



Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The number of automorphisms of a monolithic finite group

Jeffrey M. Riedl

Department of Theoretical and Applied Mathematics, University of Akron, Akron, OH 44325-4002, USA

ARTICLE INFO

Article history:

Received 19 March 2009

Available online 8 September 2009

Communicated by Ronald Solomon

Keywords:

Finite groups

p -Groups

Automorphism group

Character theory

ABSTRACT

We develop a general formula for the order of the group of automorphisms $\text{Aut}(G)$ of a monolithic finite group G in terms of information about the complex characters of G and information about how G is embedded as a subgroup of a particular finite general linear group. We show that this formula is applicable to a wide variety of finite p -groups, and we discuss several applications to particular large families of finite p -groups. Finally, we derive a useful consequence of this formula and discuss its application to a classification problem involving finite p -groups.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

Many results concerning the order of the automorphism group $\text{Aut}(G)$ of a finite group G have been published in recent years, particularly in the case where G is a p -group (see [1–5]). In this article we develop a general formula for the order of the automorphism group $\text{Aut}(G)$ of a monolithic finite group G . (A nontrivial finite group is said to be monolithic if it has a unique minimal normal subgroup.) We also discuss some applications. This formula (Theorem A) expresses the order of $\text{Aut}(G)$ purely in terms of what may be considered representation-theoretic information about G . When applying this formula to a group G , one does not deal with or even think about any automorphisms of G . Hence the method for computing the order of $\text{Aut}(G)$ presented here is indirect.

In order to state our main results, we need to introduce some definitions. For each finite group G and field F , we define $\text{mindeg}(G, F)$ to be the smallest positive integer m such that the general linear group $\text{GL}(m, F)$ contains a subgroup that is isomorphic to G . (The existence of m follows from Cayley's Theorem and the fact that for each positive integer n , the subgroup of $\text{GL}(n, F)$ consisting of all permutation matrices is isomorphic to the symmetric group of degree n .) Thus $\text{mindeg}(G, F)$ is the minimal degree among all the faithful F -representations of the group G . For each prime-power q larger than 1, we write $\text{mindeg}(G, q) = \text{mindeg}(G, F)$ where F is the field with q elements.

E-mail address: riedl@uakron.edu.

Definition 1.1. Let G be a monolithic finite group, let q be a prime-power that is relatively prime to the order of G , and let $m = \text{mindeg}(G, q)$. We say that the ordered triple (G, q, m) is a **monolithic triple** in case every faithful irreducible ordinary character of G has degree at least m . Assuming that (G, q, m) is a monolithic triple, we define $\mathcal{F}(G, q)$ to be the set of all faithful irreducible ordinary characters of G of degree m . We say that the monolithic triple (G, q, m) is **good** provided that every value of each character belonging to the set $\mathcal{F}(G, q)$ is a \mathbb{Z} -linear combination of complex $(q - 1)$ st roots of unity.

Before going further, we feel the need to justify Definition 1.1 in a certain sense. First we present an example showing that, in the context of Definition 1.1, the condition that $\text{mindeg}(G, q)$ is a lower bound on the degrees of all the faithful irreducible ordinary characters of G is not an automatic consequence of the definition of $\text{mindeg}(G, q)$. Let G be the dihedral group of order 10, let $q = 7$, and write $m = \text{mindeg}(G, 7)$. For each value $n \in \{1, 2, 3\}$, the general linear group $\text{GL}(n, 7)$ has order not divisible by 5, and hence does not contain any subgroup that is isomorphic to G . Thus $m \geq 4$. Since G has a faithful irreducible ordinary character of degree 2, indeed $(G, 7, m)$ is not a monolithic triple.

Next we present an example showing that not every monolithic triple is good. Let G be the semidihedral group of order 16 and let $q = 3$. Since $\text{GL}(2, 3)$ contains a subgroup that is isomorphic to G , indeed $\text{mindeg}(G, 3) = 2$. The group G has exactly two faithful irreducible ordinary characters, both of degree 2, and so $(G, 3, 2)$ is a monolithic triple. These two characters constitute the set $\mathcal{F}(G, 3)$. In order for this monolithic triple to be good, every value of each of these two characters would have to be an ordinary integer, but in fact this is not the case because $\sqrt{-2}$ is a value of each of these two characters.

We now state our first main result. We call it the Automorphism Counting Formula.

Theorem A. Let (G, q, m) be a good monolithic triple. Let the subgroups H_1, \dots, H_t be representatives for the distinct conjugacy classes of subgroups of $\Gamma = \text{GL}(m, q)$ whose members are isomorphic to G . For each $i \in \{1, \dots, t\}$ write $n_i = |\mathbf{N}_\Gamma(H_i)|$. Then

$$|\mathcal{F}(G, q)| = |\text{Aut}(G)|(q - 1) \sum_{i=1}^t (1/n_i),$$

and $\mathbf{C}_\Gamma(H_i) = \mathbf{Z}(\Gamma)$ has order $q - 1$ for each $i \in \{1, \dots, t\}$. Furthermore, in the special case where $t = 1$ and we write $H = H_1$, we have $|\text{Aut}(G)|(q - 1) = |\mathcal{F}(G, q)| \cdot |\mathbf{N}_\Gamma(H)|$.

Theorem A enables us to compute the cardinality $|\text{Aut}(G)|$ using the cardinalities $|\mathcal{F}(G, q)|$ and $|\mathbf{N}_\Gamma(H_i)|$ for $i \in \{1, \dots, t\}$. In this sense, Theorem A provides a formula for the order of the group of automorphisms $\text{Aut}(G)$ of a monolithic finite group G in terms of information about the complex characters of G and information about how G is embedded as a subgroup of a particular finite general linear group.

The most interesting applications of Theorem A that we have discovered are for large families of p -groups G . For p -groups, the condition of being monolithic is equivalent to the condition that the center of the group is cyclic. Interestingly, for each of the applications of Theorem A that we have discovered so far, we have been able to prove, for the good monolithic triple (G, q, m) under consideration, that the general linear group $\text{GL}(m, q)$ actually has a unique conjugacy class of subgroups whose members are isomorphic to G , and this allows us to apply the simpler version of the conclusion of Theorem A.

Throughout this article we make use of the fact that for any prime p and positive integer e , there exists a prime-power q larger than 1 such that the p -part of $q - 1$ is equal to p^e . In fact a stronger statement is true, as we now explain. Since p^{e+1} and $p^e + 1$ are relatively prime, Dirichlet's theorem on primes in arithmetic progression implies the existence of infinitely many primes q such that $q \equiv p^e + 1 \pmod{p^{e+1}}$, which is equivalent to $q - 1 \equiv p^e \pmod{p^{e+1}}$, which says that $q - 1$ is divisible by p^e but not by p^{e+1} .

We now describe one application of Theorem A to a large family of finite p -groups.

Application 1.2. Let G denote the regular wreath product group $\mathbb{Z}_{p^e} \wr Q$ where p is any prime, e is any positive integer, and Q is any nontrivial finite p -group. Write $|Q| = p^n$ and suppose that $p^{en} \geq 3$. (The condition $p^{en} \geq 3$ excludes only the case where $p = 2$ and $e = n = 1$, for which G is dihedral of order 8.) Let q be an arbitrary prime-power larger than 1 such that the p -part of $q - 1$ is equal to p^e . In [9] we establish that (G, q, p^n) is a good monolithic triple and that the general linear group $\text{GL}(p^n, q)$ has a unique conjugacy class of subgroups whose members are isomorphic to G , and then we apply Theorem A (with $t = 1$) to conclude that $|\text{Aut}(G)| = |\text{Aut}(Q)|(p - 1)p^a$ where $a = 2ep^n - e - 1$.

The regular wreath product groups to which we applied Theorem A in Application 1.2 constitute a large but rather narrow class of monolithic finite p -groups. Our next goal is to demonstrate that the notion of a good monolithic triple (and hence also Theorem A) is applicable to a much wider variety of monolithic finite p -groups. For this purpose, we shall now introduce an important family of iterated wreath product finite p -groups.

Definition 1.3. Let p be any prime and let e be any positive integer. Let $W_1^e(p)$ denote the cyclic group of order p^e . For each integer $n \geq 2$, we recursively define $W_n^e(p)$ as the regular wreath product group $W_n^e(p) = W_{n-1}^e(p) \wr \mathbb{Z}_p$. Thus, for $n \geq 2$, the group $W_n^e(p)$ is the semidirect product $N \rtimes \mathbb{Z}_p$ where N is the direct product of p copies of the group $W_{n-1}^e(p)$, and where \mathbb{Z}_p , the cyclic group of order p , acts via automorphisms on N by regularly permuting these direct factors.

