}/m}).$$

Lemma 3.1. *Z has a unique $\langle s\rangle$-submodule of each order m, namely $Z_m = \langle z_m\rangle$.*

Notation 3.2. Let D be the torsion subgroup of $\mathrm{D}(p, \mathbb{C})$. If π is a set of primes, then A_π denotes the Hall π-subgroup of $A \leq D$. So we write $A_{\{q\}}$ for the Sylow q-subgroup of A if π has a single prime q. The complement of A_π in A is denoted $A_{\pi'}$.

Remark 3.3. The scalar subgroup $Z_p = X \cap Z$ of order p lies in every non-identity $\langle s\rangle$-submodule of $D_{\{p\}}$.

Next we determine the finite $\langle s\rangle$-submodules of $X_{\{p\}}$.

Definition 3.4. For a positive integer j, let n, m be the non-negative integers such that $m < p-1$ and $j = n(p-1) - m$. Define

$$X_{p^j} = X \cap (\ker \gamma^j), \qquad x_{p^j} = \gamma^m(b_{p^n}).$$

Remark 3.5. $z_{p^{j+1}}^p = z_{p^j}$ and $x_{p^{j+p-1}}^p = x_{p^j}$.

Notation 3.6. If A is an abelian q-group, then $\Omega_k A := \{a \in A \mid a^{q^k} = 1\}$, i.e., the largest subgroup of exponent at most q^k.

Lemma 3.7. *$X_{\{p\}}$ is a uniserial $\langle s\rangle$-module; it has a unique submodule at every order p^j, namely X_{p^j}, generated as an $\langle s\rangle$-module by x_{p^j}.*

Proof. Suppose that $|X_{p^j}| = p^j$ for $j \geq 1$. The $\langle s\rangle$-epimorphism $\gamma\colon X_{p^{j+1}} \to X_{p^j}$ has kernel X_p. Thus $|X_{p^{j+1}}| = p|X_{p^j}| = p^{j+1}$, proving that $|X_{p^j}| = p^j$ for all j by induction.

Let $B \leq X_{\{p\}}$ be a non-identity $\langle s\rangle$-submodule. So B/X_p is an $\langle s\rangle$-submodule of $X_{\{p\}}/X_p \cong X_{\{p\}}$. If $B \neq X_p$ then we replace B by B/X_p in $X_{\{p\}}/X_p$ and repeat. The recursion eventually terminates, at which point $B = X_{p^j}$ for some j.

The $\langle s\rangle$-module generated by b_{p^n} is $\Omega_n X_{\{p\}} = X_{p^{n(p-1)}}$. Hence $\gamma^m(b_{p^n})$ generates $\gamma^m(X_{p^{n(p-1)}}) = X_{p^{n(p-1)-m}}$. □

We obtain all finite $\langle s\rangle$-submodules of the Sylow p-subgroup

$$D_{\{p\}}/Z_p = X_{\{p\}}/Z_p \times Z_{\{p\}}/Z_p$$

of $\mathrm{D}(p, \mathbb{C})/Z_p$ from Lemmas 3.1 and 3.7 and the following well-known theorem (for a proof, see [33, 1.6.1, p. 35]).

Theorem 3.8 (Goursat–Remak). *Let U and V be R-modules for an associative unital ring R. If θ is an R-isomorphism of a section U_1/U_2 of U onto a section V_1/V_2 of V, then*

$$W_\theta = \{uv \mid u \in U_1,\, v \in V_1,\, \theta(uU_2) = vV_2\}$$

is an R-submodule of $U \times V$ such that

$$U_2 = W_\theta \cap U, \quad V_2 = W_\theta \cap V, \quad U_1 = U \cap W_\theta V, \quad V_1 = UW_\theta \cap V,$$

and $W_\theta/U_2V_2 \cong U_1/U_2 \cong V_1/V_2$.

Conversely, let W be an R-submodule of $U \times V$. Put

$$U_2 = W \cap U, \quad V_2 = W \cap V, \quad U_1 = U \cap WV, \quad V_1 = UW \cap V,$$

and define $\alpha\colon U_1/U_2 \to V_1/V_2$ by $\alpha(uU_2) = vV_2$ where v is any element of $uW \cap V$. Then α is an R-isomorphism such that $W = W_\alpha$.

That is, apart from 'Cartesian' submodules $X_{p^j}Z_{p^k}$, the $\langle s\rangle$-submodules of $D_{\{p\}}$ are in one-to-one correspondence with the $\langle s\rangle$-isomorphisms between non-identity sections of $X_{\{p\}}/Z_p$ and $Z_{\{p\}}/Z_p$.

Definition 3.9. For $k \geq 0$, let $Y_{0,k,0} = Z_{p^k}$. For $j, k \geq 1$ and $l \geq 0$, let

$$Y_{j,k,l} = \langle x_{p^{j+1}} z^l_{p^{k+1}}, X_{p^j}, Z_{p^k}\rangle.$$

Define $\mathcal{Y}$ to be the set of all $Y_{j,k,l}$ where $0 \leq l \leq p-1$ and either $j = l = 0$ and $k \geq 0$, or j, $k \geq 1$.

Theorem 3.10 (cf. [8, 1.8])**.** *$\mathcal{Y}$ is the set of all finite $\langle s\rangle$-submodules of $D_{\{p\}}$.*

Proof. As forecast, this is an application of Theorem 3.8, relying on Lemmas 3.1 and 3.7. □

Remark 3.11.

(i) If $(j, k, l) \neq (0, 0, 0)$ then $Y_{j,k,l}$ is generated as an $\langle s\rangle$-module by $x_{p^{j+1}} z^l_{p^{k+1}}$ and z_{p^k}.
(ii) $|Y_{j,k,l}| = p^{j+k}$.
(iii) Each element of $\mathcal{Y}$ is labeled by a unique triple: $Y_{j,k,l} = Y_{a,b,c} \Rightarrow (j, k, l) = (a, b, c)$.

3.1.2. *The modules of order coprime to p.* Let q be a prime, $q \neq p$. Clearly

$$D_{\{q\}} = X_{\{q\}} \times Z_{\{q\}}.$$

As we will see, $X_{\{q\}}$ is a direct product of uniserial $\langle s\rangle$-submodules with no isomorphism between non-identity sections of the factors, and $\langle s\rangle$ acts non-trivially on every non-identity section of $X_{\{q\}}$. Hence, by the Goursat–Remak Theorem, all $\langle s\rangle$-submodules of $\mathrm{D}(p, \mathbb{C})$ of q-power order are Cartesian.

We gave a 'closed' (submodule or subgroup) generating set of each finite $\langle s\rangle$-submodule of $D_{\{p\}}$. It is infeasible to do the same for submodules of $D_{\{q\}}$. A new feature is calculation with polynomials over the q-adic integers $\mathbb{Z}_q$ (the endomorphism ring of the quasicyclic q-group C_{q^∞}, which acts on $D_{\{q\}} \cong (C_{q^\infty})^p$ by extension of the $\mathbb{Z}$-action). The complexity of these calculations varies with q and p. We undertake these calculations without imposing the 'height' restriction of [16, p. 366].

Notation 3.12. Denote reduction modulo q by overlining. So $\overline{\mathbb{Z}} = \overline{\mathbb{Z}_q} = \mathbb{F}_q$, and a polynomial $f \in \mathbb{Z}_q[\mathrm{x}]$ or $\mathbb{Z}[\mathrm{x}]$ maps to $\overline{f} \in \mathbb{F}_q[\mathrm{x}]$.

We need the following version of Hensel's Lemma. Its proof contains an algorithm that we use to construct generators for submodules of $X_{\{q\}}$ (cf. [19, Lemma 12.8, p. 40]).

Lemma 3.13. *Suppose that $f \in \mathbb{Z}_q[\mathrm{x}]$ is monic and $\overline{f} \in \mathbb{F}_q[\mathrm{x}]$ factorizes into the product of coprime monic polynomials g_0, $h_0 \in \mathbb{F}_q[\mathrm{x}]$. Then there exist monic g, $h \in \mathbb{Z}_q[\mathrm{x}]$ such that $\bar{g} = g_0$, $\bar{h} = h_0$, and $f = gh$.*

Proof. We call an integer polynomial *flat* if its coefficients lie in $\{0, 1, \ldots, q-1\}$. Each polynomial in $\mathbb{Z}_q[\mathrm{x}]$ is congruent modulo q to a unique flat polynomial.

We have $a_0 g_0 + b_0 h_0 = 1$ for some a_0, $b_0 \in \mathbb{F}_q[\mathrm{x}]$. Let a, b, g_1, $h_1 \in \mathbb{Z}[\mathrm{x}]$ be the flat preimages of a_0, b_0, g_0, h_0, respectively, modulo q. Assume inductively that $n \geq 1$ and $\overline{g_n} = g_0$, $\overline{h_n} = h_0$ for some g_n, $h_n \in \mathbb{Z}[\mathrm{x}]$ such that $f = g_n h_n + q^n c_n$ where $c_n \in \mathbb{Z}_q[\mathrm{x}]$. Then $\deg c_n < \deg f$. Also, $a g_n + b h_n \equiv 1 \bmod q$.

By division in $\mathbb{F}_q[\mathrm{x}]$ and lifting, we get unique flat v_n, w_n such that $bc_n \equiv w_n g_n + v_n \bmod q$ and $\deg v_n < \deg g_n$. Let $u_n = ac_n + w_n h_n$, and let u_n' be the unique flat polynomial congruent to u_n modulo q. Then

$$v_n h_n + u_n g_n = bc_n h_n + ac_n g_n \equiv c_n \bmod q,$$

so $u_n' g_n \equiv c_n - v_n h_n \bmod q$. Since $\deg c_n < \deg f$ and $\deg v_n < \deg g_n$, it follows that $\deg u_n' < \deg h_n$.

Define $g_{n+1} = g_n + q^n v_n$ and $h_{n+1} = h_n + q^n u_n'$. These polynomials are monic, and

$$\begin{aligned} g_{n+1} h_{n+1} &\equiv g_n h_n + q^n (u_n' g_n + v_n h_n) \\ &\equiv g_n h_n + q^n c_n \\ &\equiv f \bmod q^{n+1}. \end{aligned}$$

Hence, by induction, for each positive integer n there exist g_n, $h_n \in \mathbb{Z}[\mathrm{x}]$ such that $g_{n+1} \equiv g_n$, $h_{n+1} \equiv h_n$, and $f \equiv g_n h_n \bmod q^n$. So the polynomial sequences $\{g_n\}_{n\geq 1}$, $\{h_n\}_{n\geq 1}$ converge in the q-adic sense to monic g, $h \in \mathbb{Z}_q[\mathrm{x}]$ such that $f = gh$. $\square$

Corollary 3.14. *Suppose that $f \in \mathbb{Z}_q[\mathrm{x}]$ is monic and $\overline{f}$ has no repeated roots (in any extension of $\mathbb{F}_q$). Then f is $\mathbb{Z}_q$-irreducible if and only if $\overline{f}$ is $\mathbb{F}_q$-irreducible.*

Proof. Since $\overline{f}$ has no repeated roots, it is coprime to its formal derivative. Thus $\overline{f}$ can only properly factorize into a product of coprime polynomials, which contradicts Lemma 3.13 if f is irreducible.

For the converse, let $f_i \in \mathbb{Z}_q[\mathrm{x}]$ be the irreducible monic factors of f in $\mathbb{Z}_q[\mathrm{x}]$. Each $\overline{f_i}$ is monic and has no repeated roots. The previous paragraph implies that the $\overline{f_i}$ are $\mathbb{F}_q$-irreducible. □

Notation 3.15. $v := \frac{p-1}{d}$ where d is the multiplicative order of q modulo p.

Definition 3.16. From now on, $f = f(\mathrm{x}) := 1 + \mathrm{x} + \cdots + \mathrm{x}^{p-1} \in \mathbb{Z}_q[\mathrm{x}]$. Let g_1 be an irreducible monic factor of $\bar{f}$. For $1 \leq r \leq v-1$, define $g_{r+1}(\mathrm{x}) = \gcd(g_r(\mathrm{x}^u), \bar{f}(\mathrm{x}))$ where u is the least primitive element modulo p (see Notation 2.5).

Remark 3.17. We can impose a total ordering on $\mathbb{F}_q[\mathrm{x}]$ to ensure that the g_r (and thus submodule generators in $X_{\{q\}}$) are canonically defined.

The polynomials f and $\overline{f}$ do not have repeated roots. Indeed, if ξ is a root of g_1, then ξ is a root of $\overline{f}$, hence a primitive pth root of unity, and the roots of $\overline{f}$ are the ξ^i.

Proposition 3.18.

(i) *Each g_r is $\mathbb{F}_q$-irreducible, and $\bar{f} = g_1 \cdots g_v$.*
(ii) *There are monic irreducible factors $f_1, \ldots, f_v \in \mathbb{Z}_q[\mathrm{x}]$ of f such that $\overline{f_r} = g_r$ and $f = f_1 \cdots f_v$.*

Proof. Denote the Frobenius automorphism of $\mathbb{F}_q(\xi)/\mathbb{F}_q$ by β. Let $\Xi_r = \{\xi^{u^{1-r}q^i} \mid 1 \leq i \leq d\}$, the orbit of $\xi^{u^{1-r}}$ under $\langle\beta\rangle$. Further, let Λ_r be the set of roots of g_r. We assert that $\Lambda_r = \Xi_r$. Since $\langle\beta\rangle$ acts transitively on Ξ_r, this will prove that g_r is irreducible; since the set of roots of $\overline{f}$ is partitioned by the Ξ_r, this will also prove that $\bar{f} = g_1 \cdots g_v$.

Certainly $\Lambda_1 = \Xi_1$, because g_1 is irreducible and has ξ as a root. Assume inductively that $\Lambda_r = \Xi_r$ for some $r \geq 1$. Then $\xi^j \in \Lambda_{r+1}$ if and only if $\xi^{ju} \in \Lambda_r$. By the inductive hypothesis, this happens if and only if $j \equiv u^{1-(r+1)}q^i \bmod p$ for some i. Hence $\Lambda_{r+1} = \Xi_{r+1}$, completing the proof of (i) by induction. As the polynomial rings are UFDs, part (ii) then follows from Corollary 3.14. □

Thus, we factorize $\bar{f}$ over $\mathbb{F}_q$, then lift to the irreducible factors $f_r \in \mathbb{Z}_q[\mathrm{x}]$ of f by the algorithm in the proof of Lemma 3.13. Although this factorization depends strongly on the value of q, we omit q in some of the attendant polynomial notation to reduce clutter.

Definition 3.19.

(i) Let $X^{(r)}_{\{q\}}$ be the set of elements of $X_{\{q\}}$ annihilated by $f_r(s)$.

(ii) $X^{(r)}_{q,n} := \Omega_n X^{(r)}_{\{q\}}$.

(iii) $f_{r'} := \prod_{j\neq r} f_j$.

Remark 3.20. $X^{(r)}_{\{q\}}$ is a $\mathbb{Z}_q\langle s\rangle$-submodule.

Proposition 3.21.

(i) $X_{\{q\}} = X^{(1)}_{\{q\}} \times \cdots \times X^{(v)}_{\{q\}}$.

(ii) $X^{(r)}_{\{q\}} = X^{f_{r'}(s)}_{\{q\}}$ *for* $1 \leq r \leq v$.

Proof. There exist $h_1, \dots, h_v \in \mathbb{Q}_q[\mathrm{x}]$ such that $\sum_{r=1}^{v} f_{r'} h_r = 1$. We can choose $k \geq 0$ such that $c_r := q^k h_r \in \mathbb{Z}_q[\mathrm{x}]$ for all r. Since $X^{q^k}_{\{q\}} = X_{\{q\}}$,

$$X_{\{q\}} = \prod_{r=1}^{v} (X_{\{q\}})^{f_{r'}(s)c_r(s)} = \prod_{r=1}^{v} (X^{(r)}_{\{q\}})^{c_r(s)} \subseteq \prod_{r=1}^{v} X^{(r)}_{\{q\}}.$$

Thus $X_{\{q\}} = \prod_{r=1}^{v} X^{(r)}_{\{q\}}$.