It is well known that for an arbitrary prime p and positive integer n , the group $W_n^1(p)$ is isomorphic to a Sylow p -subgroup of the symmetric group of degree p^n . For any prime p and any positive integers e and n such that $n \geq 2$, it is straightforward to show that the order of the group $W_n^e(p)$ is $p^{\alpha(n)}$ where $\alpha(n) = 1 + p + \cdots + p^{n-2} + ep^{n-1}$. The next two results suggest that the family of groups $W_n^e(p)$ is worthy of attention.

Theorem 1.4. Let q be any prime-power larger than 1 and let p be any prime divisor of $q - 1$. Let p^e denote the p -part of $q - 1$, so that e is a positive integer. Then for every positive integer n , the general linear group $\Gamma = \text{GL}(p^{n-1}, q)$ contains a subgroup P that is isomorphic to $W_n^e(p)$. Furthermore, if $p^e \geq 3$, then P is a Sylow p -subgroup of Γ .

We mention without proof that in the situation of Theorem 1.4, it is actually true that P is a Sylow p -subgroup of Γ iff $p^e \geq 3$. (Theorem 1.4 is probably well known.)

Theorem 1.5. Let G be a finite p -group for some prime p . Let r be any prime such that $r \neq p$ and let F denote the algebraic closure of the field with r elements. Let n be any positive integer. The following conditions are equivalent.

- (a) G is isomorphic to a subgroup of the general linear group $\text{GL}(p^{n-1}, \mathbb{C})$.
- (b) G is isomorphic to a subgroup of the general linear group $\text{GL}(p^{n-1}, F)$.
- (c) G is isomorphic to a subgroup of $W_n^e(p)$ for some positive integer e .

In the following definition we describe a natural way of associating to each monolithic finite group of prime-power order a unique member of the three-parameter family of groups $W_n^e(p)$. In this definition we make use of the well-known fact that if G is any monolithic finite group, then there exists a faithful irreducible ordinary character of G .

Definition 1.6. Let G be an arbitrary monolithic finite p -group for some prime p . We define the positive integer n by letting p^{n-1} denote the minimum degree of all the faithful irreducible ordinary characters of G . Thus G is isomorphic to a subgroup of $\text{GL}(p^{n-1}, \mathbb{C})$. By Theorem 1.5, it follows that G is isomorphic to a subgroup of $W_n^e(p)$ for some positive integer e . Letting e be minimal with the

properties that $p^e \geq 3$ and G is isomorphic to a subgroup of $W_n^e(p)$, we define the ordered pair $\omega(G) = (n, e)$.

The following result establishes that every monolithic finite p -group occurs as the first component of a monolithic triple.

Theorem 1.7. *Let G be an arbitrary monolithic finite p -group for some prime p , and let $\omega(G) = (n, e)$. Let q be any prime-power larger than 1 such that the full p -part of $q - 1$ is equal to p^e . Then (G, q, p^{n-1}) is a monolithic triple.*

Naturally, one would wish to strengthen the conclusion of Theorem 1.7 to say that (G, q, p^{n-1}) is a *good* monolithic triple. We do not know if this stronger conclusion is true in general. However, one can impose certain additional hypotheses that clearly yield this stronger conclusion. In the next two paragraphs we describe two types of such hypotheses. Because these hypotheses are not overly restrictive, the notion of a good monolithic triple (and hence also Theorem A) is applicable to a wide variety of monolithic finite p -groups.

It is well known that the value of an arbitrary ordinary character on a group element of order n is a sum of complex n th roots of unity (see Lemma 2.15 in [7]). Thus, if (G, q, m) is any monolithic triple such that the exponent of the group G is a divisor of $q - 1$, then it is automatically true that this monolithic triple is good. Therefore, in the situation of Theorem 1.7, if the exponent of the group G is a divisor of p^e , then the monolithic triple (G, q, p^{n-1}) is good. In particular, in the situation of Theorem 1.7, if the group G has exponent p , then the monolithic triple (G, q, p^{n-1}) is good.

For an arbitrary finite group G having an abelian normal subgroup N of index m , it is not difficult to show that every irreducible ordinary character χ of G of degree m is induced from a linear character of N , and that χ vanishes off the subgroup N . In this situation, if the abelian subgroup N has exponent dividing $q - 1$, then every value of the restriction of χ to N is a sum of complex $(q - 1)$ st roots of unity, and hence every value of χ is a sum of complex $(q - 1)$ st roots of unity. Thus, if (G, q, m) is any monolithic triple such that G has an abelian normal subgroup of index m that has exponent dividing $q - 1$, then it is automatically true that this monolithic triple is good. Therefore, in the situation of Theorem 1.7, if the group G has an abelian normal subgroup of index p^{n-1} that has exponent dividing p^e , then the monolithic triple (G, q, p^{n-1}) is good.

We now describe another application of Theorem A to a large family of p -groups.

Application 1.8. Let $G = W_n^e(p)$ with $p^e \geq 3$ and $n \geq 2$. Let q be any prime-power larger than 1 such that the p -part of $q - 1$ is equal to p^e . In [10] we establish that (G, q, p^{n-1}) is a good monolithic triple and we show that $|\mathcal{F}(G, q)| = (p - 1)p^{\beta(n)}$ where

$$\beta(n) = (p - 1) \left[\binom{n}{2} + (e - 1)n \right] - (e - 1)(p - 2) - 1.$$

Since $p^e \geq 3$, Theorem 1.4 implies that G is isomorphic to a Sylow p -subgroup of the general linear group $GL(p^{n-1}, q)$, and from this it follows that $GL(p^{n-1}, q)$ has a unique conjugacy class of subgroups whose members are isomorphic to G . Recall that the order of the group $W_n^e(p)$ is $p^{\alpha(n)}$ where $\alpha(n) = 1 + p + \cdots + p^{n-2} + ep^{n-1}$. In [10] we apply Theorem A (with $t = 1$) to conclude that $|\text{Aut}(G)| = (p - 1)^n p^r$ where $r = \alpha(n) + \beta(n) - e$.

We now present the second main result of this article, which is an easy-to-prove consequence of Theorem A. This result (Corollary B) provides an indirect method for establishing, under certain conditions, that a finite general linear group has a unique conjugacy class of subgroups whose members are isomorphic to a given monolithic group.

Corollary B. Let (G, q, m) be a good monolithic triple and write $\mathcal{F} = \mathcal{F}(G, q)$ and $A = \text{Aut}(G)$. Let t denote the number of distinct conjugacy classes of subgroups of $\Gamma = \text{GL}(m, q)$ whose members are isomorphic to G . Let H be any subgroup of Γ that is isomorphic to G , and write $N = \mathbf{N}_\Gamma(H)$ and $C = \mathbf{C}_\Gamma(H)$.

- (a) If $|\mathcal{F}| \cdot |N : C|$ divides $|A|$, then $t = 1$ and $|\mathcal{F}| \cdot |N : C| = |A|$.
- (b) If $|\mathcal{F}| = 1$, then $t = 1$ and N/C is isomorphic to A .

We now describe a significant application of Corollary B. In [11] we classify up to isomorphism the finite p -groups having a faithful irreducible ordinary character of degree p . Using Theorem 1.5, one can show that this is equivalent to classifying up to isomorphism the nonabelian subgroups of $W_2^e(p)$ for an arbitrary prime p and positive integer e such that $p^e \geq 3$. For this classification problem, our approach is to classify up to isomorphism the nonabelian subgroups of a Sylow p -subgroup P of the general linear group $\Gamma = \text{GL}(p, q)$, where q is an arbitrary prime-power larger than 1 such that the full p -part of $q - 1$ is equal to p^e , since Theorem 1.4 implies that P is isomorphic to $W_2^e(p)$. One advantage of this approach is that by computing the conjugacy classes of nonabelian p -subgroups of $\mathbf{N}_\Gamma(P)$, we are able to recognize more pairs of nonabelian subgroups of P as being isomorphic to each other than we would by simply computing the conjugacy classes of nonabelian subgroups of P . We now describe another advantage of this approach. In several situations we encounter nonabelian subgroups L_1 and L_2 of P that appear as if they might be isomorphic to each other, but nevertheless (as we are able to show) are not conjugate subgroups of Γ . In these situations we apply Corollary B to deduce that, for each $i \in \{1, 2\}$, the group Γ has a unique conjugacy class of subgroups whose members are isomorphic to L_i , and this tells us that in fact L_1 is not isomorphic to L_2 . In this way, Corollary B plays an important role in this classification. Furthermore, in the process of obtaining this classification, we establish (using Corollary B in the manner just described) the perhaps surprising fact that every pair of nonabelian p -subgroups of the general linear group Γ that are isomorphic to each other are actually conjugate subgroups of Γ .

In [11], once the classification described above has been completed, we determine the order of the automorphism group $\text{Aut}(H)$ for each group H appearing in the classification. For those groups H of nilpotence class 3 or larger, we compute $|\text{Aut}(H)|$ using Theorem A and another result (Theorem 3.7) that is specifically designed for this application.

In Section 2 we prove Theorem A and Corollary B. In Section 3 we prove Theorems 1.4, 1.5, and 1.7. Using Theorem A to calculate the order of the automorphism group $\text{Aut}(G)$ for a given monolithic triple (G, q, m) requires knowledge of the order of the normalizer of one or more subgroups H in the general linear group $\text{GL}(m, q)$. In Section 4 we establish some results that are helpful for obtaining this information in certain situations. We make use of the results of Section 4 in our applications of Theorem A in [9–11].

Let $\text{Irr}(G)$ denote the set of irreducible ordinary characters of a finite group G .

2. Proofs of Theorem A and Corollary B

We begin with a few basic observations. Suppose that G is a finite group that is isomorphic to some subgroup of the general linear group $\Gamma = \text{GL}(m, F)$, where m is a positive integer and F is a field. If \mathcal{H} is any conjugacy class of subgroups of Γ whose members are isomorphic to G , then the set consisting of all (faithful) F -representations \mathcal{X} of G having the property that $\mathcal{X}(G) \in \mathcal{H}$ is clearly a union of similarity classes of F -representations of G . Furthermore, if either the field F is finite or the characteristic of the field F does not divide $|G|$, then clearly there exist only finitely many distinct conjugacy classes of subgroups of Γ whose members are isomorphic to G . The following result may be regarded as a preliminary version of the Automorphism Counting Formula.

Theorem 2.1. Let F be a field, let m be a positive integer, and let G be a finite group that is isomorphic to some subgroup of the general linear group $\Gamma = \text{GL}(m, F)$.

- (a) Let \mathcal{H} be any conjugacy class of subgroups of Γ whose members are isomorphic to G . Let $\mathcal{S}(\mathcal{H})$ be the set consisting of all the similarity classes of F -representations \mathcal{X} of G of degree m that satisfy $\mathcal{X}(G) \in \mathcal{H}$. Then for each subgroup $H \in \mathcal{H}$, we have $|\text{Aut}(G)| = |\mathbf{N}_\Gamma(H) : \mathbf{C}_\Gamma(H)| \cdot |\mathcal{S}(\mathcal{H})|$.
- (b) Suppose that there exist only finitely many distinct conjugacy classes of subgroups of Γ whose members are isomorphic to G , and let the subgroups H_1, \dots, H_t be representatives for these conjugacy classes. For $i \in \{1, \dots, t\}$, write $n_i = |\mathbf{N}_\Gamma(H_i)|$ and $c_i = |\mathbf{C}_\Gamma(H_i)|$. Let \mathcal{S} be the set of all similarity classes of faithful F -representations of G of degree m . Then

$$|\mathcal{S}| = |\text{Aut}(G)| \sum_{i=1}^t (c_i/n_i).$$

To exhibit an example showing that the hypothesis of part (b) need not hold, we mention without proof that if F is the algebraic closure of the field with 2 elements, then the group $\text{GL}(2, F)$ has infinitely many conjugacy classes of subgroups that are noncyclic of order 4. We are grateful to Geoff Robinson for bringing this fact to our attention.

Proof. (a) Let $H \in \mathcal{H}$. Write $N = \mathbf{N}_\Gamma(H)$ and $C = \mathbf{C}_\Gamma(H)$. Let \mathcal{R} be the set consisting of all F -representations \mathcal{X} of G that satisfy $\mathcal{X}(G) = H$. Let \mathcal{D} be the set consisting of all orbits in the action of the group N by conjugation on the set \mathcal{R} . Under this action, C is the stabilizer subgroup for each member of \mathcal{R} , and so all the orbits have size $|N : C|$. It follows that $|\mathcal{R}| = |N : C| \cdot |\mathcal{D}|$. It remains to show that $|\mathcal{R}| = |\text{Aut}(G)|$ and $|\mathcal{D}| = |\mathcal{S}(\mathcal{H})|$.

Fix any representation $\mathcal{X} \in \mathcal{R}$. Thus $\mathcal{X} : G \rightarrow H$ is an isomorphism. For each representation $\mathcal{Y} \in \mathcal{R}$, we define the automorphism $\mathcal{X}^{-1} \circ \mathcal{Y} \in \text{Aut}(G)$ by $(\mathcal{X}^{-1} \circ \mathcal{Y})(x) = \mathcal{X}^{-1}(\mathcal{Y}(x))$ for each $x \in G$. The mapping $\mathcal{R} \rightarrow \text{Aut}(G)$ defined by $\mathcal{Y} \mapsto \mathcal{X}^{-1} \circ \mathcal{Y}$ is clearly a bijection. Therefore $|\mathcal{R}| = |\text{Aut}(G)|$, as desired. It remains to show that $|\mathcal{D}| = |\mathcal{S}(\mathcal{H})|$.

We define the mapping $\Psi : \mathcal{D} \rightarrow \mathcal{S}(\mathcal{H})$ as follows. For each orbit $\mathcal{O} \in \mathcal{D}$, we choose an arbitrary representation $\mathcal{X} \in \mathcal{O}$, and define $\Psi(\mathcal{O})$ to be the unique similarity class of F -representations of G that includes \mathcal{X} as a member. To see that Ψ is well defined, suppose that the representations $\mathcal{X}_1, \mathcal{X}_2 \in \mathcal{R}$ belong to the same N -orbit \mathcal{O} . Then it is clear that \mathcal{X}_1 and \mathcal{X}_2 are similar representations, and so the similarity class $\Psi(\mathcal{O})$ is well defined.

To complete the proof of part (a), we establish that the mapping $\Psi : \mathcal{D} \rightarrow \mathcal{S}(\mathcal{H})$ is a bijection. To see that Ψ is injective, suppose that \mathcal{X}_1 and \mathcal{X}_2 are similar representations. Hence there exists a matrix $g \in \text{GL}(m, F)$ such that $g^{-1}\mathcal{X}_1(x)g = \mathcal{X}_2(x)$ for each $x \in G$. In particular, the element g conjugates the subgroup $\mathcal{X}_1(G)$ to the subgroup $\mathcal{X}_2(G)$. But since $\mathcal{X}_1(G) = H = \mathcal{X}_2(G)$, it follows that $g \in N$, and so the representations \mathcal{X}_1 and \mathcal{X}_2 belong to the same N -orbit. Hence the map Ψ is injective. To see that Ψ is surjective, note that each similarity class in $\mathcal{S}(\mathcal{H})$ clearly includes some representation in the set \mathcal{R} .

(b) Let $\mathcal{H}_1, \dots, \mathcal{H}_t$ be the conjugacy classes of subgroups of Γ that include the subgroups H_1, \dots, H_t respectively. For each index $i \in \{1, \dots, t\}$, part (a) yields $|\mathcal{S}(\mathcal{H}_i)| = |\text{Aut}(G)|(c_i/n_i)$. Since $\mathcal{S} = \bigcup_{i=1}^t \mathcal{S}(\mathcal{H}_i)$ is a disjoint union, the result follows. \square

Lemma 2.2. Let G be a monolithic finite group, let F be a field, let $m = \text{mindeg}(G, F)$. In case the field F has prime characteristic r , we further suppose that $\mathbf{O}_r(G) = 1$. Then every faithful F -representation of G of degree m is irreducible.

Proof. Let \mathcal{X} be any faithful F -representation of G of degree m . We may assume that \mathcal{X} is in block lower-triangular form. Let N be the intersection of the kernels of the irreducible constituent representations of \mathcal{X} which appear as the blocks along the diagonal. If we could show that N is trivial, then the monolithicity of G would imply that one of these irreducible constituent representations is faithful, and by the minimality of m it would follow that this constituent representation is \mathcal{X} itself, yielding the desired conclusion that \mathcal{X} is irreducible. Thus it remains to show that N is trivial. We proceed by cases. First suppose that F has characteristic zero. By Maschke's Theorem, we may assume

that \mathcal{X} is in block diagonal form. Hence $N = \ker \mathcal{X}$. Since \mathcal{X} is faithful, it follows that N is trivial, as desired. Now suppose that F has prime characteristic r . Since $\mathcal{X}(N)$ is a finite subgroup of $\mathrm{GL}(m, F)$ consisting of unitriangular matrices, we deduce that $\mathcal{X}(N)$ is an r -group. Because \mathcal{X} is faithful, we have $\mathcal{X}(N) \cong N$. Therefore $N \subseteq \mathbf{O}_r(G) = 1$, and the proof is complete. \square

The next several results involve the notion of an absolutely irreducible representation of a finite group. For a definition and discussion of this notion, see Chapter 9 of [7]. The first of these results is well known, and describes a technique to which Marty Isaacs refers informally as “sliding the field.” Because this result is well known, we omit the proof.