If $X^{(r)}_{q,1} \cap \Omega_1\big(\prod_{j\neq r} X^{(j)}_{\{q\}}\big) \neq 1$, then there is a non-identity $b \in \Omega_1 X_{\{q\}}$ such that $b = b^{f_r(s)} = b^{f_{r'}(s)} = 1$. But $f_r w + f_{r'} z \equiv 1 \bmod q$ for some w, $z \in \mathbb{Z}_q[\mathrm{x}]$. Hence $b = b^{f_r w(s)} b^{f_{r'} z(s)} = 1$. $\square$

We embark on the task of determining the finite $\langle s\rangle$-submodules of each $X^{(r)}_{\{q\}}$.

Lemma 3.22. $X^{(r)}_{q,1}$ *is irreducible as an* $\langle s\rangle$*-module.*

Proof. Let d_r be the dimension of the subspace $X^{(r)}_{q,1}$ of the $(p-1)$-dimensional $\mathbb{F}_q$-space $\Omega_1 X_{\{q\}}$. The conjugation action of $\langle s\rangle$ induces a linear transformation s_r on $X^{(r)}_{q,1}$. Its minimal polynomial is g_r, so $d \leq \mathrm{d}_r$ by the Cayley–Hamilton theorem. This shows that $\mathrm{d}_r = d$, because $\sum_r \mathrm{d}_r = dv$. Therefore s_r has characteristic polynomial g_r. Since g_r is irreducible, $X^{(r)}_{q,1}$ is an irreducible $\langle s\rangle$-module. $\square$

Definition 3.23. Let $f_{r,n}(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ be the nth approximation of f_r found by the algorithm in the proof of Lemma 3.13 ($f_{r,n+1} \equiv f_r \bmod q^n$). Define

$$f_{r',n} = \prod_{j\neq r} f_{j,n} \in \mathbb{Z}[\mathrm{x}], \qquad x^{(r)}_{q,n} = b_{q^n}^{f_{r'}(s)}.$$

Since $(x^{(r)}_{q,n})^{q^n} = 1$, we obtain the useful working formula $x^{(r)}_{q,n} = b_{q^n}^{f_{r',n}(s)}$.

Lemma 3.24. $X^{(r)}_{q,n} \cong (C_{q^n})^d$ *is generated by* $x^{(r)}_{q,n}$ *as an* $\langle s\rangle$*-module.*

Proof. We saw in the proof of Lemma 3.22 that $X_{q,n}^{(r)} \cong (C_{q^n})^d$. Also, $x_{q,n}^{(r)}$ generates $(\Omega_n X_{\{q\}})^{f_{r'}(s)} = \Omega_n\big(X_{\{q\}}^{f_{r'}(s)}\big) = X_{q,n}^{(r)}$ as an $\langle s\rangle$-module. $\square$

Proposition 3.25. *The $\langle s\rangle$-module $X_{\{q\}}^{(r)}$ is uniserial: its only finite $\langle s\rangle$-submodules are the $X_{q,n}^{(r)}$, $n \geq 0$.*

Proof. Cf. the proof of Lemma 3.7; here we use Lemma 3.22. $\square$

Definition 3.26. Let $\mathcal{W}_q$ be the set of all subgroups $X_{q,n_1}^{(1)} X_{q,n_2}^{(2)} \cdots X_{q,n_v}^{(v)} Z_{q^c}$ of $D_{\{q\}}$ as $n_1, \ldots, n_v, c$ range over the non-negative integers.

Theorem 3.27. *$\mathcal{W}_q$ is the set of all finite $\langle s\rangle$-submodules of $D_{\{q\}}$.*

Proof. This is another application of Theorem 3.8, relying now on Propositions 3.21 and 3.25. In particular, if $i \neq j$ then a non-identity section of $X_{\{q\}}^{(i)}$ is not $\langle s\rangle$-isomorphic to a non-identity section of $X_{\{q\}}^{(j)}$ (since $f_i(s)$ does not annihilate both sections). $\square$

Remark 3.28. Each element of $\mathcal{W}_q$ is labeled by a unique $(v+1)$-tuple $n_1, \ldots, n_v, c$.

3.2. **All finite submodules of** $\mathrm{D}(p, \mathbb{C})$**.** Theorems 3.10 and 3.27 give the following.

Theorem 3.29. *The set $\mathcal{A}$ of direct products $Y \times \Pi_q W_q$, where $Y \in \mathcal{Y}$ and $W_q \in \mathcal{W}_q$ for finitely many primes $q \neq p$, is the set of all finite $\langle s\rangle$-submodules of* $\mathrm{D}(p, \mathbb{C})$.

Theorem 3.29 accounts for all the modules needed. That is, the T-modules for $\langle s\rangle \leq T \leq \mathrm{Sym}(p)$ are listed by refinement of $\mathcal{A}$.

As per Remarks 3.11 (iii) and 3.28, we designate each finite $\langle s\rangle$-submodule of $\mathrm{D}(p, \mathbb{C})$ by a unique integer parameter string.

With the implementation in mind, we outline how to list all $\langle s\rangle$-submodules M of a given order $o > 1$. Let $o = p^a b$ where $a \geq 0$ and b is a positive integer not divisible by p. The possible Sylow p-subgroups of M are the $Y_{j,k,l}$ where $j + k = a$, $0 \leq l \leq p-1$, and either $j = l = 0$ or $j, k \geq 1$. Let $q^e > 1$ be the largest power of the prime q in the prime factorization of b. Then $M_{\{p\}'} \cap X_{\{q\}}$ is some $W_q \in \mathcal{W}_q$; the choices for W_q correspond to the strings $n_1, \ldots, n_v, c$ of non-negative integers such that $e = d(n_1 + \cdots + n_v) + c$. We reckon thus for each prime factor q of b, and get all $\langle s\rangle$-submodules as direct products of these parts. The module generating sets are sufficient to assemble group generating sets of the T-extensions in $\mathrm{M}(p, \mathbb{C})$.

3.3. **Modules for every solvable permutation part.** Let $a \geq 1$ be a proper divisor of $p-1$. The next two lemmas enable us to refine the list $\mathcal{A}$ of Theorem 3.29 to a list of finite $\langle s, t^a\rangle$-modules, and are also used in solving the conjugacy problem.

Note that each finite $\langle s\rangle$-submodule of $X_{\{p\}}$ is a $\langle t\rangle$-module, by Lemma 3.7.

Lemma 3.30. *$Y^t_{j,k,l} = Y_{j,k,l'}$ where l' is the image of l under $t^j \in \mathrm{Sym}(p)$, i.e., $l' \equiv lu^j \bmod p$.*

Proof. Let m be the residue of $-j$ modulo $p-1$, and let $n = (j+m)/(p-1)$. If a_{p^k} denotes the diagonal matrix with $e^{2\pi \mathrm{i}/p^k}$ in position $(1,1)$ and 1s elsewhere on the main diagonal, then $x_{p^{j+1}} = \gamma^m(a_{p^n})$ for $m \neq 0$ and $x_{p^{j+1}} = \gamma^{p-1}(a_{p^{n+1}})$ for $m = 0$.

Suppose that $m > 0$; the proof for $m = 0$ is similar. It may be checked that $x^t_{p^{j+1}} = a_{p^n}^{t(1-s^u)^m}$ and $a^t_{p^n} = a_{p^n}^{s^{u-1}}$. Since $\langle s\rangle$ acts trivially on $X_{p^{j+1}}/X_{p^j}$,

$$x^t_{p^{j+1}} \equiv a_{p^n}^{(1-s^u)^m} \bmod X_{p^j}.$$

Binomial expansion in $\mathbb{Z}\langle s\rangle$ gives

$$(1-s^u)^m = (1-s)^m u^m + (\text{terms divisible by } (1-s)^{m+1}).$$

Thus $x^t_{p^{j+1}} \equiv x^{u^m}_{p^{j+1}} \bmod X_{p^j}$.

Let $y = x_{p^{j+1}} z^l_{p^{k+1}}$. Since $Y_{j,k,0}$ is a $\langle t\rangle$-module, we assume that $l > 0$. By the above, $y^t \in x^{u^m}_{p^{j+1}} z^l_{p^{k+1}} X_{p^j}$; so $(y^t)^{u^j} \in x_{p^{j+1}} z^{lu^j}_{p^{k+1}} X_{p^j}$. Hence $Y_{j,k,l'} \subseteq Y^t_{j,k,l}$. As these modules have the same order, they are equal. □

Lemma 3.31. $(X^{(1)}_{q,n_1} X^{(2)}_{q,n_2} \cdots X^{(v)}_{q,n_v})^t = X^{(1)}_{q,n_v} X^{(2)}_{q,n_1} \cdots X^{(v)}_{q,n_{v-1}}$.

Proof. The only indecomposable direct factors of $X_{\{q\}}$ are the $X^{(r)}_{\{q\}}$. Thus $(X^{(r)}_{\{q\}})^t = X^{(j)}_{\{q\}}$ for some j. The $X^{(1)}_{q,1}, \ldots, X^{(v)}_{q,1}$ are pairwise non-isomorphic $\langle s\rangle$-modules, so it is enough to prove that $(X^{(r)}_{q,1})^t \cong X^{(r+1)}_{q,1}$ (reading superscripts modulo v).

By Definition 3.16, $g_{r+1}(\mathrm{x})$ divides $g_r(\mathrm{x}^u)$, whence $g_r(s)^t \in g_{r+1}(s)\mathbb{Z}_q\langle s\rangle$. Each element of $X^{(r+1)}_{q,1}$ is annihilated by $g_{r+1}(s)$, and therefore by $g_r(s)^t$. Thus $(X^{(r+1)}_{q,1})^{t^{-1}} \subseteq X^{(r)}_{q,1}$; then $(X^{(r)}_{q,1})^t = X^{(r+1)}_{q,1}$ by Lemma 3.22. □

4. Monomial groups with cyclic permutation part

This section presents our first solutions of the extension and conjugacy problems. The resulting classification subsumes that in [8, §§2–3].

Definition 4.1. Let $\mathcal{L}$ be the set of all groups $\langle s z^i_{p^{k+1}}, A\rangle$ where $0 \leq i \leq p-1$ and $A \in \mathcal{A}$ as in Theorem 3.29 with $A \cap Z_{\{p\}} = Z_{p^k}$.

Proposition 4.2. *A finite subgroup of $\widetilde{\mathrm{M}}(p,\mathbb{C})$ with permutation part $\langle s\rangle$ is D-conjugate to a group in $\mathcal{L}$.*

Proof. Let G be a subgroup of $\widetilde{\mathrm{M}}(p,\mathbb{C})$ with $\phi(G)=\langle s\rangle$, so $sxz\in G$ for some torsion elements $x\in X$ and $z\in Z$. Since $\gamma(X)=X$, there exists $y\in X$ such that $G^y=\langle sz, D\cap G\rangle$. Then $z^p=(sz)^p\in(G\cap Z_{\{p\}})(G\cap Z_{\{p\}'})$ implies that we may multiply z by scalars from $D\cap G$ to get $z\in Z_{\{p\}}$. □

By Theorem 2.12, the irreducible groups in $\mathcal{L}$ are precisely the non-abelian ones: those with non-scalar diagonal subgroup.

Since each group in $\mathcal{L}$ is normalized by $\langle s\rangle$, and $N_{\mathrm{Sym}(p)}(\langle s\rangle)=\langle s,t\rangle$, Theorems 2.9 and 2.10 guarantee that the irreducible groups with a unique abelian normal subgroup of index p are $\mathrm{GL}(p,\mathbb{C})$-conjugate if and only if they are $D\langle t\rangle$-conjugate. We decide conjugacy of this type using the next two lemmas.

Lemma 4.3. *Let $G\in\mathcal{L}$, with $G\cap Z_{\{p\}}=Z_{p^k}$. Then G is $\langle t\rangle$-conjugate to some $H\in\mathcal{L}$ such that $s\in H$ or $sz_{p^{k+1}}\in H$.*

Proof. If $i\neq 0$ and $i^{-1}\equiv u^e \bmod p$, for u as in Notation 2.5, then $(sz_{p^{k+1}})^{t^e}\equiv(sz^i_{p^{k+1}})^{u^e} \bmod Z_{p^k}$. □

Lemma 4.4. *Distinct G, $H\in\mathcal{L}$ are D-conjugate if and only if $G\cap D=H\cap D$ and $G\cap D_{\{p\}}\in\{1, Y_{j,k,l}\mid l\neq 0\}$.*

Proof. Suppose that $G^d=H$ for some $d\in D$. Thus $G\cap H=D\cap H$. If $G\cap D_{\{p\}}=Y_{j,k,0}\neq 1$, then $[s,d]\in(G\cap D)Z\cap X\leq G\cap X\leq H$. As a consequence, $H=G$.

If $G\cap D_{\{p\}}=1$ then all $\langle sz^i_p, G\cap D\rangle$ in $\mathcal{L}$ are $\langle x_{p^2}\rangle$-conjugate.

Lastly, suppose that $G\cap D_{\{p\}}=Y_{j,k,l}$ where $1\leq l\leq p-1$. Now $\langle s, G\cap D_{\{p\}}\rangle^x=\langle sz^{-l}_{p^{k+1}}, G\cap D_{\{p\}}\rangle$ for $x\in D$ such that $\gamma(x)=x_{p^{j+1}}$. Hence all $\langle sz^i_{p^{k+1}}, G\cap D\rangle\in\mathcal{L}$ are $\langle x\rangle$-conjugate. □

If $G,H\in\mathcal{L}$ are conjugate by a non-monomial matrix, then each has more than one abelian normal subgroup of index p. Such a group G has a scalar subgroup of index p^2, so is nilpotent of class 2.

Lemma 4.5.

(i) *The groups in $\mathcal{L}$ that are nilpotent of class 2 are the $\langle sz^i_{p^{k+1}}, Y_{1,k,l}, Z_m\rangle$ where $k\geq 1$, $l\geq 0$, and $\gcd(p,m)=1$.*

(ii) *Let $\gcd(p,m)=1$. Up to $\mathrm{GL}(p,\mathbb{C})$-conjugacy, exactly two groups of order $p^{k+2}m$ in $\mathcal{L}$ are nilpotent of class 2, namely $\langle s, Y_{1,k,0}, Z_m\rangle$ and $\langle sz_{p^{k+1}}, Y_{1,k,0}, Z_m\rangle$.*

Proof. By Remark 3.11 (ii), if $G \in \mathcal{L}$ is nilpotent of class 2 then $G \cap D_{\{p\}} = Y_{1,k,l}$ for some l and $k \geq 1$.

We prove (ii) for $p \geq 3$. By (the proof of) Lemma 4.3, $H = \langle sz_{p^{k+1}}, Y_{1,k,0}\rangle = \langle sz_{p^{k+1}}, x_{p^2}\rangle$ is conjugate to each group $\langle sz^i_{p^{k+1}}, Y_{1,k,0}\rangle$ for $1 < i \leq p-1$. Let $e \in \mathrm{GL}(p,\mathbb{C})$ be the Vandermonde matrix with entry ϵ^{rc} in row r, column c, where $|\epsilon| = p$ (cf. [8, 4.1]). Then $s^e = x_{p^2}$ and $x^e_{p^2} = s^{-1}$; so $H^e = \langle s, Y_{1,k,1}\rangle$. Lemmas 3.30 and 4.4 show that H and the $\langle sz^i_{p^{k+1}}, Y_{1,k,l}\rangle$ for $i \geq 1$ or $l \geq 1$ are all conjugate to each other. However, H is not conjugate to $\langle s, Y_{1,k,0}\rangle$: this group has an elementary abelian subgroup of order p^3, while H does not. □

We now define sublists $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_4$ of groups $\langle sz^i_{p^{k+1}}, A\rangle \in \mathcal{L}$, on the way to eliminating redundancy in $\mathcal{L}$.