Lemma 2.3. *Let G be a finite group, let F be a finite field, and let \bar{F} be the algebraic closure of F . Suppose that V is a faithful irreducible finite-dimensional $F[G]$ -module that is not absolutely irreducible. Then there exists a finite field E such that $F < E < \bar{F}$ and such that V is a faithful absolutely irreducible $E[G]$ -module.*

Theorem 2.4. *Let (G, q, m) be a monolithic triple. Let F be the field with q elements.*

- (a) *Every faithful F -representation of G of degree m is absolutely irreducible.*
- (b) *For each subgroup H of the general linear group $\Gamma = \mathrm{GL}(m, q)$ that is isomorphic to G , we have $\mathbf{C}_\Gamma(H) = \mathbf{Z}(\Gamma)$, and so $\mathbf{C}_\Gamma(H)$ is cyclic of order $q - 1$.*

Proof. (a) Let \mathcal{X} be any faithful F -representation of G of degree m . By Lemma 2.2, \mathcal{X} is irreducible. Suppose that \mathcal{X} is not absolutely irreducible. Let V denote the $F[G]$ -module corresponding to \mathcal{X} and let \bar{F} be the algebraic closure of F . By Lemma 2.3, there exists a finite field E such that $F < E < \bar{F}$ and V is a faithful absolutely irreducible $E[G]$ -module. Let \mathcal{Y} denote an E -representation of G corresponding to the module V . Writing $f = |E : F|$, it follows that $f > 1$ and that the absolutely irreducible E -representation \mathcal{Y} has degree m/f . Hence we may view \mathcal{Y} as a faithful irreducible \bar{F} -representation of G of degree m/f . Let r be the unique prime divisor of the prime-power q . Since r does not divide $|G|$, we have the identification $\mathrm{IBr}(G) = \mathrm{Irr}(G)$. It follows that the r -Brauer character associated with \mathcal{Y} is a faithful irreducible ordinary character of G of degree m/f where $f > 1$, and this contradicts the hypothesis that (G, q, m) is a monolithic triple.

(b) Let H be any subgroup of $\Gamma = \mathrm{GL}(m, q)$ that is isomorphic to G . Let $\mathcal{Z} : G \rightarrow H$ be an isomorphism. Thus \mathcal{Z} is a faithful F -representation of G of degree m . By part (a), \mathcal{Z} is absolutely irreducible. By Theorem 9.2 in [7], it follows that the centralizer of H in the matrix algebra $\mathrm{Mat}(m, F)$ consists of scalar matrices. Since $\mathbf{Z}(\Gamma)$ consists of all the nonzero scalar matrices in $\mathrm{Mat}(m, F)$ and is cyclic of order $q - 1$, the result follows. \square

Theorem 2.5. *Let (G, q, m) be any good monolithic triple and let F be the field with q elements. Then $|\mathcal{F}(G, q)|$ is equal to the number of similarity classes of faithful F -representations of G of degree m .*

Proof. Let $\mathcal{F} = \mathcal{F}(G, q)$ and let S be the set consisting of all similarity classes of faithful F -representations of G of degree m . We now define a bijective mapping from \mathcal{F} to S .

Let r be the unique prime divisor of the prime-power q . Let R be the ring of algebraic integers in \mathbb{C} and let S be the localization of R with respect to some arbitrarily-chosen maximal ideal M of R that contains the ideal rR (see [8]). Let \bar{F} denote the algebraic closure of F . We have a surjective ring homomorphism $*$: $S \rightarrow \bar{F}$, and this determines a surjective ring homomorphism $*$: $\mathrm{Mat}(n, S) \rightarrow \mathrm{Mat}(n, \bar{F})$ for arbitrary $n \geq 1$.

Let $\chi \in \mathcal{F}$ be arbitrary. By Theorem 2.7 in [8], there exists a representation \mathcal{X}_χ with matrix entries in S that affords χ . We define the \bar{F} -representation \mathcal{X}_χ^* by $\mathcal{X}_\chi^*(x) = \mathcal{X}_\chi(x)^*$ for $x \in G$. The representation \mathcal{X}_χ^* affords the Brauer character $\chi^\circ = \chi$. Since r does not divide the order of G , every element in the kernel of \mathcal{X}_χ^* belongs to the kernel of the r -Brauer character $\chi^\circ = \chi$. Thus, since χ is faithful, the representation \mathcal{X}_χ^* is faithful. Since r does not divide $|G|$, we have $\mathrm{IBr}(G) = \mathrm{Irr}(G)$ and so by the proof of Theorem 2.12 in [8], \mathcal{X}_χ^* is irreducible. Because the monolithic triple (G, q, m) is good, for each element $x \in G$, the character value $\chi(x)$ is a \mathbb{Z} -linear combination of complex $(q - 1)$ th roots of

unity. (We mention that every complex $(q-1)$ th root of unity is contained in R , and hence in S .) Since $*$: $S \rightarrow \bar{F}$ is a ring homomorphism, it follows that $\chi(x)^*$ is a \mathbb{Z} -linear combination of $(q-1)$ th roots of unity in the field \bar{F} , and this implies that $\chi(x)^* \in F$.

By Lemma 2.4 in [8], χ^* is the \bar{F} -character afforded by the \bar{F} -representation \mathcal{X}_χ^* . Because all the values of χ^* belong to the subfield F , Theorem 9.14 in [7] implies the existence of a (faithful) F -representation \mathcal{Y}_χ that is \bar{F} -similar to \mathcal{X}_χ^* . Let $[\mathcal{Y}_\chi]$ be the member of \mathcal{S} that contains \mathcal{Y}_χ . We claim that the corresponding map $\chi \mapsto [\mathcal{Y}_\chi]$ is a bijection from the set \mathcal{F} to the set \mathcal{S} . We have established that this map is well defined.

To show that this map is injective, we must show for distinct characters $\chi, \psi \in \mathcal{F}$ that $[\mathcal{Y}_\chi] \neq [\mathcal{Y}_\psi]$. If $[\mathcal{Y}_\chi] = [\mathcal{Y}_\psi]$, then since \mathcal{X}_χ^* is similar to \mathcal{Y}_χ and \mathcal{X}_ψ^* is similar to \mathcal{Y}_ψ , it follows that \mathcal{X}_χ^* and \mathcal{X}_ψ^* are similar \bar{F} -representations affording distinct Brauer characters χ and ψ , and this is a contradiction. Hence the map is injective.

Finally we argue that the map is surjective. Let \mathcal{Z} be any faithful F -representation of G of degree m . By Theorem 2.4(a), \mathcal{Z} is absolutely irreducible. Regarding \mathcal{Z} as an \bar{F} -representation, let χ be the Brauer character afforded by \mathcal{Z} . Thus $\chi \in \text{IBr}(G) = \text{Irr}(G)$. For each element $x \in G$, we have $\chi(x)^* \in F$, and so $\chi \in \mathcal{F}$. We now see that $[\mathcal{Y}_\chi] = [\mathcal{Z}]$. \square

Proof of Theorem A. Apply Theorems 2.1(b), 2.4(b), and 2.5. \square

Proof of Corollary B. (a) Let the subgroups H_1, \dots, H_t be representatives for the distinct conjugacy classes of subgroups of Γ whose members are isomorphic to G . We may assume that $H_1 = H$. For each $i \in \{1, \dots, t\}$, write $N_i = \mathbf{N}_\Gamma(H_i)$ and $C_i = \mathbf{C}_\Gamma(H_i)$. By hypothesis, $|A| = k|\mathcal{F}| \cdot |N_1 : C_1|$ for some positive integer k . Theorem A implies that

$$|\mathcal{F}| = k|\mathcal{F}| \frac{|N_1|}{|C_1|} \sum_{i=1}^t \frac{|C_i|}{|N_i|}, \quad \text{from which we obtain } \frac{|C_1|}{|N_1|} \geq \frac{|C_1|}{|N_1|k} = \sum_{i=1}^t \frac{|C_i|}{|N_i|} \geq \frac{|C_1|}{|N_1|}.$$

Both inequalities are forced to be equalities, and this yields $k=1$ and $t=1$, as desired.

(b) Because N/C is isomorphic to a subgroup of A , we know that $|N : C|$ divides $|A|$. Since $|\mathcal{F}| = 1$, it follows that $|\mathcal{F}| \cdot |N : C|$ divides $|A|$. Now the statement of part (a) implies that $t=1$ and $|N : C| = |A|$. Therefore N/C is isomorphic to A , as desired. \square

3. Proofs of Theorems 1.4, 1.5, and 1.7

In this section we prove Theorems 1.4, 1.5, and 1.7. We begin by stating a well-known number-theoretic lemma whose proof we omit.

Lemma 3.1. *Let q be any prime-power larger than 1 and let p be any prime divisor of $q-1$. Let p^e denote the full p -part of $q-1$, and suppose that $p^e \geq 3$. Let k be any positive integer and let p^a denote the full p -part of k . Then the full p -part of $q^k - 1$ is p^{e+a} .*

The next result gives the orders of Sylow p -subgroups of certain general linear groups.

Lemma 3.2. *Let q be any prime-power larger than 1 and let p be any prime divisor of $q-1$. Let p^e denote the full p -part of $q-1$, and suppose that $p^e \geq 3$. Then for every positive integer m , the full p -part of $|\text{GL}(m, q)|$ is p^{em+s} where p^s is the full p -part of $m!$.*

Proof. For each positive integer k , Lemma 3.1 states that the full p -part of $q^k - 1$ is $p^{e+v(k)}$ where $p^{v(k)}$ denotes the full p -part of k . Using a well-known formula, we write $|\text{GL}(m, q)| = q^r n$ where $n = (q-1)(q^2-1) \cdots (q^m-1)$ and where r is some nonnegative integer. The full p -part of $|\text{GL}(m, q)|$ is therefore equal to the full p -part of n , namely

$$\prod_{k=1}^m p^{e+v(k)} = p^{em} \prod_{k=1}^m p^{v(k)} = p^{em} p^s,$$

as desired. \square

Let q be a prime-power and let p be a prime that satisfy the hypothesis of Lemma 3.2. For any integers k and m such that $1 \leq k < m$, the full p -part of $k!$ is less than or equal to the full p -part of $m!$, and so by Lemma 3.2, the full p -part of $|\mathrm{GL}(k, q)|$ is strictly smaller than the full p -part of $|\mathrm{GL}(m, q)|$. Hence a Sylow p -subgroup of $\mathrm{GL}(k, q)$ has smaller order than a Sylow p -subgroup of $\mathrm{GL}(m, q)$. We shall use this fact in the proof of Theorem 1.7.

In Definition 1.3, in case $n \geq 2$ we recursively defined $W_n^e(p)$ as the semidirect product $N \rtimes \mathbb{Z}_p$ where N is the direct product of p copies of $W_{n-1}^e(p)$. We now describe another way to regard $W_n^e(p)$ as a semidirect product that is useful for stating and proving the following lemma. First note that for $n \geq 2$, the fact that $W_{n-1}^1(p)$ is isomorphic to a Sylow p -subgroup of the symmetric group of degree p^{n-1} provides us with a transitive action of $W_{n-1}^1(p)$ on a set of size p^{n-1} . For each positive integer n , the group $W_n^e(p)$ is isomorphic to the semidirect product $B \rtimes Q$ where B is the direct product of p^{n-1} copies of the cyclic group of order p^e and where the group Q and its action on B are defined as follows. In case $n = 1$, the group Q is trivial and thus its action on B is trivial. In case $n \geq 2$, the group Q is isomorphic to $W_{n-1}^1(p)$ and acts via automorphisms on B by transitively permuting the p^{n-1} direct factors of B in a manner described earlier in this paragraph.

Lemma 3.3. *Let p be a prime, let e and n be positive integers, and write $W_n^e(p) = B \rtimes Q$ where B and Q are defined as in the preceding paragraph. Let F be any field containing a primitive p^e th root of unity. Then there exists a faithful F -representation \mathcal{Y} of $W_n^e(p)$ of degree p^{n-1} such that $\mathcal{Y}(B)$ is the group of all diagonal matrices of order dividing p^e in the general linear group $\mathrm{GL}(p^{n-1}, F)$ while $\mathcal{Y}(Q)$ is a transitive group of permutation matrices.*

Proof. We proceed via induction on n . The base case $n = 1$ is trivial. Let $n > 1$ and assume inductively that \mathcal{X} is a faithful F -representation of $W_{n-1}^e(p)$ of degree p^{n-2} having the desired properties. By definition we have $W_n^e(p) = N \rtimes \langle w \rangle$ where N is the direct product of p copies of the group $W_{n-1}^e(p)$, and where the automorphism $w \in \mathrm{Aut}(N)$ cyclically permutes these p direct factors. We now define the homomorphism $\mathcal{Y}: W_n^e(p) \rightarrow \mathrm{GL}(p^{n-1}, F)$ as follows. For each element $x = (x_1, \dots, x_p) \in N$, we let

$$\mathcal{Y}(x) = \begin{pmatrix} \mathcal{X}(x_1) & 0 & \cdots & 0 \\ 0 & \mathcal{X}(x_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathcal{X}(x_p) \end{pmatrix}.$$

Furthermore, letting I denote the p^{n-2} -by- p^{n-2} identity matrix, we define the matrix

$$\mathcal{Y}(w) = \begin{pmatrix} 0 & 0 & 0 & 0 & I \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & I & 0 \end{pmatrix}.$$

The proof is complete. \square

Proof of Theorem 1.4. Let F be the field with q elements. By hypothesis, F contains a primitive p^e th root of unity. Write $\Gamma = \text{GL}(p^{n-1}, q)$ and $W = W_n^e(p)$. By Lemma 3.3, there exists a faithful representation $\mathcal{X} : W \rightarrow \Gamma$. Letting $P = \mathcal{X}(W)$, we see that $P \cong W$.

Now suppose that $p^e \geq 3$. For $m = p^{n-1}$, the full p -part of $m!$ is p^s where $s = 1 + p + p^2 + \dots + p^{n-2}$. By Lemma 3.2, each Sylow p -subgroup of Γ has order $p^{\alpha(n)}$. Since $P \cong W$ and $|W| = p^{\alpha(n)}$, it follows that P is a Sylow p -subgroup of Γ . \square

Proof of Theorem 1.5. (a) \Rightarrow (b). Let $\mathcal{X} : G \rightarrow \text{GL}(p^{n-1}, \mathbb{C})$ be a faithful representation. We now use a standard technique (see Chapter 2 in [8]) for using \mathcal{X} to construct an F -representation of G . Let R be the ring of algebraic integers in \mathbb{C} and let M be any maximal ideal of R that contains the ideal rR . By Lemma 2.1 in [8], the quotient ring R/M is isomorphic to the field F . Hence there exists a surjective ring homomorphism $*$: $R \rightarrow F$. We define the ring $S = \{\frac{r}{s} \mid r \in R, s \in R - M\}$, and we note that $R \subseteq S$. We extend the domain of $*$ to define the surjective ring homomorphism $*$: $S \rightarrow F$ by $(\frac{r}{s})^* = r^*(s^*)^{-1}$. If m is a matrix with entries in the ring S , we denote by m^* the matrix in F that results from applying $*$ to every entry of m . It is clear that $*$: $\text{Mat}(p^{n-1}, S) \rightarrow \text{Mat}(p^{n-1}, F)$ is a surjective ring homomorphism, and that $\det m^* = (\det m)^*$ for each $m \in \text{Mat}(p^{n-1}, S)$.

By Theorem 2.7 in [8], \mathcal{X} is similar to some (faithful) representation \mathcal{Y} with matrix entries in S . We define the F -representation \mathcal{Y}^* by $\mathcal{Y}^*(x) = \mathcal{Y}(x)^*$ for $x \in G$. Since r does not divide the order of G , the r -Brauer character afforded by the representation \mathcal{Y}^* is actually the ordinary character afforded by the faithful representation \mathcal{X} . It follows that the representation $\mathcal{Y}^* : G \rightarrow \text{GL}(p^{n-1}, F)$ is faithful, as desired.

(b) \Rightarrow (c). Suppose that there exists a faithful F -representation $\mathcal{X} : G \rightarrow \text{GL}(p^{n-1}, F)$. Since G is finite, all the matrix entries of the representation \mathcal{X} are contained in some finite subfield K of F . Let $|K| = q$ where $q = r^m$ for some positive integer m . Thus we have a faithful representation $\mathcal{X} : G \rightarrow \text{GL}(p^{n-1}, q)$. Since the p -group G is isomorphic to the subgroup $\mathcal{X}(G)$ of $\text{GL}(p^{n-1}, q)$, indeed $\mathcal{X}(G)$ is contained in some Sylow p -subgroup P of $\text{GL}(p^{n-1}, q)$. Replacing K by a larger field if necessary, we may assume that $2(p-1)$ divides m . Let p^e denote the full p -part of $q-1$. Since $p-1$ divides m , by elementary number theory p divides $r^m - 1 = q - 1$, and so $e \geq 1$. We now argue that $p^e \geq 3$. In case p is odd, this is clearly true. We may assume that $p = 2$, and so r is odd. Since $q = r^m$ while m is even, it follows that $q-1$ is divisible by $4 = p^2$, yielding $e \geq 2$, as desired. Since $p^e \geq 3$, Theorem 1.4 implies that P is isomorphic to $W_n^e(p)$.