Definition 4.6. Groups in $\mathcal{L}_1$ have $A = \langle Y_{1,k,0}, Z_m\rangle$ for m coprime to p. Groups in $\mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$ have $A = \langle Y_{j,k,l}, \Pi_q W_q\rangle$ for finitely many primes $q \neq p$ where $W_q \in \mathcal{W}_q$. Conditions that govern membership of such $\langle sz^i_{p^{k+1}}, A\rangle$ in an $\mathcal{L}_i$ are as follows.

$\mathcal{L}_1$: $i \in \{0,1\}$ and $k \geq 1$.

$\mathcal{L}_2$: $i = 1$; $l = 0$; either $j = k = 0$ or $k \geq 1$; and either $j \geq 2$ or some W_q is non-scalar.

$\mathcal{L}_3$: $i = l = 0$; $k \geq 1$; and either $j \geq 2$ or some W_q is non-scalar.

$\mathcal{L}_4$: $i = 0$; $1 \leq l \leq p-1$; $j, k \geq 1$; and either $j \geq 2$ or some W_q is non-scalar.

Let $\mathcal{L}_0 = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$.

Each group in $\mathcal{L}_0$ has non-scalar diagonal subgroup, hence is irreducible.

Theorem 4.7.

(i) *Up to* $\mathrm{GL}(p,\mathbb{C})$*-conjugacy,* $\mathcal{L}_0$ *is a complete list of the finite irreducible subgroups of* $\mathrm{M}(p,\mathbb{C})$ *with permutation part* C_p*. That is, an irreducible group in* $\mathcal{L}$ *is conjugate to at least one group in* $\mathcal{L}_0$*.*

(ii) *Distinct* $G, H \in \mathcal{L}_0$ *are conjugate only if they are both in the same sublist* $\mathcal{L}_2$*,* $\mathcal{L}_3$*, or* $\mathcal{L}_4$*. If* $G, H \in \mathcal{L}_2$ *are conjugate, then* $G \cap D_{\{p\}} = H \cap D_{\{p\}} = 1$ *and* $G \cap D$ *is* $\langle t\rangle$*-conjugate to* $H \cap D$*. If* $G, H \in \mathcal{L}_i$ *for* $i = 3$ *or* 4 *are conjugate, then* G *is* $\langle t\rangle$*-conjugate to* H*.*

Proof. By Lemma 4.5, every group in $\mathcal{L}_1$ is nilpotent of class 2; a nilpotent group of class 2 in $\mathcal{L}$ is conjugate to a single group in $\mathcal{L}_1$; and no group in $\mathcal{L}_1$ can be conjugate to a group in $\mathcal{L}_0 \setminus \mathcal{L}_1$.

Assume now that $G \in \mathcal{L}$ is irreducible and not nilpotent of class 2. Then $G \cap D$ is the unique abelian normal subgroup of G with index p, so G is $\mathrm{GL}(p,\mathbb{C})$-conjugate to

$H \in \mathcal{L}$ only if G is $D\langle t\rangle$-conjugate to H. A laborious check against the definition of the $\mathcal{L}_i$ and Lemmas 4.3–4.5 confirm that G is conjugate to a group in $\mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$.

It remains to prove (ii) for $G, H \in \mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$. Suppose that $G = \langle sz_{p^{k+1}}, Y_{j,k,0}, M\rangle \in \mathcal{L}_2$ and $H \in \mathcal{L}_3 \cup \mathcal{L}_4$ are conjugate. Then $|G \cap D_{\{p\}}| = |H \cap D_{\{p\}}|$ implies that $k \geq 1$. Since H splits over its diagonal subgroup, G does too. But this is false: there is no $d \in D \cap G$ such that $|sz_{p^{k+1}}d| = p$ for $k \geq 1$ (if there were such a d, then $z_{p^k} = z_{p^{k+1}}^p$ would be in $\chi(Y_{j,k,0}) = Z_{p^{k-1}}$).

A group $G \in \mathcal{L}_2$ has $p-1$ different $\langle t\rangle$-conjugates of the form $\langle sz^i_{p^{k+1}}, A\rangle$, one for each $i \in \{1, \ldots, p-1\}$. By Lemmas 3.30 and 4.4, if $G \cap D_{\{p\}} \neq 1$ then the only one of these that is D-conjugate to a group in $\mathcal{L}_2$ is G itself.

Since $\langle t\rangle$-conjugacy leaves $\mathcal{L}_3$ and $\mathcal{L}_4$ setwise invariant, no group in $\mathcal{L}_3$ is $D\langle t\rangle$-conjugate to a group in $\mathcal{L}_4$ by Lemma 4.4. If $G, H \in \mathcal{L}_3 \cup \mathcal{L}_4$ are D-conjugate then $G = H$; hence G and H can be conjugate only if they are $\langle t\rangle$-conjugate. □

Corollary 4.8.

(i) *Groups in $\mathcal{L}_2$ are conjugate if and only if their diagonal subgroups have p'-order and are $\langle t\rangle$-conjugate.*

(ii) *Groups in either $\mathcal{L}_3$ or $\mathcal{L}_4$ are conjugate if and only if their diagonal subgroups are $\langle t\rangle$-conjugate.*

Theorem 4.9. *If $p = 2$ then $\mathcal{L}_0$ is a (complete and irredundant) classification of the finite irreducible subgroups of $\mathrm{M}(2, \mathbb{C})$.*

Proof. Here $t = 1$. Since $\mathcal{L}_1$ is irredundant and there is a single group in $\mathcal{L}_0 \setminus \mathcal{L}_1$ with given diagonal subgroup, the result follows from Theorem 4.7 and Corollary 4.8. □

If $G \in \mathcal{L}_2 \cup \mathcal{L}_3$ then we need only worry about $\langle t\rangle$-orbits in the $\mathcal{W}_q$. However, if $G \in \mathcal{L}_4$ then $\langle t\rangle$-conjugacy might change $G \cap D_{\{p\}}$.

We encode the action of $\langle t\rangle$ on the set of finite $\langle s\rangle$-submodules of $D_{\{p\}'}$ as an action by $\langle t\rangle$ on a set of arrays N. Each such array has $p-1$ columns and finitely many non-zero rows. Let $q \neq p$, and suppose that the Sylow q-subgroup of $A \in \mathcal{A}$ is $X^{(1)}_{q,n_1} X^{(2)}_{q,n_2} \cdots X^{(v)}_{q,n_v} Z_{q^c}$, where as usual $(p-1)/v$ is the multiplicative order of q modulo p. Row q of the array N_A has n_r in column r for $r \leq v$, and n_{r-v} in column r for $r > v$. By Lemma 3.31, N^t_A is the array obtained from N_A by shifting columns of N_A one place rightward, modulo $p-1$.

A lexicographic ordering is defined on these arrays. Specifically, $\mathsf{N} \leq \mathsf{N}'$ if and only if the first entry in the first row of N where N and N' differ is at most the matching entry in N'. We select a minimal element of each $\langle t\rangle$-orbit of N_A. Although cumbersome, this formulation of $\langle t\rangle$-conjugacy in $\cup_q \mathcal{W}_q$ is easily automated.

Definition 4.10. Let $\mathcal{L}^* := \mathcal{L}_1 \cup \mathcal{L}_2^* \cup \mathcal{L}_3^* \cup \mathcal{L}_4^*$, where

(i) $\mathcal{L}_2^*$ consists of those $G \in \mathcal{L}_2$ such that either $G \cap D_{\{p\}} \neq 1$, or $\mathsf{N}_{G\cap D}$ is $\langle t\rangle$-minimal (i.e., minimal in its $\langle t\rangle$-orbit);

(ii) $\mathcal{L}_3^*$ consists of those $G \in \mathcal{L}_3$ such that $\mathsf{N}_{G\cap D}$ is $\langle t\rangle$-minimal;

(iii) $\mathcal{L}_4^*$ consists of those $G \in \mathcal{L}_4$ such that
  - $G \cap D_{\{p\}} = Y_{j,k,l}$ for $l \in \{u, u^2, \ldots, u^{j'}\}$ modulo p where $j' = \gcd(j, p-1)$ and u is the least primitive integer modulo p,
  - $\mathsf{N}_{G\cap D}$ is $\langle t^{(p-1)/j'}\rangle$-minimal.

Theorem 4.7, Corollary 4.8, and the foregoing provide our first major classification of irreducible monomial groups.

Theorem 4.11. *Up to* $\mathrm{GL}(p,\mathbb{C})$*-conjugacy,* $\mathcal{L}^*$ *is a complete and irredundant list of the finite irreducible subgroups of* $\mathrm{M}(p,\mathbb{C})$ *with permutation part* C_p*.*

Proof. We prove that $\mathcal{L}^* \setminus \mathcal{L}_1$ is irredundant and complete.

By Definition 4.10 and Corollary 4.8, each group in $\mathcal{L}_3$ is conjugate to one in $\mathcal{L}_3^*$. Suppose that $G, H \in \mathcal{L}_3^*$ are conjugate. Minimality and Corollary 4.8 force $G \cap D = H \cap D$. But the groups in $\mathcal{L}_3$ are distinguished by their diagonal subgroups, so $G = H$. The reasoning for $\mathcal{L}_2^*$ is similar.

Now let $G = \langle s, G \cap D\rangle \in \mathcal{L}_4$, with $G \cap D_{\{p\}} = Y_{j,k,l}$. By Lemma 3.30, there is a unique non-negative integer a such that $a < (p-1)/j'$ and $H \cap D_{\{p\}} = Y_{j,k,\ell}$ where $H = G^{t^a}$ and $\ell \in \{u, u^2, \ldots, u^{j'}\}$ modulo p. Conjugation of H by some t^b preserves this value of ℓ (i.e., does not change $\langle s, H \cap D_{\{p\}}\rangle$) if and only if b is divisible by $(p-1)/j'$. Completeness of $\mathcal{L}^*$ is proved.

If $G, H \in \mathcal{L}_4^*$ are conjugate then $G \cap D_{\{p\}}$ and $H \cap D_{\{p\}}$ are $\langle t\rangle$-conjugate. By the uniqueness statement above, $G \cap D$ and $H \cap D$ can only be $\langle t^{(p-1)/j'}\rangle$-conjugate; so they are the same. Hence $G = H$. □

5. THE REMAINING SOLVABLE MONOMIAL GROUPS

In this section we classify the finite irreducible solvable subgroups of $\mathrm{M}(p,\mathbb{C})$ with non-cyclic permutation part. To that end, p is assumed odd (by Theorem 4.9).

Definition 5.1. Let $T = \langle s, t^a\rangle$ where $a \geq 1$ is a proper divisor of $p-1$, and let $\hat{a} = (p-1)/a$.

Up to conjugacy, the groups $T \cong C_p \rtimes C_{\hat{a}}$ in Definition 5.1 are the non-cyclic solvable transitive subgroups of $\mathrm{Sym}(p)$.

Recall the discussion before Definition 4.10 of $\langle t\rangle$-conjugacy in $\cup_q \mathcal{W}_q$.

Lemma 5.2. *The subset $\mathcal{A}^{[a]}$ of $\mathcal{A}$ (see Theorem 3.29) consisting of all A such that $\mathsf{N}_A^{t^a} = \mathsf{N}_A$ and either $l = 0$ or $aj \equiv 0 \bmod p-1$, where $A \cap D_{\{p\}} = Y_{j,k,l}$, is the set of all finite T-submodules of D.*

Proof. We refine $\mathcal{A}$ using Lemma 3.30. □

If $A \in \mathcal{A}^{[a]}$ and $X_{q,n_1}^{(1)} \cdots X_{q,n_v}^{(v)}$ is the Sylow q-subgroup of $A \cap X$, then $\mathsf{N}_A^{t^a} = \mathsf{N}_A$ is equivalent to $n_r = n_{r+a}$ for all r and q (see Lemma 3.31). These conditions are again straightforward to implement, building on our implementation of $\mathcal{A}$.

Definition 5.3. Let $\mathcal{M}^{[a]}$ be the set of all $\langle s, t^a z_{m\hat{a}}^c, A\rangle$ where $A \in \mathcal{A}^{[a]}$, $A \cap Z_{\{p\}'} = Z_m$, and $0 \le c < \hat{a}$.

Theorem 5.4. *A finite subgroup of DT with permutation part T is D-conjugate to a group in $\mathcal{M}^{[a]}$.*

Proof. Denote t^a by $\overline{t}$. Let G be a finite subgroup of DT such that $\phi(G) = T$. Put $A = G \cap D$ and $F = \phi^{-1}(\langle s\rangle) \cap G$. By Proposition 4.2, we assume that $F \in \mathcal{L}$.

The Frattini argument shows that if P is a Sylow p-subgroup of F, then there is $h \in N_G(P)$ such that $\phi(h) = \overline{t}$. We may replace h by an appropriate power of h to arrange that $h^{\hat{a}} \in A_{\{p\}'}$. Choose $g \in P$ with $\phi(g) = s$. Then $[h^{\hat{a}}, g] \in P \cap A_{\{p\}'} = 1$. Hence $h^{\hat{a}}$ is scalar (it is centralized by s).

So $h^{\hat{a}} = \lambda^{\hat{a}} 1_p$ for $\lambda \in \mathbb{C}^\times$ of p'-order such that $\det(h) = \lambda^p$. Define $y = (-1)^a \lambda 1_p$ and $x = \overline{t}^{\,-1} h y^{-1}$. Then $y^{\hat{a}} = h^{\hat{a}}$, $x \in X$ (as $\det(x) = 1$), and $h^{\hat{a}} = x^{\psi} y^{\hat{a}}$ where ψ is the element $1 + \overline{t} + \overline{t}^2 + \cdots + \overline{t}^{\,\hat{a}-1}$ of the integral group ring $\mathbb{Z}\langle s, t\rangle$. Thus $x^{\psi} = 1$.

Now $g = sz$ for $z \in Z_{\{p\}}$ such that $z^p \in A$. Since $g^h \in F$ and $s^t = s^u$, we have $d := x^{1-s^{\overline{t}}} \in z^{u^a - 1}A$ (remember $s^t = s^u$). Raising d to the power $1 + s^{\overline{t}} + \cdots + s^{\overline{t}(\tilde{u}-1)}$, where $\tilde{u} \equiv u^{-a} \bmod p$, reveals that $x^{1-s} \in z^{1-\tilde{u}}A$. Thus $\gamma^{p-1}(x) \in A$. The $\langle s\rangle$-module generated by x^p is the same as the one generated by $\gamma^{p-1}(x)$, so $x^p \in A$.

Fortunately, x can be conjugated away. Let $\mu = \overline{t} + 2\overline{t}^2 + \cdots + (\hat{a}-1)\overline{t}^{\,\hat{a}-1}$. Then $\mu(1-\overline{t}) = \psi - \hat{a}$, and we further calculate that G is conjugate by $x^{-a\mu}$ to

$$\langle szx^{a\mu(s-1)}, \overline{t}y, A\rangle.$$

(Note: the inclusion $(\overline{t}y)^{\hat{a}} \in A \cap Z_{\{p\}'}$ implies the possibilities for the generator with permutation part $\overline{t}$ in Definition 5.3.) Starting from the identity

$$t^b(s-1) = (s-1)(1 + s + \cdots + s^{u^{-b}-1})t^b$$

in $\mathbb{Z}\langle s,t\rangle$, we can prove the existence of $\nu \in \mathbb{Z}\langle s,t\rangle$ with coefficient sum

$$c \equiv \tilde{u} + 2\tilde{u}^2 + \cdots + (\hat{a}-1)\tilde{u}^{(\hat{a}-1)} \bmod p$$

such that $\mu(s-1) = (s-1)\nu$. Together with $x^{s-1} \in z^{\tilde{u}-1}A$, this yields $z^{(1-\tilde{u})ac}x^{a\mu(s-1)} \in A$. Also,

$$\begin{aligned}(\tilde{u}-1)c &\equiv -\tilde{u} - \tilde{u}^2 - \cdots - \tilde{u}^{\hat{a}-1} + (\hat{a}-1)\tilde{u}^{\hat{a}} \\ &\equiv 1 + (\hat{a}-1)\tilde{u}^{\hat{a}} \\ &\equiv \hat{a} \bmod p.\end{aligned}$$

Thus $(\tilde{u}-1)ac \equiv -1 \bmod p$. It follows that $zx^{a\mu(s-1)} \in A$, as required. □

Remark 5.5. The relative simplicity of the family $\mathcal{M}^{[a]}$ places restrictions on degree p representations of $\mathrm{Aut}(G)$ for $G \in \mathcal{L}$ (cf. [8, § 6]).