(c) \Rightarrow (a). Suppose that G is isomorphic to a subgroup of $W_n^e(p)$ for some integer $e \geq 1$. By Lemma 3.3, $W_n^e(p)$ is isomorphic to a subgroup of $\text{GL}(p^{n-1}, \mathbb{C})$. Hence G is isomorphic to a subgroup of $\text{GL}(p^{n-1}, \mathbb{C})$, as desired. \square

The next several lemmas are needed for our proof of Theorem 1.7.

Lemma 3.4. Let q be any prime-power larger than 1 and let p be any prime divisor of $q-1$. Let p^e denote the full p -part of $q-1$, and suppose that $p^e \geq 3$. Then for each integer $n \geq 2$, the full p -part of the order of $\text{GL}(p^{n-1}-1, q)$ is p^a where $a = \alpha(n) - e - n + 1$.

Proof. We apply Lemma 3.2, taking $m = p^{n-1} - 1$. Let p^s denote the full p -part of $m!$. It is not difficult to show that the full p -part of $(p^{n-1})!$ is p^t where $t = 1 + p + p^2 + \dots + p^{n-2}$. Since $(p^{n-1})! = p^{n-1}m!$, it follows that $s = t - n + 1$. Recall that $\alpha(n) = ep^{n-1} + t$. By Lemma 3.2, the full p -part of $|\text{GL}(p^{n-1}-1, q)|$ is p^a where

$$a = em + s = e(p^{n-1} - 1) + t - n + 1 = \alpha(n) - e - n + 1,$$

as desired. \square

Lemma 3.5. Let p be a prime and let e be a positive integer such that $p^e \geq 3$. For each positive integer k , let Q_k denote the direct product of $p-1$ copies of the group $W_k^e(p)$. Let q be any prime-power larger than 1 such

that the full p -part of $q - 1$ is equal to p^e . Then for each integer $n \geq 2$, a Sylow p -subgroup of the general linear group $\mathrm{GL}(p^{n-1} - 1, q)$ is isomorphic to the direct product $Q_1 \times Q_2 \times \cdots \times Q_{n-1}$.

Proof. We proceed via induction on n . For the base case $n = 2$, the group $\mathrm{GL}(p - 1, q)$ contains a subgroup consisting of diagonal matrices that is isomorphic to the homocyclic group Q_1 of rank $p - 1$ and of exponent p^e . By Lemma 3.4 and the fact that $\alpha(2) = ep + 1$, the full p -part of the order of $\mathrm{GL}(p - 1, q)$ is $p^{e(p-1)}$. Hence the previously-mentioned subgroup that is isomorphic to Q_1 is actually a Sylow p -subgroup of $\mathrm{GL}(p - 1, q)$.

Henceforth let $n \geq 3$. Let H denote the subgroup of $\mathrm{GL}(p^{n-1} - 1, q)$ consisting of block diagonal matrices where one block is $\mathrm{GL}(p^{n-2} - 1, q)$ and $p - 1$ blocks are $\mathrm{GL}(p^{n-2}, q)$. By the inductive hypothesis, a Sylow p -subgroup of $\mathrm{GL}(p^{n-2} - 1, q)$ is isomorphic to the direct product $Q_1 \times Q_2 \times \cdots \times Q_{n-2}$. By Theorem 1.4, a Sylow p -subgroup of $\mathrm{GL}(p^{n-2}, q)$ is isomorphic to $W_{n-1}^e(p)$. Thus a Sylow p -subgroup of H is isomorphic to the direct product $Q_1 \times Q_2 \times \cdots \times Q_{n-2} \times Q_{n-1}$. To complete the proof, we show that a Sylow p -subgroup of H is actually a Sylow p -subgroup of $\mathrm{GL}(p^{n-1} - 1, q)$. For this it suffices to show that the full p -part of the order of H is equal to the full p -part of the order of $\mathrm{GL}(p^{n-1} - 1, q)$. First we consider the full p -part of the order of H . By Lemma 3.4, the full p -part of the order of $\mathrm{GL}(p^{n-2} - 1, q)$ is $p^{\alpha(n-1)-e-(n-1)+1}$. As we mentioned earlier, a Sylow p -subgroup of $\mathrm{GL}(p^{n-2}, q)$ is isomorphic to $W_{n-1}^e(p)$. Recall that $W_{n-1}^e(p)$ has order $p^{\alpha(n-1)}$. Hence the full p -part of the order of H is p^a where

$$a = \alpha(n - 1) - e - (n - 1) + 1 + (p - 1)\alpha(n - 1) = p\alpha(n - 1) - e - n + 2.$$

Using $p\alpha(n - 1) + 1 = \alpha(n)$, we obtain $a = \alpha(n) - e - n + 1$. On the other hand, Lemma 3.4 implies that the full p -part of the order of $\mathrm{GL}(p^{n-1} - 1, q)$ is $p^{\alpha(n)-e-n+1}$. \square

The following lemma is a useful fact about monolithic groups.

Lemma 3.6. Let H_1, \dots, H_n be a collection of finite groups and let G be a monolithic finite group that is isomorphic to a subgroup of the direct product $H = H_1 \times \cdots \times H_n$. Then G is isomorphic to a subgroup of H_k for some $k \in \{1, \dots, n\}$.

Proof. For each $i \in \{1, \dots, n\}$, the “projection map” $\pi_i : H \rightarrow H_i$ is a homomorphism. By hypothesis, there exists an injective homomorphism $\theta : G \rightarrow H$. Let N be the unique minimal normal subgroup of G . Since $N > 1$, we have $\theta(N) > 1$, and so $\pi_k(\theta(N)) > 1$ for some $k \in \{1, \dots, n\}$. The composition $\pi_k \circ \theta$ is a homomorphism from G to H_k whose kernel does not contain N , and is therefore injective. \square

Proof of Theorem 1.7. First we argue that $\mathrm{mindeg}(G, q) = p^{n-1}$. By Theorem 1.4, $W_n^e(p)$ is isomorphic to a subgroup of $\mathrm{GL}(p^{n-1}, q)$. Since G is isomorphic to a subgroup of $W_n^e(p)$, we deduce that $\mathrm{mindeg}(G, q) \leq p^{n-1}$. We suppose that $\mathrm{mindeg}(G, q) < p^{n-1}$. Since $p^e \geq 3$, Lemma 3.5 implies that G is isomorphic to a subgroup of the direct product $Q_1 \times Q_2 \times \cdots \times Q_{n-1}$. Since G is monolithic, Lemma 3.6 implies that G is isomorphic to a subgroup of $W_k^e(p)$ for some $k \in \{1, \dots, n - 1\}$. By Theorem 1.5, G is isomorphic to a subgroup of $\mathrm{GL}(p^{k-2}, \mathbb{C})$. It follows that G has a faithful irreducible ordinary character of degree p^{k-1} , which contradicts the definition of n . Hence $\mathrm{mindeg}(G, q) = p^{n-1}$, as desired. Finally, by the definition of n , we know that every faithful irreducible ordinary character of G has degree at least p^{n-1} . Therefore (G, q, p^{n-1}) is a monolithic triple. \square

In [11] we make heavy use of the following result in conjunction with Theorem A.

Theorem 3.7. Let G be a nonabelian monolithic subgroup of $W_2^e(p)$ where p is some prime and e is a positive integer such that $p^e \geq 3$. Let q be any prime-power larger than 1 such that the p -part of $q - 1$ is equal to p^e . Then (G, q, p) is a good monolithic triple and $|\mathcal{F}(G, q)| = |G|(p - 1)/p^3$.

Proof. By Theorem 1.4, the group $W_2^e(p)$ is isomorphic to a subgroup of $GL(p, q)$. Thus $\text{mindeg}(G, q) \leq p$. On the other hand, whenever $n < p$, the group $GL(n, q)$ has an abelian Sylow p -subgroup consisting of diagonal matrices, and therefore does not contain any subgroup that is isomorphic to the nonabelian p -group G . Hence $\text{mindeg}(G, q) = p$. The group $W_2^e(p)$ has a normal subgroup B of index p that is homocyclic of exponent p^e and of rank p . Since $B \cap G$ is abelian normal of index p in G , every nonlinear irreducible ordinary character of G has degree p . Therefore (G, q, p) is a monolithic triple.