We move on to the conjugacy problem.

Lemma 5.6. *Each group in $\mathcal{M}^{[a]}$ is normalized by $\langle s\rangle$, and stays in $\mathcal{M}^{[a]}$ under $\langle t\rangle$-conjugation. If $G^d \in \mathcal{M}^{[a]}$ for $d \in D$, then $G^d = G$.*

Theorem 5.7. *If G, $H \in \mathcal{M}^{[a]}$ are irreducible and $\mathrm{GL}(p,\mathbb{C})$-conjugate, then either they are $\langle t\rangle$-conjugate, or they are $\langle e\rangle$-conjugate, where e is a Vandermonde matrix. The latter can occur only when each of G and H has more than one abelian normal subgroup with quotient T.*

Proof. Suppose that $G^w = H$ for some $w \in \mathrm{GL}(p,\mathbb{C})$. If $(G\cap D)^w = H \cap D$ then $w \in D\langle s,t\rangle$ up to scalars. Thus G and H are $\langle t\rangle$-conjugate by Lemma 5.6.

Suppose now that $(G\cap D)^w \neq H\cap D$. By the definition of $\mathcal{Y}$ and Lemma 5.2, $G\cap D = \langle x, G\cap Z\rangle$ where $x = x_{p^2}$; i.e., $G\cap D_{\{p\}} = H \cap D_{\{p\}} = Y_{1,k,0}$ for some k. The Fitting subgroup $\langle s, G\cap D\rangle$ of G (and of H) has unique Sylow p-subgroup $E = \langle s, x\rangle$, an extraspecial group of order p^3 and exponent p. Therefore $w \in N := N_{\mathrm{GL}(p,\mathbb{C})}(E)$.

It is proved in [5, § 3] that $N_{\mathrm{PGL}(p,\mathbb{C})}(EZ/Z)/(EZ/Z) \cong \mathrm{SL}(2,p)$. As the largest subgroup of exponent p, E is characteristic in EZ. Hence $N/EZ \cong \mathrm{SL}(2,p)$.

For the Vandermonde matrix e defined in the proof of Lemma 4.5, $s^e = x$ and $x^e = s^{-1}$. Also $t^e = t^{-1}$. (We know from the proof of Lemma 3.30 that $x^t = x^{\tilde{u}}$ where $\tilde{u} \equiv u^{-1} \bmod p$. Thus $t^e t$ centralizes E. So the scalar $t^e t$ is 1, because t^{-1} and t^e have trace 1.) Let σ be the natural surjection of N onto $\mathrm{SL}(2,p)$. If $d := x_{p^3}$ then $\sigma(d)$ has order p, so generates a Sylow p-subgroup of $\mathrm{SL}(2,p)$. Its normalizer $\sigma(\langle d,t\rangle)$ is maximal in $\mathrm{SL}(2,p)$. Consequently $\mathrm{SL}(2,p) = \sigma(\langle d,t,e\rangle)$.

Observe that $\sigma(w)$ normalizes $\langle\sigma(t^a)\rangle = \sigma(G) = \sigma(H)$. Representing $\sigma(d)$, $\sigma(t)$, and $\sigma(e)$ in $\mathrm{SL}(2,p)$ according to conjugation action on the basis $\{sZ(E), xZ(E)\}$ of $\mathbb{F}_p^2$, we find that $\sigma(\langle t, e\rangle)$ is monomial. If the diagonal subgroup $\sigma(\langle t^a\rangle)$ is non-scalar then it has normalizer $\sigma(\langle t, e\rangle)$ in $\mathrm{SL}(2,p)$; otherwise $G^d = G$. Since $G^t = G$, this completes the proof. □

Definition 5.8. Let $\mathcal{M}_1^{[a]}$, $\mathcal{M}_2^{[a]}$, and $\mathcal{M}_3^{[a]}$ respectively denote the sublists of $\mathcal{M}^{[a]}$ consisting of $G = \langle s, t^a z_{m\hat{a}}^c, Y_{j,k,l}, G \cap D_{\{p\}'}\rangle$ that satisfy (1), (2), (3) below.

(1) $l = 0$, $0 \leq c \leq \hat{a}/2$, $j = 1$, and $\mathsf{N}_{G\cap D} = 0$.

(2) $l = 0$, either $j \geq 2$ or $\mathsf{N}_{G\cap D} \neq 0$, and $\mathsf{N}_{G\cap D}$ is $\langle t\rangle$-minimal.

(3) $j \geq 2$ is divisible by $\hat{a}$, $l \in \{u, u^2, \ldots, u^{j'}\}$ modulo p where $j' = \gcd(j, p-1)$, and $\mathsf{N}_{G\cap D}$ is $\langle t^{(p-1)/j'}\rangle$-minimal.

Let $\mathcal{M}^*$ be the union of all $\mathcal{M}^{[a]*} := \mathcal{M}_1^{[a]} \cup \mathcal{M}_2^{[a]} \cup \mathcal{M}_3^{[a]}$ as a ranges over the proper divisors of $p-1$.

The solvable groups are now classified.

Theorem 5.9. *For $\mathcal{L}^*$ as in Definition* 4.10*, $\mathcal{L}^* \cup \mathcal{M}^*$ is a complete and irredundant list of the solvable finite irreducible monomial subgroups of* $\mathrm{GL}(p,\mathbb{C})$.

Proof. All groups in $\mathcal{M}^*$ are irreducible (Theorem 2.12). By Theorems 2.9, 4.11, and 5.4, we must show that each element of $\mathcal{M}^{[a]}$ (for fixed a) is conjugate to one and only one element of $\mathcal{M}^{[a]*}$.

Let $G = \langle s, t^a z_{m\hat{a}}^c, A\rangle \in \mathcal{M}^{[a]}$ where $A \cap D_{\{p\}} = Y_{j,k,l}$. Heeding Lemma 5.2, we first suppose that $l = 0$. By Lemma 3.30 and Theorem 5.7, if G has a unique abelian normal subgroup with quotient T, then the only group in $\mathcal{M}^{[a]*}$ that is conjugate to G lies in $\mathcal{M}_2^{[a]}$. Otherwise, $j = 1$ and $\mathsf{N}_{G\cap D} = 0$. We have $G^e = \langle s, t^a z_{m\hat{a}}^{\hat{a}-c}, A\rangle$. Thus the $\langle e\rangle$-orbit of G contains just one group H with $c \leq \hat{a}/2$. Since $H \in \mathcal{M}_1^{[a]}$, the only element of $\mathcal{M}^{[a]*}$ conjugate to G is H.

Suppose next that $l \geq 1$, so j is positive and $j \equiv 0 \bmod \hat{a}$. Only $\langle t\rangle$-conjugacy matters here, and G cannot be conjugate to a group in $\mathcal{M}_1^{[a]} \cup \mathcal{M}_2^{[a]}$. The rest of the proof echoes the last two paragraphs in the proof of Theorem 4.11. □

6. Non-solvable monomial groups

Our objective in this section is to prove general-purpose results for (finite) subgroups of $\mathrm{M}(p,\mathbb{C})$ with non-solvable transitive permutation part T. In later sections, we treat $T = \mathrm{Sym}(p)$, $T = \mathrm{Alt}(p)$, and special cases of T required to facilitate the classifications for $p \leq 11$.

Notation 6.1. Let $p \geq 5$, let q be a prime, let T be a non-solvable subgroup of $\mathrm{Sym}(p)$ containing s, and let π be the set of primes other than p that divide $|T|$.

Note that all primes in π are less than p.

A finite T-submodule of $D_{\{p\}}$ is sandwiched between $\Omega_n X_{\{p\}}$ and $Z_{\{p\}} \cdot \Omega_n D_{\{p\}}$ for some $n \geq 0$.

Lemma 6.2. *If $A = Y_{j,k,l} \in \mathcal{Y}$ then the following are equivalent.*

(i) *A is a T-module.*

(ii) *A is a $\mathrm{Sym}(p)$-module.*

(iii) *Either $j \equiv 0 \bmod (p-1)$, or both $l = 0$ and $j \equiv -1 \bmod (p-1)$.*

Proof. Let $j = n(p-1)$. Then $X_{p^j} = \Omega_n X_{\{p\}}$ and thus $Y_{j-1,k,0} = X_{p^j} Z_{p^k}$ are $\mathrm{Sym}(p)$-modules. Since $M := \Omega_n D_{\{p\}}$ is a $\mathrm{Sym}(p)$-module of order p^{np}, and $Y_{j-1,n,0}$ has index p in M, it follows that $M = Y_{j,n,l}$ for some $l \neq 0$. Hence $X \cap ZM = X_{p^{j+1}}$ is a $\mathrm{Sym}(p)$-module. Taking p^n-powers, we deduce that $X_{p^{j+1}}/X_{p^j} \cong Z_p$ is trivial as a $\mathrm{Sym}(p)$-module, so (iii) $\Rightarrow$ (ii) by Theorem 3.8.

Suppose that A is a (non-identity) T-module. If $l \neq 0$ (resp., $l = 0$) then $A \cap X = X_{p^j}$ (resp., $A \cap X = X_{p^{j+1}}$). By [31, Satz 5.1], the only non-identity proper T-submodules of $\Omega_1 D_{\{p\}}$ are $X_p = Z_p$ and $\Omega_1 X_{\{p\}} = X_{p^{p-1}}$. Since $(A \cap X)^r \in \Omega_1 X_{\{p\}}$ for some p-power r, necessarily $A \cap X$ is $X_{p^{n(p-1)}}$ or $X_{p^{n(p-1)+1}}$ for some $n \geq 1$. The permitted values of j and l in (iii) are now evident. □

We derive a weaker statement for submodules of p'-order.

Proposition 6.3. *If $q \neq p$ then $X_{\{q\}}$ is an indecomposable T-module.*

Proof. Let $W = \Omega_1 D_{\{q\}}$. We prove that the $\mathbb{F}_q$-space $\mathrm{End}_T W$ has dimension 2. Since $W = Z_q \times \Omega_1 X_{\{q\}}$, this will imply that $\Omega_1 X_{\{q\}}$ and thus $X_{\{q\}}$ are indecomposable T-modules.

The permutation matrix group T embeds in $\mathrm{GL}(p,q)$ under entrywise reduction modulo q, and T thereby acts on $\mathrm{Mat}(p, \mathbb{F}_q)$ by conjugation, with fixed-point space $\mathrm{End}_T W$. By a result of Burnside [30, Theorem 3], T is 2-transitive. Hence the elementary matrices in $\mathrm{Mat}(p, \mathbb{F}_q)$ are permuted in two orbits by T:

$$\{[\delta_{i,k}\delta_{l,j}]_{i,j} \mid k \neq l,\ 1 \leq k, l \leq p\} \qquad \text{and} \qquad \{[\delta_{i,k}\delta_{k,j}]_{i,j} \mid 1 \leq k \leq p\}.$$

Summing the elements in each orbit gives a basis of $\mathrm{End}_T W$. □

Corollary 6.4. *For q coprime to $|T|$, the $\Omega_n X_{\{q\}}$ are all the finite T-submodules of $X_{\{q\}}$.*

Proof. (Cf. the proof of Lemma 3.7.) By Maschke's Theorem, $\Omega_1 X_{\{q\}}$ is a completely reducible $\mathbb{F}_q T$-module. Hence $\Omega_1 X_{\{q\}}$ is irreducible by Proposition 6.3, so is in every non-identity T-submodule of $X_{\{q\}}$. □

We show that p and primes not dividing $|T|$ can be set aside from submodule orders that appear in our solution of the extension problem for T.

Proposition 6.5. *Let G be a finite subgroup of DT such that $\phi(G) = T$. Then there exists $H \leq TD_\pi$ such that $s \in H$ and G is D-conjugate to $H.(G \cap D_{\pi'})$.*

Proof. By [27, Satz V.21.1 c)], $N_T(\langle s \rangle) \neq \langle s \rangle$. Thus G has a subgroup with solvable non-cyclic permutation part, and we may suppose that $s \in G$ by Theorem 5.4.

Denote the natural surjection of $TD = GD$ onto $TD/(G \cap D_{\pi'})D_\pi$ by an overline; then $\overline{GD} = \overline{TD} = \overline{G} \ltimes \overline{D} = \overline{T} \ltimes \overline{D}$. Also, $|\overline{T} : \overline{T} \cap \overline{G}|$ is a π-number, while $\overline{D}$ is a π'-group. Therefore, by [14, Lemma 1, corrected], $\overline{T}$ and $\overline{G}$ are $\overline{D}$-conjugate. This implies that, for some $d \in D_{\pi'}$,

$$G^d D_\pi = (GD_\pi)^d = TD_\pi(G \cap D_{\pi'}) = TD_\pi(G^d \cap D_{\pi'}).$$

Then $G^d = H.(G \cap D_{\pi'})$ where $H = G^d \cap TD_\pi$. Since $s[s,d] = s^d \in TD_\pi(G^d \cap D_{\pi'})$ and thus $[s,d] \in D_\pi(G^d \cap D_{\pi'})$, we have $[s,d] \in G^d \cap D_{\pi'}$. Hence $s = s^d[s,d]^{-1} \in G^d \cap T \leq H$. □

So each group with non-solvable permutation part T in our final list is the semi-direct product of a T-submodule of $D_{\pi'}$ by a 'hub group' in TD_π containing s.

The next result is a companion piece to Proposition 6.5, dealing with a ubiquitous kind of hub group. If the hypotheses are fulfilled, then we can discard even more of a diagonal subgroup when solving the extension problem. (Recall that for a group K and K-module U, there is a one-to-one correspondence between the first cohomology group $H^1(K,U)$ and the set of conjugacy classes of complements of U in $U \rtimes K$.)

Proposition 6.6. *Let G be a finite subgroup of TD_π such that $\phi(G) = T$ and $s \in G$. Suppose that $D_\pi = B \times C$ for T-modules B and C where $H^1(T, B/G \cap B) = 0$. Then G is B-conjugate to $H.(G \cap B)$ for some $H \leq TC$ such that $\phi(H) = T$ and $s \in H$.*

Proof. By Theorem 3.27, $G \cap D_\pi = (G \cap B)(G \cap C)$. We mimic the proof of Proposition 6.5, with D_π, B, C here in place of D, $D_{\pi'}$, D_π there, respectively; $\overline{G}$ and $\overline{T}$ are B-conjugate because $H^1(T, D_\pi/(G \cap B)C) \cong H^1(T, B/G \cap B) = 0$. □

Occasionally the T-module structure of $B/(B \cap G)$ is independent of G.

Lemma 6.7. *Let ζ be a subset of π consisting of q such that $\Omega_1 X_{\{q\}}$ is an irreducible T-module, and let $B = \prod_{q\in\zeta} X_{\{q\}} \cdot \prod_{q\in\eta} Z_{\{q\}}$ where η is any subset of π. Then $B/A \cong B$ as T-modules for every finite T-submodule A of B.*

Proof. It suffices to assume that $B = X_{\{q\}}$ for $q \in \zeta$. Since $\Omega_1 B$ is an irreducible T-module, A must be some $\Omega_n B$. Certainly $B/\Omega_n B \cong B$. □

We record basic results for calculating first cohomology. These use the following definition. If $R \leq T$ and M is a right R-module, then M_R^T denotes the T-module co-induced from M. That is, M_R^T has element set $\mathrm{Hom}_R(\mathbb{Z}T, M)$, and becomes a T-module by setting $\rho y(x) = \rho(yx)$ for $\rho \in \mathrm{Hom}_R(\mathbb{Z}T, M)$, $y \in T$, and $x \in \mathbb{Z}T$.

Lemma 6.8 (Eckmann–Shapiro [32, p. 561])**.** $H^n(R, M) \cong H^n(T, M_R^T)$ *for all* $n \geq 0$.

Lemma 6.9. *Let $R = T \cap \mathrm{S}_{p-1}$, where $\mathrm{S}_{p-1} \cong \mathrm{Sym}(p-1)$ is the group of permutation matrices in $\mathrm{GL}(p, \mathbb{C})$ whose elements have 1 in position (p, p). Then $D_{\{q\}} \cong (Z_{\{q\}})_R^T$ as T-modules.*

Proof. Since each $\rho \in (Z_{\{q\}})_R^T$ is determined by its values on a transversal U for the p cosets of R in T, as a group $(Z_{\{q\}})_R^T$ is isomorphic to the group of all set maps $U \to Z_{\{q\}}$, which in turn is isomorphic to $D_{\{q\}}$.

Let θ be the R-homomorphism from $D_{\{q\}}$ into $Z_{\{q\}}$ defined by $\mathrm{diag}(a_1, \ldots, a_p) \mapsto \mathrm{diag}(a_p, \ldots, a_p)$. By [28, Theorem 4.9, p. 55], there is a T-homomorphism $\theta' \colon D_{\{q\}} \to (Z_{\{q\}})_R^T$ with kernel in $\ker\theta$. But $\ker\theta$ contains no non-identity T-modules. Thus θ' is an isomorphism, as desired. □

Remark 6.10. If K is perfect and M is a trivial K-module, then $H^1(K, M) = 0$.

7. Permutation part $\mathrm{Sym}(p)$

We maintain Notation 6.1, writing S_n for $\mathrm{Sym}(n)$.

Definition 7.1. Let $\mathcal{A}^{[S]}$ be the set of $A \in \mathcal{A}$ such that $\mathsf{N}_A^t = \mathsf{N}_A$, and if $A \cap D_{\{p\}} = Y_{j,k,l}$, then either $j \equiv 0 \bmod (p-1)$, or both $l = 0$ and $j \equiv -1 \bmod (p-1)$.

Lemma 7.2. $\mathcal{A}^{[S]}$ *is the set of all finite* S_p*-submodules of* $\mathrm{D}(p, \mathbb{C})$.

Proof. Follows from Lemmas 3.31 and 6.2. □

In particular, for $q \neq p$, the $\Omega_n X_{\{q\}}$ are all the finite S_p-submodules of $X_{\{q\}}$.

Lemma 7.3. $H^1(\mathrm{S}_p, X_{\{2\}}) = 0$ *and* $H^1(\mathrm{S}_p, D_{\{q\}}) = 0$ *if q is odd.*

Proof. By Lemmas 6.8 and 6.9, $H^1(\mathrm{S}_p, D_{\{q\}}) \cong H^1(\mathrm{S}_{p-1}, Z_{\{q\}})$. Now $H^1(\mathrm{S}_n, Z_{\{q\}}) = \mathrm{Hom}(\mathrm{S}_n/\mathrm{S}_n', Z_{\{q\}})$. Thus $H^1(\mathrm{S}_p, D_{\{q\}}) = 0$ if q is odd, whereas $H^1(\mathrm{S}_p, D_{\{2\}}) \cong C_2$. Since $D_{\{2\}} = X_{\{2\}} \times Z_{\{2\}}$ implies that $H^1(\mathrm{S}_p, D_{\{2\}}) = H^1(\mathrm{S}_p, X_{\{2\}}) \oplus H^1(\mathrm{S}_p, Z_{\{2\}})$, the rest of the lemma is clear. □

Definition 7.4. Let $r = (1, 2) \in \mathrm{S}_p$; so $\mathrm{S}_p = \langle s, r\rangle$. Define $\mathcal{R}$ to be the set of groups $\langle s, r, A\rangle$ and $\langle s, rz_{2^{n+1}}, A\rangle$ where $A \in \mathcal{A}^{[S]}$ and $|A \cap Z_{\{2\}}| = 2^n$, for all $n \geq 0$.

Proposition 7.5. *If G is a finite subgroup of $\mathrm{M}(p, \mathbb{C})$ with permutation part S_p, then G is D-conjugate to a group in $\mathcal{R}$.*

Proof. Let G be a hub group, i.e., $G \leq \mathrm{S}_p D_\pi$ and $s \in G$ (see Proposition 6.5). We have $D_\pi = B \times Z_{\{2\}}$ where $B = X_{\{2\}} \prod_{q\in\pi\setminus\{2\}} D_{\{q\}}$. By Lemma 7.3, $H^1(\mathrm{S}_p, B) = 0$, and $B/(G \cap B) \cong B$ as S_p-modules by Lemmas 6.7 and 7.2. Proposition 6.6 then gives $d \in D$ such that $G^d = H.(B \cap G)$ where $H = G^d \cap \mathrm{S}_p Z_{\{2\}}$ and $s \in H$. Thus $H = \langle s, rz, Z_{2^n}\rangle$ for some n and $z \in Z_{\{2\}}$. So $G^d \in \mathcal{R}$ because $z^2 = (rz)^2 \in Z_{2^n}$. □

Lemma 7.6. *A finite subgroup of $\mathrm{M}(p, \mathbb{C})$ with permutation part S_p is reducible if and only if its diagonal subgroup is scalar.*

Proof. If $G \in \mathcal{R}$ and $G \cap D \leq Z$ then $G \leq \mathrm{S}_p Z$ is reducible. □

Lemma 7.7. *Distinct irreducible groups in $\mathcal{R}$ are not $\mathrm{GL}(p, \mathbb{C})$-conjugate.*

Proof. Let $G \in \mathcal{R}$ be irreducible with diagonal subgroup A, and suppose that $G^h \in \mathcal{R}$ for some $h \in \mathrm{GL}(p, \mathbb{C})$. By Theorem 2.9, $A^h = G^h \cap D$. Then $G^h \cap D = A$ by Theorem 2.10. The two groups in $\mathcal{R}$ with diagonal subgroup A are not conjugate (their images under the determinant map have different 2-parts), so $G^h = G$. □

We next delete the reducible groups from $\mathcal{R}$.

Definition 7.8. Let $\mathcal{R}^*$ be the subset of $\mathcal{R}$ consisting of all groups G such that $A = G \cap D \in \mathcal{A}^{[S]}$ as in Definition 7.1 satisfies one of the following:

(i) $j \neq 0$ and $j \equiv 0 \bmod (p-1)$;
(ii) $j \equiv -1 \bmod (p-1)$ and $l = 0$;
(iii) $j = l = 0$ and $\mathsf{N}_A \neq 0$.

The main problems for $T = \mathrm{Sym}(p)$ are now solved.

Theorem 7.9. *$\mathcal{R}^*$ is a classification of the finite irreducible subgroups of $\mathrm{M}(p, \mathbb{C})$ with permutation part $\mathrm{Sym}(p)$.*

8. Permutation part $\mathrm{Alt}(p)$

This section incidentally disposes of all degrees at most 5. Degree 5 requires added care.

Let $p \geq 5$ and $\mathrm{A}_n := \mathrm{Alt}(n)$.

Proposition 8.1. *A finite A_p-submodule of $\mathrm{D}(p, \mathbb{C})$ is an S_p-module.*

Proof. By Lemma 6.2, we need only show that $M := \Omega_1 X_{\{q\}}$ is an irreducible A_p-module for primes $q \neq p$. By Proposition 3.21, Lemma 3.22, and the proof of Theorem 3.27, M is a direct product of v irreducible pairwise non-isomorphic $\langle s \rangle$-submodules $X_{q,1}^{(i)}$. We infer from Lemma 3.31 that M is an irreducible $\langle s, t^2 \rangle$-module when v is odd. Let v be even. As an A_p-module, if M were reducible then it would be the direct sum of its $\langle s, t^2 \rangle$-submodules $\prod_{i \text{ odd}} X_{q,1}^{(i)}$ and $\prod_{i \text{ even}} X_{q,1}^{(i)}$. This contradicts Proposition 6.3. $\square$

Lemma 8.2. $H^1(\mathrm{A}_5, X_{\{3\}}) = C_3$ *and* $H^1(\mathrm{A}_p, D_{\{q\}}) = 0$ *for* $(p, q) \neq (5, 3)$.

Proof. Cf. the proof of Lemma 7.3. $\square$

Definition 8.3. Let $w = (1, 2, 3) \in \mathrm{P}(p)$, so $\mathrm{A}_p = \langle s, w \rangle$. Let $\mathcal{U}_0$ be the set of groups $\langle s, w, A \rangle$ for $A \in \mathcal{A}^{[S]}$.

Proposition 8.4. *If $p > 5$ and G is a finite subgroup of $\mathrm{M}(p, \mathbb{C})$ with permutation part A_p, then G is D-conjugate to a group in $\mathcal{U}_0$.*

Proof. Since $H^1(\mathrm{A}_p, D_\pi) = 0$ by Lemma 8.2, and we may take $\zeta = \eta = \pi$ in Lemma 6.7, G is conjugate to $\langle \mathrm{A}_p, G \cap D \rangle$ by Proposition 6.6. $\square$

Lemma 8.5. *Distinct irreducible groups in $\mathcal{U}_0$ are not $\mathrm{GL}(p, \mathbb{C})$-conjugate.*

Proof. Cf. the proof of Lemma 7.7. Proposition 8.1 comes into play; reducibility of G is again equivalent to $G \cap D \leq Z$, and there is a single group in $\mathcal{U}_0$ with a given diagonal subgroup. $\square$

Definition 8.6. Let $\mathcal{U}_0^*$ be the set of $\langle s, w, A \rangle \in \mathcal{U}_0$ such that one of (i)–(iii) as in Definition 7.8 holds for $A \in \mathcal{A}^{[S]}$.

Thus, $\mathcal{U}_0^*$ is the subset of irreducible groups in $\mathcal{U}_0$.

Theorem 8.7. *If $p \geq 7$ then $\mathcal{U}_0^*$ is a classification of the finite irreducible subgroups of $\mathrm{M}(p, \mathbb{C})$ with permutation part $\mathrm{Alt}(p)$.*

Proof. Proposition 8.4 and Lemma 8.5 show that $\mathcal{U}_0^*$ is complete and irredundant. $\square$

8.1. **Degree** 5. Now fix $p = 5$.

Definition 8.8. Let $c_n = \mathrm{diag}(1, \epsilon_n, \epsilon_n^{-1}, \epsilon_n^{-1}, \epsilon_n)$ where $\epsilon_n = e^{2\pi \mathrm{i}/3^n}$. For $i \in \{1, 2\}$, define $\mathcal{U}_i$ to be the set of groups $\langle s, wc_{n+1}^i, A\rangle \leq \mathrm{M}(5, \mathbb{C})$ where $A \in \mathcal{A}^{[S]}$ and $A \cap X_{\{3\}} = \Omega_n X_{\{3\}}$, as n ranges over the non-negative integers.

Remark 8.9. $\langle s, wc_{n+1}^i\rangle$ has diagonal subgroup $\Omega_n X_{\{3\}}$.

Lemma 8.10. *The* $W_i = \langle s, wc_1^i\rangle$ *for* $i \in \{0, 1, 2\}$ *are isomorphic to* A_5*, and no two of these groups are conjugate in* $D\mathrm{A}_5$*.*

Proof. Obviously $W_0 = \mathrm{A}_5$ is reducible. Also, W_1 and W_2 correspond to the ordinary irreducible character of A_5 of degree 5 (hence they are $\mathrm{GL}(5, \mathbb{C})$-conjugate). If W_1 and W_2 were $D\mathrm{A}_5$-conjugate, then they would be D-conjugate; but $s^d \notin W_2$ for non-scalar $d \in D$. $\square$

Theorem 8.11. *A finite subgroup* G *of* $D\mathrm{A}_5$ *such that* $\phi(G) = \mathrm{A}_5$ *is conjugate to a group in* $\mathcal{U}_0 \cup \mathcal{U}_1 \cup \mathcal{U}_2$*.*

Proof. By Proposition 6.6, and Lemmas 6.7 and 8.2, we may suppose that the hub group G is in $M := X_{\{3\}}\mathrm{A}_5$. So $G \cap D = \Omega_n X_{\{3\}}$ for some n. Let τ be the surjective endomorphism of M that is the identity on A_5 and maps $x \in X_{\{3\}}$ to x^{3^n}. Note that $\ker \tau = G \cap D$.

The W_i and $\tau(G)$ are all complements of $X_{\{3\}}$ in M. Since $|H^1(\mathrm{A}_5, X_{\{3\}})| = 3$, Lemma 8.10 implies that $\tau(G)$ is M-conjugate, i.e., $\tau(M)$-conjugate, to $W_i = \tau(\langle s, wc_{n+1}^i\rangle)$ for some i. Therefore G is M-conjugate to $\langle s, wc_{n+1}^i\rangle$. $\square$

Lemma 8.12. *Each group in* $\mathcal{U}_2$ *is conjugate to a group in* $\mathcal{U}_1$*.*

Proof. Here $t = (1, 2, 4, 3)$. Matrix multiplication establishes that $(wc_n)^{s^3 wc_n s^2} \equiv w^t c_n^{2t}$ modulo the diagonal subgroup $\Omega_{n-1} X_{\{3\}}$ of $\langle s, wc_n\rangle$. $\square$

Lemma 8.13. *All groups in* $\mathcal{U}_1$ *are irreducible.*

Proof. Let $G = \langle s, wc_{n+1}, A\rangle \in \mathcal{U}_1$. If $n = 0$ then G contains the irreducible group W_1. If $n \geq 1$ then A is non-scalar. $\square$

Lemma 8.14. *Distinct groups in* $\mathcal{U}_0 \cup \mathcal{U}_1$ *are not* $\mathrm{GL}(5, \mathbb{C})$*-conjugate.*

Proof. We proceed as in the proofs of Lemmas 7.7 and 8.5. Suppose that $\langle s, wc_{n+1}, A\rangle^d = \langle s, w, A\rangle$ for some $d \in D$, where $A \cap X_{\{3\}} = \Omega_n X_{\{3\}}$. Then $[w, d]c_{n+1} \in A \cap X$. However, $[w, d]c_{n+1}$ has a diagonal entry of order 3^{n+1}. $\square$

Theorem 8.15. $\mathcal{U}_0^* \cup \mathcal{U}_1$ *is a classification of the finite irreducible subgroups of* $\mathrm{M}(5, \mathbb{C})$ *with permutation part* $\mathrm{Alt}(5)$*.*

9. Degrees greater than 5

Let G be a finite irreducible subgroup of $\mathrm{M}(p,\mathbb{C})$ with permutation part T. In previous sections we classified all G such that T is compulsory. A member of the non-compulsory 'projective' family, $\mathrm{SL}(3,2)$, is self-normalizing in $\mathrm{Sym}(7)$, hence is the only non-compulsory T for $p=7$. In degrees 11 and 23, the non-compulsory T are M_{11}, $\mathrm{PSL}(2,11)$, and M_{23}.

9.1. **Degree** 7.

Let $p=7$ and $T\cong \mathrm{SL}(3,2)$. Thus $\pi=\{2,3\}$.