We argue that $|\mathcal{F}(G, q)| = |G|(p-1)/p^3$. Let \mathcal{A} be the set of all faithful irreducible characters of G and let $\mathcal{B} = \text{Irr}(G) - \mathcal{A}$. Since G is nonabelian, every linear character of G belongs to \mathcal{B} . Thus every character in the set \mathcal{A} has degree p , and so $\mathcal{A} = \mathcal{F}(G, q)$. Let M be the unique minimal normal subgroup of G . We have $\mathcal{B} = \{\psi \in \text{Irr}(G) \mid M \subseteq \ker \psi\}$. We may identify the set \mathcal{B} with the set $\text{Irr}(G/M)$. Since $|M| = p$, we have $|G/M| = |G|/p$. By Corollary 2.7 in [7] and the fact that $\text{Irr}(P) = \mathcal{A} \cup \mathcal{B}$ is a disjoint union, we deduce that

$$|P| = \sum_{\psi \in \mathcal{A}} \psi(1)^2 + \sum_{\psi \in \mathcal{B}} \psi(1)^2 = |\mathcal{A}| \cdot p^{2n} + |P|/p.$$

Solving this equation for $|\mathcal{A}|$, we obtain $|\mathcal{A}| = |G|(p-1)/p^3$, as desired.

We argue that the monolithic triple (G, q, p) is good. Because $B \cap G$ is abelian normal of index p in G , an arbitrary character $\chi \in \mathcal{F}(G, q)$, whose degree is known to be p , is induced from a linear character of $B \cap G$ and vanishes off the subgroup $B \cap G$. Since $B \cap G$ is abelian of exponent dividing p^e , every value of the restriction of χ to $B \cap G$ is a sum of complex p^e th roots of unity, and hence every value of χ is a sum of complex p^e th roots of unity. Since p^e divides $q-1$, it follows that the monolithic triple (G, q, p) is good. \square

4. Normalizers of subgroups in general linear groups

In this section we establish some results that may be used to calculate the order of the normalizer of a subgroup in a general linear group in certain situations. We make use of the results of this section in our applications of Theorem A in [9–11].

We now fix some notations for use throughout this section. Let F be an arbitrary field, let n be any positive integer, and let $\Gamma = GL(n, F)$ be the general linear group. Let D be the subgroup of Γ consisting of all diagonal matrices. Let S be the subgroup of Γ consisting of all permutation matrices, and note that S is isomorphic to the symmetric group of degree n . Let M be the subgroup of Γ consisting of all monomial matrices. Observe that $D \triangleleft M$ and $M = SD$ and $D \cap S = 1$, which says that $M = D \rtimes S$ is a semidirect product group. Let $\theta : M \rightarrow S$ be the homomorphism defined by $\theta(m) = \pi$ where the elements $\pi \in S$ and $d \in D$ are uniquely determined by the condition $m = \pi d$.

Definition 4.1. Let D_0 be a subgroup of the general linear group Γ that consists of diagonal matrices. We say that D_0 is a **separator subgroup** of Γ provided that for each pair $i, j \in \{1, \dots, n\}$ such that $i \neq j$, the group D_0 contains a matrix whose (i, i) -entry is not equal to its (j, j) -entry.

The following result states that if D_0 is any subgroup of the general linear group Γ that consists of diagonal matrices, then the normalizer $\mathbf{N}_\Gamma(D_0)$ consists of monomial matrices iff D_0 is a separator subgroup of Γ . This result is a generalization of Satz II.7.2(a) in [6]. Our proof is an adaptation of the proof of Satz II.7.2(a) in [6].

Lemma 4.2. Let $V = F^n$ be the vector space consisting of row vectors on which the general linear group Γ acts by ordinary matrix multiplication. For each $k \in \{1, \dots, n\}$, let v_k denote the row vector in V whose k th component is 1 and each of whose other components is 0. Let D_0 be any subgroup of Γ that consists of diagonal matrices. The following conditions are equivalent:

- (a) D_0 is a separator subgroup of Γ .
- (b) The only D_0 -invariant one-dimensional subspaces of V are $\langle v_1 \rangle, \dots, \langle v_n \rangle$.
- (c) The normalizer $\mathbf{N}_F(D_0)$ consists of monomial matrices.

Proof. For each pair $i, j \in \{1, \dots, n\}$, let $e_{i,j}$ denote the n -by- n matrix whose (i, j) -entry is 1 and each of whose other entries is 0.

(a) \Rightarrow (b). Because D_0 consists of diagonal matrices, the subspaces $\langle v_1 \rangle, \dots, \langle v_n \rangle$ are all D_0 -invariant. Let $v = (c_1, \dots, c_n) \in V$ and suppose that the subspace $\langle v \rangle$ is D_0 -invariant. To establish condition (b), we show that the vector v has at most one nonzero component. Assume instead that there exists a pair $i, j \in \{1, \dots, n\}$ such that $i \neq j$ and $c_i \neq 0 \neq c_j$. By condition (a), there exists $d \in D_0$ such that when we write $d = \sum_{k=1}^n d_k e_{k,k}$ for scalars $d_k \in F$, we have $d_i \neq d_j$. It is evident that the vector $vd = (c_1 d_1, \dots, c_n d_n)$ is not a scalar multiple of the vector v , contradicting that $\langle v \rangle$ is D_0 -invariant.

(b) \Rightarrow (c). Let $g \in \mathbf{N}_F(D_0)$ and $k \in \{1, \dots, n\}$. We argue that the one-dimensional subspace $\langle v_k g \rangle$ is D_0 -invariant. For arbitrary $d \in D_0$, we know that $gd = d'g$ for some $d' \in D_0$, and there exists a scalar $c \in F$ such that $(v_k g)d = (v_k d')g = (cv_k)g = c(v_k g)$. Hence $\langle v_k g \rangle$ is D_0 -invariant. By condition (b), this implies that $\langle v_k g \rangle = \langle v_\ell \rangle$ for some $\ell \in \{1, \dots, n\}$. Since $k \in \{1, \dots, n\}$ is arbitrary, it follows that g is a monomial matrix.

(c) \Rightarrow (a). Assuming condition (a) is false, let the pair i, j be a counterexample. Let $d \in D_0$ be arbitrary and write $d = \sum_{k=1}^n d_k e_{k,k}$ for scalars $d_k \in F$. Thus $d_i = d_j$. Let e denote the identity matrix. Write $g = e + e_{i,j} \in \Gamma$ and note that $g^{-1} = e - e_{i,j} \in \Gamma$. Observe that $g^{-1}dg = d + de_{i,j} - e_{i,j}d - e_{i,j}de_{i,j}$. But $de_{i,j} = d_i e_{i,j}$ and $e_{i,j}d = d_j e_{i,j}$ while $e_{i,j}de_{i,j} = 0$. It follows that $g^{-1}dg = d + (d_i - d_j)e_{i,j}$, and since $d_i = d_j$ this says that $g \in \mathbf{C}_F(D_0) \subseteq \mathbf{N}_F(D_0)$. Since g is not a monomial matrix, condition (c) is false. \square

We now describe the type of situation in which we shall use Lemma 4.2. Suppose that we have a subgroup H of M and that we wish to calculate its normalizer $\mathbf{N}_F(H)$. In this situation, suppose that we can find a group D_0 consisting of diagonal matrices that is both a characteristic subgroup of H and a separator subgroup of Γ . Since D_0 is a characteristic subgroup of H , we have $D_0 \triangleleft \mathbf{N}_F(H)$, and this yields $\mathbf{N}_F(H) \subseteq \mathbf{N}_F(D_0)$. Since D_0 is a separator subgroup of Γ , Lemma 4.2 implies that $\mathbf{N}_F(D_0) \subseteq M$. Thus we obtain $\mathbf{N}_F(H) \subseteq M$, which says that $\mathbf{N}_F(H) = \mathbf{N}_M(H)$. In this manner, the problem of calculating $\mathbf{N}_F(H)$ is reduced to the smaller problem of calculating $\mathbf{N}_M(H)$.

The next result (used in [11]) is designed to facilitate the calculation of $\mathbf{N}_M(H)$. Its proof uses the obvious fact that for each monomial matrix $m \in M = SD$, when we write $m = \pi d$ for a unique permutation matrix $\pi \in S$ and a unique diagonal matrix $d \in D$, the set of all nonzero entries of m is equal to the set of all diagonal entries of d .

Theorem 4.3. Let F_0 be any subgroup of the multiplicative group $F^\times = F - \{0\}$ and let E be the group consisting of all diagonal matrices in Γ having the property that each entry along the diagonal belongs to F_0 . Let H be a subgroup of SE and let $Q = \theta(H)$. Suppose that Q is a transitive subgroup of the symmetric group S and let $N = \mathbf{N}_S(Q)$. Then $\mathbf{N}_M(H) = \mathbf{N}_{NE}(H)\mathbf{Z}(\Gamma)$. Furthermore, if the field F is finite, then for $q = |F|$ we have $|\mathbf{N}_M(H)| = |\mathbf{N}_{NE}(H)|(q-1)/|F_0|$.