Definition 9.1. $V\cong \mathrm{SL}(3,2)$ is the subgroup of S_7 generated by s and $v=(1,2)(3,5)$.

Lemma 9.2. *If q is an odd prime then a finite V-submodule of $D_{\{q\}}$ is an S_7-module.*

Proof. We combine Lemma 6.2, Corollary 6.4, and Proposition 3.25 (for $q=3$, as $X_{\{3\}}=X^{(1)}_{\{3\}}$). □

The V-submodule structure of $X_{\{2\}}=X^{(1)}_{\{2\}}X^{(2)}_{\{2\}}$ is less tractable. Here we resume the conventions of Section 3.1.2, fixing $q=2$. In $\mathbb{Z}_2[\mathrm{x}]$, $f(\mathrm{x})=\mathrm{x}^6+\mathrm{x}^5+\mathrm{x}^4+\mathrm{x}^3+\mathrm{x}^2+\mathrm{x}+1$ factorizes as the product of irreducibles f_1, f_2, with integer polynomial approximations

$$\begin{aligned} f_{1,1}(\mathrm{x}) &= \mathrm{x}^3+\mathrm{x}+1 & \qquad f_{2,1}(\mathrm{x}) &= \mathrm{x}^3+\mathrm{x}^2+1\\ f_{1,2}(\mathrm{x}) &= \mathrm{x}^3+2\mathrm{x}^2+\mathrm{x}+3 & \qquad f_{2,2}(\mathrm{x}) &= \mathrm{x}^3+3\mathrm{x}^2+2\mathrm{x}+3 \end{aligned}$$

(see the proof of Lemma 3.13 for the method to calculate each $f_{i,n}$).

Lemma 9.3.

(i) $X^{(1)}_{2,m}X^{(2)}_{2,n}$ *is a V-module if and only if $m=n$ or $m=n+1$.*

(ii) $X^{(1)}_{2,m}X^{(2)}_{2,n}$ *is an S_7-module if and only if $m=n$.*

Proof. Since $X^{(1)}_{2,1}$ is annihilated by $f_{1,1}(s)$, the $\mathbb{F}_2$-space $X^{(1)}_{2,1}$ has basis $\{x_1, x_1^s, x_1^{s^2}\}$ where $x_1 := x^{(1)}_{2,1}=\mathrm{diag}(-1,-1,-1,1,-1,1,1)$. This basis maps to another under action by v. Hence $X^{(1)}_{2,1}$ is a V-module.

Clearly $X^{(1)}_{2,n}X^{(2)}_{2,n}=\Omega_n X_{\{2\}}$ is a V-module; as is $X^{(1)}_{2,n+1}X^{(2)}_{2,n}$, being the inverse image of $X^{(1)}_{2,1}$ under the endomorphism κ^n on $X_{\{2\}}$ that maps x to x^{2^n}.

Suppose that $m<n$ and $X^{(1)}_{2,m}X^{(2)}_{2,n}$ is a V-module. Then $X^{(2)}_{2,1}=\kappa^{n-1}\big(X^{(1)}_{2,m}X^{(2)}_{2,n}\big)$ is a V-module. But $\Omega_1 X_{\{2\}}=X^{(1)}_{2,1}\times X^{(2)}_{2,1}$ is V-indecomposable by Proposition 6.3.

Let $x_2=x^{(1)}_{2,2}=\mathrm{diag}(-\mathrm{i},-\mathrm{i},\mathrm{i},-1,-\mathrm{i},1,1)$. Observe that $x_2^v\notin X^{(1)}_{2,2}$, as x_2^v is not annihilated by $f_{1,2}(s)$. So $X^{(1)}_{2,2}$ is not a V-module. However, if $m>n+1$ and

$X_{2,m}^{(1)} X_{2,n}^{(2)}$ were a V-module, then $X_{2,2}^{(1)} = \kappa^{m-2}\big(X_{2,m}^{(1)} X_{2,n}^{(2)}\big)$ would be one too. This rules out the final possibility for (m,n). □

Definition 9.4. Let $\mathcal{A}^{[V]}$ be the set of $A \in \mathcal{A}$ in degree 7 for which the following hold.

(i) If $A \cap D_{\{7\}} = Y_{j,k,l}$, then either $j \equiv 0 \bmod p-1$, or both $l = 0$ and $j \equiv -1 \bmod p-1$.

(ii) Either $\mathsf{N}_A = \mathsf{N}_A^t$, or $A \cap X_{\{2\}} = X_{2,n+1}^{(2)} X_{2,n}^{(2)}$ for some n and N_A agrees with N_A^t in each row apart from the row for $q = 2$.

Proposition 9.5. *$\mathcal{A}^{[V]}$ is the set of all finite V-submodules of D.*

Since $V \cap \mathrm{S}_6 \cong \mathrm{S}_4$, Lemmas 6.8 and 6.9 give the following.

Lemma 9.6. *$H^1(V, D_{\{q\}}) = 0$ if q is odd.*

Next we carry out some matrix arithmetic.

Lemma 9.7. *If $d \in \mathrm{D}(7,\mathbb{C})$ and $\langle s, vd\rangle \cap D \le X_{2,1}^{(1)}$, then $d^2 = 1$.*

Proof. Let $d = \mathrm{diag}(a_1, \dots, a_7)$. We evaluate the containment of $(vd)^2, (svd)^4, (s^2vd)^3$ in $\Omega_1 D_{\{2\}}$ and $(vd)^2, (svd)^4$ in $\ker f_{1,1}(s)$ to get a system of equations in the a_i whose simultaneous solution implies that each a_i is ± 1. □

Definition 9.8. Let $g_n = \mathrm{diag}(1,1,1,\epsilon_n,1,\epsilon_n^{-1},1)$ and $h_n = \mathrm{diag}(\epsilon_n,\epsilon_n,1,\epsilon_n^{-1},1,1,\epsilon_n^{-1})$ where $\epsilon_n = e^{\pi \mathrm{i}/2^{n-1}}$.

Remark 9.9. The diagonal subgroup of $\langle s, vg_1\rangle$ is $X_2^{(1)}$, and $\langle s, vh_1\rangle \cong V$ is irreducible.

Lemma 9.10. *Let $d \in \mathrm{D}(7,\mathbb{C})$. If $\langle s, vd\rangle \cap D = X_{2,1}^{(1)}$ (resp., $\langle s, vd\rangle \cap D = 1$), then $d \in X_{2,1}^{(1)}$ or $g_1 X_{2,1}^{(1)}$ (resp., $d \in \langle h_1\rangle$).*

Proof. Follows from Lemma 9.7 and calculations similar to those in its proof. □

Definition 9.11. Let

$$\begin{aligned}
\mathcal{V}_0 &= \{\langle s, v, A\rangle \mid A \in \mathcal{A}^{[V]}\},\\
\mathcal{V}_1 &= \textstyle\bigcup_{n\ge 1}\big\{\langle s, vg_n, A\rangle \mid A \in \mathcal{A}^{[V]} \setminus \mathcal{A}^{[S]} \text{ and } A \cap X_{\{2\}}^{(1)} = X_{2,n}^{(1)}\big\},\\
\mathcal{V}_2 &= \textstyle\bigcup_{n\ge 0}\big\{\langle s, vh_{n+1}, A\rangle \mid A \in \mathcal{A}^{[S]} \text{ and } A \cap X_{\{2\}}^{(1)} = X_{2,n}^{(1)}\big\}.
\end{aligned}$$

Then let $\mathcal{V} = \mathcal{V}_0 \cup \mathcal{V}_1 \cup \mathcal{V}_2$.

Theorem 9.12. *A finite subgroup of $\mathrm{M}(7,\mathbb{C})$ with permutation part $\mathrm{SL}(3,2)$ is $D\mathrm{S}_7$-conjugate to a group in $\mathcal{V}$.*

Proof. (Cf. the proof of Theorem 8.11.) By Lemmas 9.2 and 9.6, we consider a finite hub group $G \leq VX_{\{2\}}$ with $\phi(G) = V$ and $s \in G$. Lemma 9.3 indicates that $\Omega_n X_{\{2\}} \leq D \cap G \leq \Omega_{n+1} X_{\{2\}}$ for some n.

Let κ be the group endomorphism of $\mathrm{S}_7 X_{\{2\}}$ that squares elements of $X_{\{2\}}$ and is the identity on S_7. If $G \cap D = X^{(1)}_{2,n+1} X^{(2)}_{2,n}$ then $\kappa^n(G) \cap D = X^{(1)}_{2,1}$. By Lemma 9.10, $\kappa^n(G) = VX^{(1)}_{2,1}$ or $\langle s, vg_1 \rangle$. The preimages of these groups under κ^n are in $\mathcal{V}_0 \cup \mathcal{V}_1$.

Suppose that $G \cap D = \Omega_n X_{\{2\}}$. By Lemma 9.10, $\kappa^n(G)$ is then V or $\langle s, vh_1 \rangle$. Hence $G \in \mathcal{V}_0 \cup \mathcal{V}_2$. $\square$

Lemma 9.13. *$G \in \mathcal{V}$ is irreducible if and only if $G \notin \mathcal{V}_0$ or $G \cap D \nleq Z$.*

Proof. Suppose that $G \in \mathcal{V}_1 \cup \mathcal{V}_2$ and $G \cap D \leq Z$. Then $G \in \mathcal{V}_2$ by Definition 9.11, and we know that $\langle s, vh_1 \rangle \leq G$ is irreducible. $\square$

Definition 9.14. Let $\mathcal{V}^*$ be the sublist of $\mathcal{V}$ that excludes all members of $\mathcal{V}_0$ with scalar diagonal subgroup.

Theorem 9.15. *$\mathcal{V}^*$ is a classification of the finite irreducible subgroups of* $\mathrm{M}(7, \mathbb{C})$ *with permutation part* $\mathrm{SL}(3, 2)$.

Proof. To prove irredundancy of $\mathcal{V}^*$, suppose that $G \in \mathcal{V}_0$ and $H \in \mathcal{V}_1 \cup \mathcal{V}_2$ are $D\mathrm{S}_7$-conjugate, hence DV-conjugate (as $N_{\mathrm{S}_7}(V) = V$), with the same diagonal subgroup A. Let $A \cap X^{(1)}_{\{2\}} = X^{(1)}_{2,n}$. Then there is $d \in \mathrm{D}(7, \mathbb{C})$ such that $[v, d]b \in A$ where $b = g_n$ ($n \geq 1$) or h_{n+1} ($n \geq 0$). Since the last two (and fourth) diagonal entries of $[v, d]$ are 1s, b cannot be h_{n+1}. Also, $\kappa^{n-1}([v, d]g_n) \notin X^{(1)}_{2,1}$ for any d. $\square$

9.2. **Degree** 11**.** There are two non-isomorphic permutation parts of degree 11, each of which is is self-normalizing in $\mathrm{Sym}(11)$.

Definition 9.16. Let w_1, w_2 be the permutation matrices corresponding respectively to $(1, 7)(2, 3)(4, 8)(5, 9)$, $(1, 3)(2, 8)(4, 7)(5, 6) \in \mathrm{Sym}(11)$. Then let $P = \langle s, w_1 \rangle$ and $Q = \langle s, w_2 \rangle$.

In fact $P \cong \mathrm{PSL}(2, 11)$, $Q \cong M_{11}$, and $P \leq Q$. For both groups, $\pi = \{2, 3, 5\}$.

Lemma 9.17. *If $q \neq 3$ then the finite P-submodules of $D_{\{q\}}$ are S_{11}-modules.*

Proof. For $q \notin \{3, 5\}$, cf. the proof of Lemma 9.2. Inspecting the actions of $f_{1,1}(s)$ and $f_{2,1}(s)$ on $(x^{(1)}_{5,1})^{w_1}$ and $(x^{(2)}_{5,1})^{w_1}$, we see that $X^{(1)}_{5,1}$ and $X^{(2)}_{5,1}$ are not P-modules. Thus $\Omega_1 X_{\{5\}}$ is irreducible. $\square$

Lemma 9.18. *$X^{(1)}_{3,m} X^{(2)}_{3,n}$ is a P-module if and only if $n = m$ or $n = m + 1$.*

Proof. Cf. the proof of Lemma 9.3; $X_{3,1}^{(2)}$ is a P-module, while $X_{3,2}^{(2)}$ is not. □

Lemmas 9.17 and 9.18 inform the next definition.

Definition 9.19. Let $\mathcal{A}^{[P]}$ be the set of $A \in \mathcal{A}$ in degree 11 for which the following hold.

(1) If $A \cap D_{\{p\}} = Y_{j,k,l}$, then either $j \equiv 0 \bmod p-1$, or both $l = 0$ and $j+1 \equiv 0 \bmod p-1$.
(2) Either $\mathsf{N}_A = \mathsf{N}_A^t$, or $A \cap X_{\{3\}} = X_{3,n}^{(1)} X_{3,n+1}^{(2)}$ for some $n \geq 0$ and N_A agrees with N_A^t in each row apart from the row for $q = 3$.

Moving between $\mathcal{A}^{[V]}$ and $\mathcal{A}^{[P]}$, the roles of $X_{q,*}^{(1)}$ and $X_{q,*}^{(2)}$ are switched as the critical prime q switches between 2 and 3. The Hasse diagram of the T-submodule lattice of $X_{\{q\}}$ is a zig-zag chain.

Proposition 9.20.

(i) *$\mathcal{A}^{[P]}$ is the set of all finite P-submodules of D.*
(ii) *$\mathcal{A}^{[S]}$ is the set of all finite Q-submodules of D.*

Proof. Part (ii) follows from part (i): $P \leq Q$, and $X_{3,n}^{(1)} X_{3,n+1}^{(2)}$ is not a Q-module because $(x_{3,1}^{(2)})^{w_2} \notin X_{3,1}^{(2)}$. □

Since $P \cap \mathrm{S}_{10} \cong \mathrm{A}_5$ and $Q \cap \mathrm{S}_{10} \cong \mathrm{A}_6 \cdot 2$, we deduce the following.

Lemma 9.21.

(i) $H^1(P, D_{\{q\}}) = 0$ *for all primes q.*
(ii) $H^1(Q, D_{\{q\}}) = 0$ *for odd primes q, and $H^1(Q, X_{\{2\}}) = C_2$.*

Lemma 9.22. *If G is a finite subgroup of $\mathrm{M}(11, \mathbb{C})$ with permutation part P, then G is D-conjugate to $P.(G \cap D)$.*

Proof. By Proposition 6.6, Lemma 6.7 (with $T = \mathrm{S}_{11}$), and Lemma 9.21 (i), we may suppose that $G \cap D \in \mathcal{A}^{[P]} \setminus \mathcal{A}^{[S]}$. Let W be the largest S_{11}-module in $G \cap D_\pi$, i.e., $(G \cap D_\pi)/W \cong A := X_{3,1}^{(2)}$. Then $D_\pi/W \cong D_\pi$ by Lemma 6.7, so that $D_\pi/(G \cap D_\pi) \cong D_\pi/A$. The short exact sequence

$$1 \to A \to D_\pi \to D_\pi/A \to 1$$

gives rise to the fragment

$$H^1(P, D_\pi) \to H^1(P, D_\pi/(G \cap D_\pi)) \to H^2(P, A)$$

of a long exact sequence (see [32, p. 573]). Since $H^1(P, D_\pi) = H^2(P, A) = 0$ by Lemma 9.21 (i) and [26, p. 229], the proof is complete by Proposition 6.6. □

Theorem 9.23. *The set of all PA where $A \in \mathcal{A}^{[P]}$ is non-scalar is a classification of the finite irreducible subgroups of* $\mathrm{M}(11, \mathbb{C})$ *with permutation part* $\mathrm{PSL}(2, 11)$.

Proof. Let $A, B \in \mathcal{A}^{[P]}$. If $A \le Z$ then the split extension $A \rtimes P$ is reducible. If PA and PB are $\mathrm{GL}(11, \mathbb{C})$-conjugate, then $A = B$ by Theorems 2.9 and 2.10, because $N_{\mathrm{S}_{11}}(P) = P$. □

To conclude degree 11, we list the groups with permutation part M_{11}.

Definition 9.24. Let $d_n = \mathrm{diag}(\epsilon_n, \epsilon_n^{-1}, \epsilon_n^{-1}, 1, \epsilon_n^{-1}, \epsilon_n, 1, \epsilon_n, 1, 1, 1)$ where $\epsilon_n = e^{\pi \mathrm{i}/2^{n-1}}$. Define $\mathcal{Q}$ to be the set of groups $\langle s, w_2, A\rangle$ and $\langle s, w_2 d_{n+1}, A\rangle$ for $A \in \mathcal{A}^{[S]}$ such that $A \cap X_{\{2\}} = \Omega_n X_{\{2\}}$, for all $n \ge 0$.

Theorem 9.25. *The subset of $\mathcal{Q}$ that excludes (only) the groups $\langle s, w_2, A\rangle$, where $A \le Z$, is a classification of the finite irreducible subgroups of* $\mathrm{M}(11, \mathbb{C})$ *with permutation part M_{11}.*

Proof. Let G be a hub group in $QX_{\{2\}}$ (by way of Lemma 9.21 (ii), Proposition 6.6, and Lemma 6.7). Repeated squaring on G reduces to Q or $\langle s, w_2 d_1\rangle$, the only copies of M_{11} in $QX_{\{2\}}$ up to conjugacy (see Lemma 9.21 (ii)). These have preimages in $\mathcal{Q}$.

Since $\langle s, w_2 d_1\rangle$ is irreducible, the reducible groups in $\mathcal{Q}$ are the QA with A scalar.

Suppose that $A \cap X_{\{2\}} = \Omega_n X_{\{2\}}$ and $G = QA$ is DQ-conjugate, hence D-conjugate, to $\langle s, w_2 d_{n+1}, A\rangle$. Then there is a diagonal matrix b such that $b^{1-sw_2} = d_{n+1} \in A \cap X$. However, b^{1-sw_2} has diagonal entries of order 2^{n+1}. □

9.3. **Degree 23.** Let $p = 23$. A non-compulsory transitive subgroup of $\mathrm{P}(23)$ is conjugate to the group $Q \cong M_{23}$ generated by s and

$$(1,3)(4,19)(5,17)(6,9)(7,8)(10,16)(12,15)(13,18).$$

(We recycle the notation Q from Section 9.2.)

Definition 9.26. Let $\mathcal{A}^{[Q]}$ be the sublist of $A \in \mathcal{A}$ in degree 23 for which the following hold.

(1) If $A \cap D_{\{p\}} = Y_{j,k,l}$, then either $j \equiv 0 \mod p-1$, or both $l = 0$ and $j + 1 \equiv 0 \mod p-1$.
(2) Either $\mathsf{N}_A = \mathsf{N}_A^t$, or $A \cap X_{\{2\}} = X_{2,n+1}^{(1)} X_{2,n}^{(2)}$ for some $n \ge 0$ and $\mathsf{N}_A^t = \mathsf{N}_A$ apart from the row for $q = 2$.

Proofs of the next three results are left as exercises.

Lemma 9.27. $\mathcal{A}^{[Q]}$ *is the set of all finite Q-submodules of* $\mathrm{D}(23, \mathbb{C})$.

Lemma 9.28. *If q is prime then $H^1(Q, D_{\{q\}}) = 0$.*

Theorem 9.29. *The set of all AQ for non-scalar $A \in \mathcal{A}^{[Q]}$ is a classification of the finite irreducible subgroups of $\mathrm{M}(23, \mathbb{C})$ with permutation part M_{23}.*

10. Overview

We have completely and irredundantly classified up to conjugacy in $\mathrm{GL}(p, \mathbb{C})$ all finite irreducible monomial subgroups that

- are solvable;
- have permutation part containing $\mathrm{Alt}(p)$;
- are non-solvable in degrees $p \in \{7, 11, 23\}$.

Hence, we have classified the groups for $p \leq 11$, $p = 23$, and the infinitely many p not of the form $(q^d - 1)/(q - 1)$ where q is a prime power.

Our methodology may be used to settle all prime degrees $p < 31$. If $p = 19$ or 29 then the permutation part T is compulsory. If $p = 13$ or 17 then the non-compulsory T are projective, with one or three possible isomorphism types, respectively.

A hermetic classification of the finite irreducible subgroups of $\mathrm{M}(p, \mathbb{C})$ for arbitary prime p is obstructed by a lack of solutions to the T-module listing problem (in $D_{\{p\}'}$) and the extension problem for projective T. We pose some conjectures, suggested by existing evidence, whose resolution might aid in closing these gaps. Note that [16] is also stymied by the projective family case, there being a question about 'basic subgroups' of 'height' greater than 1 [16, p. 366].

Let T be a non-solvable transitive subgroup of $\mathrm{Sym}(p)$.

Conjecture 10.1. Every finite T-submodule of $D_{\{p\}'}$ is an $N_{\mathrm{Sym}(p)}(T)$-submodule.

Suppose that $\mathrm{SL}(d, q) \trianglelefteq T \leq \Sigma\mathrm{L}(d, q)$. If q is prime then $N_{\mathrm{Sym}(p)}(T) = T$. The only p such that $5 < p < 10^6$ and $p = (q^d - 1)/(q - 1)$ with q composite are $p = 17$, 73, 257, 757, 65537, and 262657. Since finite $\mathrm{SL}(2, 16)$-submodules of $\mathrm{D}(17, \mathbb{C})$ are $\mathrm{Sym}(17)$-modules (cf. the proof of Lemma 9.2), the smallest degree at which Conjecture 10.1 could fail is 73. This conjecture has a bearing on the conjugacy problem (see Theorems 2.9 and 2.10).

Conjecture 10.2. Every finite T-submodule of D has the same number of T-extensions in $\widetilde{\mathrm{M}}(p, \mathbb{C})$ up to $\widetilde{\mathrm{M}}(p, \mathbb{C})$-conjugacy.

The number n_T in Conjecture 10.2 is 2, 1, 2, 2, 1, 2, 1 for $T = \mathrm{S}_p$, A_p ($p > 5$), A_5, $\mathrm{SL}(3, 2)$, $\mathrm{PSL}(2, 11)$, M_{11}, M_{23}, respectively. In degrees $p \in \{13, 17\}$, the conjecture is true for $T = \mathrm{SL}(3,3)$ and $\mathrm{SL}(2,16)$, with $n_T = 2$ and 4, respectively; we suppress the proofs. Surjective endomorphisms of TD_π that act identically on T (e.g., denoted as powers of κ when $p = 7$ and $T = V$) were used to validate Conjecture 10.2 in the cases so far examined. Such maps need not always exist: it can be shown that there are none for $T \cong \mathrm{SL}(5,2)$. However, another pattern emerges from the body of results about $X_{\{q\}}$ for $p \le 31$ and $q \neq p$.

Conjecture 10.3. Every indecomposable T-submodule of D is uniserial.

Rather than pursuing such conjectures to ever higher degrees, it seems more fruitful to classify primitive groups of moderate prime degree. The non-solvable finite primitive subgroups of $\mathrm{SL}(p,\mathbb{C})$ are listed up to isomorphism in [15]. Our ultimate goal is a (complete, irredundant, explicit) classification of all finite irreducible subgroups of $\mathrm{GL}(p,\mathbb{C})$ for $p \le 11$ (at least). The next section begins this work.

11. Finite complex linear groups of degrees 2 and 3

Some material in this section pertaining to finite primitive subgroups of $\mathrm{SL}(2,\mathbb{C})$ and $\mathrm{SL}(3,\mathbb{C})$ is common knowledge, tracing back to old classifications referenced in Section 1. A convenient source is [29, Chapters X, XII].

The following easy lemma and its corollary assist in irredundancy proofs.

Lemma 11.1. *Let G be a finite irreducible subgroup of $\mathrm{GL}(n,\mathbb{F})$. Then $\mathrm{Aut}(G)$ has a natural action on the set of equivalence classes $[\rho]$ of faithful irreducible representations $\rho \to \mathrm{GL}(n,\mathbb{F})$, defined by $[\rho]\theta = [\rho \circ \theta]$. Under this action,*

(i) $\mathrm{Stab}_{\mathrm{Aut}(G)}([\rho]) \cong N_{\mathrm{GL}(n,\mathbb{F})}(\rho(G))/C_{\mathrm{GL}(n,\mathbb{F})}(\rho(G))$;

(ii) *the orbits are in one-to-one correspondence with the $\mathrm{GL}(n,\mathbb{F})$-conjugacy classes of all irreducible subgroups of $\mathrm{GL}(n,\mathbb{F})$ isomorphic to G.*

Corollary 11.2. *Let G be a finite absolutely irreducible subgroup of $\mathrm{GL}(n,\mathbb{F})$ that is self-normalizing in $\mathrm{GL}(n,\mathbb{F})$ modulo scalars. If there are precisely $|\mathrm{Out}(G)|$ inequivalent faithful absolutely irreducible representations of G in $\mathrm{GL}(n,\mathbb{F})$, then every absolutely irreducible subgroup of $\mathrm{GL}(n,\mathbb{F})$ isomorphic to G is conjugate to G.*

11.1. **Degree 2.**

Some of our generators for the primitive groups in degree 2 are taken from [29, §§102–103]. The others are in $D_{\{p\}}$; see Section 3.1.1.

Definition 11.3. Let

$$a = \tfrac{1}{2}\begin{bmatrix} \mathrm{i}-1 & \mathrm{i}-1 \\ \mathrm{i}+1 & -\mathrm{i}-1 \end{bmatrix}, \qquad b = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1+\mathrm{i} & 0 \\ 0 & 1-\mathrm{i} \end{bmatrix}, \qquad c = \tfrac{1}{2}\begin{bmatrix} \mathrm{i} & \lambda_1-\lambda_2\mathrm{i} \\ -\lambda_1-\lambda_2\mathrm{i} & -\mathrm{i} \end{bmatrix},$$

where $\lambda_1 = \frac{1-\sqrt{5}}{2}$ and $\lambda_2 = \frac{1+\sqrt{5}}{2}$.

Theorem 11.4.

(i) *A finite subgroup G of* $\mathrm{GL}(2,\mathbb{C})$ *is (irreducible) primitive if and only if* $G \cap \mathrm{D}(2,\mathbb{C}) = Z(G)$ *has even order and* $G/Z(G)$ *is isomorphic to* $\mathrm{Alt}(4)$ *or* $\mathrm{Sym}(4)$ *or* $\mathrm{Alt}(5)$.

(ii) *Let $n \geq 2$ be an even integer.*
- *For $K = \mathrm{Alt}(4)$ and $K = \mathrm{Sym}(4)$, there are precisely two conjugacy classes of groups $G \leq \mathrm{GL}(2,\mathbb{C})$ such that $|Z(G)| = n$ and $G/Z(G) \cong K$. These have representatives $\langle a, x_4, z_n \rangle$, $\langle az_{3n}, x_4 \rangle$ when $K = \mathrm{Alt}(4)$, and $\langle a, b, z_n \rangle$, $\langle a, bz_{2n}, z_n \rangle$ when $K = \mathrm{Sym}(4)$.*
- *Every subgroup of* $\mathrm{GL}(2,\mathbb{C})$ *with center of order n and central quotient* $\mathrm{Alt}(5)$ *is conjugate to $\langle a, c, x_4, z_n \rangle$.*

Proof. The proofs of parallel statements in [22, Theorem 5.4] and [23, Theorems 5.8, 5.11] for non-modular absolutely irreducible primitive groups transfer with minor adjustments. There is a finite primitive group $H \leq \mathrm{SL}(2,\mathbb{C})$ such that $GZ = HZ$ and so $G/Z(G) \cong H/Z(H)$. The possible isomomorphism types of $H/Z(H)$ are identified in [29, §§ 102–103]. We solve central extension problems for subgroups of $\mathrm{GL}(2,\mathbb{C})$ using standard 2-cohomology to prove completeness. □

Theorem 11.5. *The union of $\mathcal{L}_0$ as in Theorem 4.9 and the set of all groups listed in Theorem 11.4 (ii) as n ranges over the positive even integers is a classification of the finite irreducible (i.e., finite non-abelian) subgroups of* $\mathrm{GL}(2,\mathbb{C})$.

11.2. **Degree 3.**

Theorem 11.6. *Let G be a finite solvable primitive subgroup of* $\mathrm{GL}(3,\mathbb{C})$.

(i) *$G \cap \mathrm{D}(3,\mathbb{C}) = Z(G)$ has order divisible by 3.*

(ii) *$G/Z(G) \cong E_H := (C_3 \times C_3) \rtimes H$ where H is C_4 or Q_8 (the quaternion group of order 8) or* $\mathrm{SL}(2,3)$.

(iii) *For $n \equiv 0 \bmod 3$, denote by $m_{n,H}$ the number of* $\mathrm{GL}(3,\mathbb{C})$*-conjugacy classes of G such that $|Z(G)| = n$ and $G/Z(G) \cong E_H$. If $H = Q_8$ then $m_{n,H} = 2$. If H is C_4 or* $\mathrm{SL}(2,3)$ *then $m_{n,H} = 3$.*

Proof. Once more we appeal to our proofs of these results for non-modular absolutely irreducible primitive groups: see [23, § 6.4]. □

We give a more detailed version of Theorem 11.6. The generating sets below are transcribed from those in Theorems 6.22–6.24 and Corollary 6.26 of [23] (deleting redundant generators).

Theorem 11.7. *Let* $n \equiv 0 \bmod 3$. *Define*

$$u = \frac{1}{\epsilon - \epsilon^2}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{bmatrix} \quad \text{and} \quad u' = \frac{1}{\epsilon - \epsilon^2}\begin{bmatrix} 1 & \epsilon & \epsilon \\ \epsilon^2 & \epsilon & \epsilon^2 \\ \epsilon^2 & \epsilon^2 & \epsilon \end{bmatrix}$$

where $\epsilon = e^{2\pi \mathrm{i}/3}$. *Up to conjugacy, the finite solvable primitive subgroups of* $\mathrm{GL}(3, \mathbb{C})$ *with center of order* n *and central quotient* E_H *are as follows.*

(i) *For* $H = C_4$:

$$\begin{array}{ll} \langle s, u, z_n\rangle & \text{all } n \\ \left.\begin{array}{l} \langle s, -u, z_n\rangle \\ \langle s, \mathrm{i}u, z_n\rangle \end{array}\right\} & n \text{ odd} \\ \left.\begin{array}{l} \langle s, z_{4n}u, z_n\rangle \\ \langle s, z_{4n}^2 u, z_n\rangle \end{array}\right\} & n \equiv 0 \bmod 4 \\ \left.\begin{array}{l} \langle s, \mathrm{i}u, z_n\rangle \\ \langle s, \sqrt{\mathrm{i}}u, z_n\rangle \end{array}\right\} & n \equiv 2 \bmod 4. \end{array}$$

(ii) *For* $H = Q_8$:

$$\begin{array}{ll} \langle s, u, u', z_n\rangle & \\ \langle s, u, -u', z_n\rangle & n \text{ odd only} \\ \langle s, uz_{2n}, u', z_n\rangle & n \text{ even only}. \end{array}$$

(iii) *For* $H = \mathrm{SL}(2,3)$: $\langle u, x_{27}, z_n\rangle$, $\langle u, z_{3n}x_{27}, z_n\rangle$, $\langle u, z_{3n}^2 x_{27}, z_n\rangle$.

It would be pleasing to have classifications of finite solvable primitive subgroups of $\mathrm{GL}(p, \mathbb{C})$ for larger p.

The finite non-solvable primitive subgroups of $\mathrm{SL}(3, \mathbb{C})$ were also listed by Blichfeldt [4]. We fill out this listing to all of $\mathrm{GL}(3, \mathbb{C})$ via the techniques employed in degree 2 to prove Theorem 11.4.

Definition 11.8. Let

$$a' = \frac{1}{2}\begin{bmatrix} -1 & \mu_2 & \mu_1 \\ \mu_2 & \mu_1 & -1 \\ \mu_1 & -1 & \mu_2 \end{bmatrix} \quad \text{and} \quad b' = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -\epsilon^2 \\ 0 & -\epsilon & 0 \end{bmatrix},$$

where $\mu_1 = \frac{-1+\sqrt{5}}{2}$, $\mu_2 = \frac{-1-\sqrt{5}}{2}$, and $\epsilon = e^{2\pi \mathrm{i}/3}$. Let c' be the 3×3 back-circulant matrix whose first row is $\frac{1}{\sqrt{-7}}\,[\omega^4 - \omega^3, \omega^2 - \omega^5, \omega - \omega^6]$ where $\omega = e^{2\pi \mathrm{i}/7}$.

Theorem 11.9. *A finite non-solvable subgroup G of $\mathrm{GL}(3,\mathbb{C})$, with center of order n, is primitive if and only if G is $\mathrm{GL}(3,\mathbb{C})$-conjugate to one of*

(i) $\langle s, \mathrm{diag}(1,-1,-1), a', z_n\rangle \cong \mathrm{Alt}(5) \times Z(G)$;

(ii) $\langle s, \mathrm{diag}(1,-1,-1), a', b', z_n\rangle$ *for* $n \equiv 0 \bmod 3$*, containing* $3 \cdot \mathrm{Alt}(6)$ *and with central quotient* $\mathrm{Alt}(6)$;

(iii) $\langle \mathrm{diag}(\omega, \omega^2, \omega^4), c', z_n\rangle \cong \mathrm{PSL}(2,7) \times Z(G)$.

Proof. The possible isomorphism types of central quotient, and the matrix generators, are apparent from [29, pp. 250–251].

We sketch a proof of (i) only. Let G be a finite subgroup of $\mathrm{GL}(3,\mathbb{C})$ such that $G/Z(G) \cong \mathrm{A}_5$. Since $|H^2(\mathrm{A}_5, Z(G))| \leq 2$, and the Schur cover $\mathrm{SL}(2,5)$ of A_5 has no faithful irreducible ordinary representation of degree 3, G must split over its center. Also, $\mathrm{GL}(3,\mathbb{C})$ does not contain a subgroup with central quotient S_5. The hypotheses of Corollary 11.2 are therefore satisfied. Direct computation shows that $\langle s, \mathrm{diag}(1,-1,-1), a'\rangle \cong \mathrm{A}_5$. □

Theorem 11.10. *The union of $\mathcal{L}^* \cup \mathcal{M}^*$ for $p = 3$ (see Theorem 5.9) together with the set of all groups listed in Theorems 11.7 and 11.9 is a classification of the finite irreducible subgroups of* $\mathrm{GL}(3,\mathbb{C})$.

12. VERIFICATION AND ACCESS TO THE LISTS

We implemented our classifications in MAGMA: see [24]. The input is a positive integer m and a prime p dividing m; the output is a list of irreducible monomial subgroups of $\mathrm{GL}(p,\mathbb{C})$ of order m up to $\mathrm{GL}(p,\mathbb{C})$-conjugacy and their labels. The projective family is implemented only for $p \leq 11$. Other groups are returned for all input m and p.

Each output group G is given by a generating set of monomial matrices over a cyclotomic field determined by m. Currently, such fields can be realized up to size 2^{30} in MAGMA. Our default is the 'sparse' option. An isomorphic copy of G defined over a finite field may be constructed as in [13, § 4.3], and then we may use other algorithms for finite matrix groups to study G.

Hensel lifting (see Lemma 3.13) is done using MAGMA intrinsic functions. We could avoid p-adic polynomial arithmetic by computing over residue rings $\mathbb{Z}/q^n\mathbb{Z}$ (for n and primes q determined by m).

We consider briefly the cost of setting up the groups of order m in $\mathrm{M}(p,\mathbb{C})$. Timings depend on m, the number of prime factors of m, and v (see Notation 3.15). For many orders, setup takes just a few CPU seconds. More expensive examples include those where $m = pq$ for a prime q of order 1 modulo p. In Table 2, we state the CPU time in seconds taken to construct representatives of all t classes of order at most m for degrees 3 and 5. We used MAGMA V2.25-2 on a 2.6GHz machine.

m	p	t	Time	p	t	Time
2000	3	2229	28	5	373	7
4000	3	4994	206	5	850	54
6000	3	7943	778	5	1328	210
8000	3	10993	2033	5	1892	525
10000	3	14131	4711	5	2445	1089

TABLE 2. Setting up all t classes of order at most m in $\mathrm{M}(p, \mathbb{C})$

Conjugacy class representatives for all finite irreducible subgroups of $\mathrm{GL}(2, \mathbb{C})$ and $\mathrm{GL}(3, \mathbb{C})$ are also available.

12.1. **Checking correctness.** Much data about the groups is routinely corroborated using MAGMA. We can test whether a finite $G \leq \mathrm{GL}(p, \mathbb{C})$ is (absolutely) irreducible. By exploiting the isomorphic copy of G defined over a finite field, we can check $|G|$ and other group-theoretic properties, such as the isomorphism type of $G/Z(G)$. We verified claims for solvable groups of orders $m \leq 10^4$ and all p dividing m. Non-solvable groups were checked for $p \leq 11$ and up to order 10^6.

Lemma 11.1 (ii) underpins a rudimentary but effective correctness testing procedure, which we now summarize.

(1) Fix $m > 1$ and a prime p dividing m.
(2) List the monomial groups of order m and degree p from our implementation.
(3) Partition this list by isomorphism.
(4) For each isomorphism type G, use the algorithm of [7] to construct its inequivalent faithful irreducible monomial representations in $\mathrm{GL}(p, \mathbb{C})$. Compute the number of $\mathrm{Aut}(G)$-orbits in the set of equivalence classes.
(5) If all groups of order m are known, then apply step (4) to each.

If the lists produced in steps (3) and (4) coincide for every isomorphism type, then we have verified that the output from step (2) is irredundant. If the list produced in step (5) also coincides, then the output is complete. For non-solvable G, the algorithm of [7] constructs only those representations defined over $\mathbb{Q}$, so correlation between lists is more limited.

In step (5), we use the following criterion to isolate monomial groups.

Lemma 12.1. *A finite irreducible solvable subgroup of* $\mathrm{GL}(p, \mathbb{C})$ *is monomial if and only if it has a non-central abelian normal subgroup.*

Note that a finite irreducible monomial subgroup of $\mathrm{GL}(p, \mathbb{C})$ is not isomorphic to any primitive subgroup of $\mathrm{GL}(p, \mathbb{C})$ [22, Theorem 2.15].

We applied steps (2), (3), and (4) of the correctness test to solvable monomial groups of order at most 10000. The SMALLGROUPS library [3] contains the groups of order at most 2000 (excluding 2^{10}); step (5) was applied to all. We thereby reconciled our results with the classification in [8] of the finite irreducible p-subgroups of $\mathrm{GL}(p, \mathbb{C})$, and that in [16] of the finite irreducible subgroups of $\mathrm{SL}(p, \mathbb{C}) \cap \mathrm{M}(p, \mathbb{C})$.

An (obvious) variant of the procedure was used to check accuracy of the primitive group lists from Section 11.

12.2. **The number of conjugacy classes of monomial groups.** Our implementation can simply *count* the $\mathrm{GL}(p, \mathbb{C})$-conjugacy classes of irreducible subgroups of $\mathrm{M}(p, \mathbb{C})$ having order m. Since neither fields nor generators are constructed, this number is computed quickly, even for large m.

As an illustration, we counted the conjugacy classes of solvable groups of order m up to 10^6 and all p dividing m. We did likewise for non-solvable groups in degrees $p \leq 11$. Table 3 shows the orders with the most conjugacy classes (solvable groups are on the left).

Order	No. classes
$2^6 \cdot 3^4 \cdot 5^2 \cdot 7$	684
$2^4 \cdot 3^4 \cdot 7^2 \cdot 13$	648
$2^7 \cdot 3^4 \cdot 7 \cdot 13$	640
$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$	621
$2^6 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$	620
$2^4 \cdot 3^3 \cdot 7 \cdot 13 \cdot 19$	588
$2^8 \cdot 3^4 \cdot 5 \cdot 7$	585
$2^6 \cdot 3^5 \cdot 7^2$	573
$2^7 \cdot 3^3 \cdot 5 \cdot 7^2$	568
$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	564

Order	No. classes
$2^4 \cdot 3 \cdot 5^6$	25
$2^3 \cdot 3 \cdot 5^6$	25
$2^{11} \cdot 3^2 \cdot 5 \cdot 7$	17
$2^{13} \cdot 3 \cdot 5 \cdot 7$	16
$2^{12} \cdot 3 \cdot 5 \cdot 7$	16
$2^{10} \cdot 3^3 \cdot 5 \cdot 7$	15
$2^{10} \cdot 3^2 \cdot 5 \cdot 7$	15
$2^{11} \cdot 3 \cdot 5 \cdot 7$	14
$2^{16} \cdot 3 \cdot 5$	13
$2^{15} \cdot 3 \cdot 5$	13

TABLE 3. Monomial group orders with the most $\mathrm{GL}(p, \mathbb{C})$-conjugacy classes

Acknowledgments. We thank Alla Detinko for astute comments. The second and third authors were supported by Marsden Fund of New Zealand grant UOA 1626; and by the Hausdorff Research Institute for Mathematics, as participants in the 2018 Trimester in Logic and Group Theory.

References

1. Z. Bácskai, Finite irreducible monomial groups of small prime degree. PhD thesis, Australian National University, 1999.
2. P. T. Bateman and R. M. Stemmler, Waring's Problem for algebraic number fields and primes of the form $(p^r - 1)/(p^d - 1)$. Illinois J. Math. **6** (1962), 142–156.
3. H. U. Besche, B. Eick, and E. A. O'Brien, A millennium project: constructing small groups. *Internat. J. Algebra Comput.* **12** (2002), 623–644.
4. H. F. Blichfeldt, Finite collineation groups. University of Chicago Press, Chicago, 1917.
5. B. Bolt, T. G. Room, and G. E. Wall, On the Clifford collineation, transform and similarity groups. I. J. Austral. Math. Soc. **2** (1961), 60–79.
6. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
7. J. J. Cannon and D. F. Holt, Computing projective indecomposable modules and higher cohomology groups. Exp. Math. **22** (2013), no. 1, 51–59.
8. S. B. Conlon, p-groups with an abelian maximal subgroup and cyclic center. J. Austral. Math. Soc. Ser. A **22** (1976), no. 2, 221–233.
9. S. B. Conlon, Nonabelian subgroups of prime-power order of classical groups of the same prime degree. Group Theory (Proc. Miniconf., Australian Nat. Univ., Canberra, 1975), pp. 17–50, Lecture Notes in Math., vol. 573. Springer, Berlin, 1977.
10. H. J. Coutts, M. Quick, and C. Roney-Dougal, The primitive permutation groups of degree less than 4096. Comm. Algebra **39** (2011), no. 10, 3526–3546.
11. A. S. Detinko, Maximal solvable subgroups of the special linear group over an arbitrary field. Siberian Math. J. **33** (1992), no. 6, 973–979.
12. A. S. Detinko, The classification of irreducible maximal solvable subgroups of classical groups of prime degree over an arbitrary field. PhD thesis, Minsk, 1996.
13. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, Recognizing finite matrix groups over infinite fields. J. Symbolic Comput. **50** (2013), 100–109.
14. J. D. Dixon, Complements of normal subgroups in infinite groups. Proc. London Math. Soc. (3) **17** (1967), 431–446; Corrigenda, ibid. **18** (1968), 768.
15. J. D. Dixon and A. E. Zalesskii, Finite primitive linear groups of prime degree. J. London Math. Soc. (2) **57** (1998), no. 1, 126–134; Corrigendum, ibid. **77** (2008), no. 3, 808–812.
16. J. D. Dixon and A. E. Zalesskii, Finite imprimitive linear groups of prime degree. J. Algebra **276** (2004), no. 1, 340–370.
17. B. Eick and B. Höfling, The solvable primitive permutation groups of degree at most 6560. LMS J. Comput. Math. **6** (2003), 29–39 (electronic).

18. W. Feit, The current situation in the theory of finite simple groups. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, pp. 55–93. Gauthier-Villars, Paris, 1971.
19. W. Feit, The representation theory of finite groups. North-Holland Mathematical Library, 25. North-Holland Publishing Co., Amsterdam-New York, 1982.
20. D. L. Flannery, The finite irreducible linear 2-groups of degree 4. Mem. Amer. Math. Soc. **129** (1997), no. 613.
21. D. L. Flannery, The finite irreducible monomial linear groups of degree 4. J. Algebra **218** (1999), no. 2, 436–469.
22. D. L. Flannery, Irreducible monomial linear groups of degree four over finite fields. Internat. J. Algebra Comput. **14** (2004), no. 3, 253–294.
23. D. L. Flannery and E. A. O'Brien, Linear groups of small degree over finite fields. Internat. J. Algebra Comput. **15** (2005), no. 3, 467–502.
24. D. L. Flannery and E. A. O'Brien, *Monomial*. `https://github.com/eamonnaobrien/Monomial`
25. B. Höfling, Finite irreducible imprimitive nonmonomial complex linear groups of degree 4. J. Algebra **236** (2001), no. 2, 419–470.
26. D. F. Holt and W. Plesken, Perfect groups. Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1989.
27. B. Huppert, Endliche Gruppen. I. Grundlehren der Mathematischen Wissenschaften, 134, Springer-Verlag, Berlin-New York, 1967.
28. B. Huppert and N. Blackburn, Finite groups. II. Grundlehren der Mathematischen Wissenschaften, 242, Springer-Verlag, Berlin-New York, 1982.
29. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, Theory and applications of finite groups. G. E. Stechert & Co., New York, 1938.
30. P. M. Neumann, Transitive permutation groups of prime degree. Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), pp. 520–535. Lecture Notes in Math., vol. 372, Springer, Berlin, 1974.
31. P. M. Neumann, Permutationsgruppen von Primzahlgrad und verwandte Themen. Vorlesungen aus dem Mathematisches Institut Giessen, Heft 5. Mathematisches Institut Giessen, Giessen, 1977.
32. J. J. Rotman, An introduction to homological algebra. Second edition. Universitext. Springer, New York, 2009.
33. R. Schmidt, Subgroup lattices of groups. De Gruyter Expositions in Mathematics, 14. Walter de Gruyter & Co., Berlin, 1994.
34. M. W. Short, The primitive soluble permutation groups of degree less than 256. Lecture Notes in Math., vol. 1519. Springer-Verlag, Berlin, 1992.
35. H.-S. Sim, Metacyclic primitive linear groups. Comm. Algebra **22** (1994), no. 1, 269–278.
36. D. A. Suprunenko, Matrix groups. Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
37. P. H. Tiep and A. E. Zalesskii, Some aspects of finite linear groups: a survey. Algebra, 12. J. Math. Sci. (New York) **100** (2000), no. 1, 1893–1914.
38. A. E. Zalesskii, Linear groups. Algebra, IV, Encyclopaedia Math. Sci., vol. 37, Springer, Berlin, 1993, pp. 97–196.

DEFENCE SCIENCE TECHNOLOGY GROUP, CANBERRA, AUSTRALIA
E-mail address: zoltan.bacskai@defence.gov.au

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND, GALWAY, IRELAND
E-mail address: dane.flannery@nuigalway.ie

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