Proof. To prove $\mathbf{N}_M(H) = \mathbf{N}_{NE}(H)\mathbf{Z}(\Gamma)$, it suffices to show that $\mathbf{N}_M(H) \subseteq NE\mathbf{Z}(\Gamma)$. Let $m \in \mathbf{N}_M(H)$ be arbitrary and write $m = \pi d$ for unique elements $\pi \in S$ and $d \in D$. Since $\theta : M \rightarrow S$ is a homomorphism and $H \subseteq M$, indeed $\theta(\mathbf{N}_M(H)) \subseteq \mathbf{N}_S(Q) = N$. Thus since $m \in \mathbf{N}_M(H)$, we deduce that the matrix $\theta(m) = \pi$ belongs to N .

It remains to show that $d \in E\mathbf{Z}(\Gamma)$. Write $d = \text{diag}(c_1, \dots, c_n)$ with $c_1, \dots, c_n \in F^\times$. Let z be the scalar matrix that is c_1 times the identity matrix, and note that $z \in \mathbf{Z}(\Gamma)$. Let e be the diagonal matrix whose (i, i) -entry is $c_1^{-1}c_i$ for $i \in \{1, \dots, n\}$, and note that $d = ez$. It remains to show that $e \in E$. Let $i \in \{1, \dots, n\}$ be arbitrary. It suffices to show that $c_1^{-1}c_i \in F_0$. Since Q is a transitive subgroup of the symmetric group S , its conjugate subgroup Q^π is transitive. Hence there exists a permutation matrix $\pi_* \in Q$ such that the $(1, i)$ -entry of the permutation matrix π_*^π is 1. Since $\pi_* \in Q = \theta(H)$,

there exists a monomial matrix $m_* \in H$ of the form $m_* = \pi_* d_*$ for some diagonal matrix $d_* \in E$. By matrix multiplication, the $(1, i)$ -entry of the matrix $(\pi_*^\pi)^d = d^{-1} \pi_*^\pi d$ is $c_1^{-1} c_i$. Since $\pi_*^\pi \in S$ and $d \in D$, we have $(\pi_*^\pi)^d \in M$, and we define the diagonal matrix a by $(\pi_*^\pi)^d = \pi_*^\pi a$, and we note using the preceding sentence that $c_1^{-1} c_i$ is one of the diagonal entries of a . Thus it suffices to show that $a \in E$. Using $(\pi_*^\pi)^d = \pi_*^\pi a$ along with the fact that the diagonal matrices d_*^π and d commute with each other, we calculate that

$$m_*^m = \pi_*^\pi d_*^\pi d_*^\pi = \pi_*^\pi a d_*^\pi$$

with $\pi_*^\pi \in S$ and $a d_*^\pi \in D$. Since $m_* \in H$ and $m \in \mathbf{N}_M(H)$, indeed $m_*^m \in H$, and because $H \subseteq SE$, the preceding sentence yields $a d_*^\pi \in E$. Since $d_* \in E$, we have $d_*^\pi \in E$. The preceding two sentences imply that $a \in E$. Therefore $\mathbf{N}_M(H) = \mathbf{N}_{NE}(H)\mathbf{Z}(\Gamma)$.

Now suppose that the field F is finite and let $q = |F|$. Since $NE \cap \mathbf{Z}(\Gamma)$ normalizes H , we have $NE \cap \mathbf{Z}(\Gamma) \subseteq \mathbf{N}_{NE}(H)$. It follows that $NE \cap \mathbf{Z}(\Gamma) \subseteq \mathbf{N}_{NE}(H) \cap \mathbf{Z}(\Gamma)$. The reverse inclusion is immediate, and so we have $\mathbf{N}_{NE}(H) \cap \mathbf{Z}(\Gamma) = NE \cap \mathbf{Z}(\Gamma)$.

Since N consists of permutation matrices while E consists of diagonal matrices, we have $NE \cap D = E$. The center $\mathbf{Z}(\Gamma)$ consists of all the scalar matrices in Γ . Using $\mathbf{Z}(\Gamma) \subseteq D$ and $NE \cap D = E$, we obtain $NE \cap \mathbf{Z}(\Gamma) = NE \cap D \cap \mathbf{Z}(\Gamma) = E \cap \mathbf{Z}(\Gamma)$.

The last two paragraphs yield $\mathbf{N}_{NE}(H) \cap \mathbf{Z}(\Gamma) = E \cap \mathbf{Z}(\Gamma)$. Since $|E \cap \mathbf{Z}(\Gamma)| = |F_0|$ and $|\mathbf{Z}(\Gamma)| = q - 1$, we conclude that $|\mathbf{N}_{NE}(H)\mathbf{Z}(\Gamma)| = |\mathbf{N}_{NE}(H)|(q - 1)/|F_0|$. \square

We make use of the following result in [9] and in [10].

Theorem 4.4. *Let F_0 be any nontrivial subgroup of the multiplicative group $F^\times = F - \{0\}$ and let E be the group consisting of all diagonal matrices in Γ having the property that each entry along the diagonal belongs to F_0 . Let Q be a transitive subgroup of the symmetric group S and let $H = QE$. Suppose that E is a characteristic subgroup of H . Then $\mathbf{N}_\Gamma(H) = \mathbf{N}_S(Q)E\mathbf{Z}(\Gamma)$. Furthermore, if the field F is finite, then for $q = |F|$ we have $|\mathbf{N}_\Gamma(H)| = |\mathbf{N}_S(Q) : Q| \cdot |H|(q - 1)/|F_0|$.*

Proof. Because E is a characteristic subgroup of H , we deduce that $E \triangleleft \mathbf{N}_\Gamma(H)$ and $\mathbf{N}_\Gamma(H) \subseteq \mathbf{N}_\Gamma(E)$. Since F_0 is nontrivial, it is clear that E is a separator subgroup of Γ , and so Lemma 4.2 yields $\mathbf{N}_\Gamma(E) \subseteq M$. Hence $\mathbf{N}_\Gamma(H) \subseteq M$, and so $\mathbf{N}_\Gamma(H) = \mathbf{N}_M(H)$. Since $H = QE$ is a subgroup of SE while $\theta(H) = Q$ consists of permutation matrices and is a transitive subgroup of the symmetric group S , Theorem 4.3 implies that $\mathbf{N}_M(H) = \mathbf{N}_{NE}(H)\mathbf{Z}(\Gamma)$ where $N = \mathbf{N}_S(Q)$. Since $Q \triangleleft N$, we have $H = QE \triangleleft NE$, which says that $\mathbf{N}_{NE}(H) = NE$. Therefore $\mathbf{N}_\Gamma(H) = \mathbf{N}_M(H) = NE\mathbf{Z}(\Gamma)$, as desired.

Suppose that the field F is finite and let $q = |F|$. In view of $\mathbf{N}_\Gamma(H) = \mathbf{N}_M(H)$, Theorem 4.3 yields $|\mathbf{N}_\Gamma(H)| = |NE|(q - 1)/|F_0|$. It remains to show that $|NE| = |N : Q| \cdot |H|$. Since each of Q and N consists of permutation matrices while E consists of diagonal matrices, we have $|NE| = |N| \cdot |E|$ and $|H| = |QE| = |Q| \cdot |E|$. It follows that

$$|NE| = |N| \cdot |E| = |N : Q| \cdot |Q| \cdot |E| = |N : Q| \cdot |H|,$$

and the proof is complete. \square

We remark that in the situation and notation of Theorem 4.4, the conclusion of that result that is based on the additional assumption that the field F is finite reduces the problem of calculating the order of $\mathbf{N}_\Gamma(H)$ to the problem of calculating $|\mathbf{N}_S(T) : T|$.

In the statement of Theorem A, in case the group $\text{GL}(m, q)$ has a unique conjugacy class of subgroups whose members are isomorphic to G , the conclusion of Theorem A has a particularly simple and convenient form. The following consequence of Lemma 4.2 is used to establish this condition in the proof of Application 1.2 that appears in [9].

Lemma 4.5. *Let F be a field containing a primitive p^e th root of unity where p is some prime and e is some positive integer. Let G be any finite group containing an abelian normal p -subgroup B of exponent p^e and of rank r . Then every faithful F -representation of G of degree r is similar to a representation \mathcal{V} such that $\mathcal{V}(B)$ consists of diagonal matrices and $\mathcal{V}(G)$ consists of monomial matrices.*

Proof. Let \mathcal{X} be any faithful F -representation of G of degree n . Thus $\mathcal{X} : G \rightarrow \Gamma$ is an injective homomorphism. Since B is abelian of exponent p^e while F contains a primitive p^e th root of unity, Maschke's Theorem implies that \mathcal{X} is similar to a faithful representation \mathcal{V} such that $\mathcal{V}(B) \subseteq D$. Because \mathcal{V} is faithful, $\mathcal{V}(B)$ is an abelian p -group of rank n , and from this it is clear that $\mathcal{V}(B)$ is a separator subgroup of Γ . Thus Lemma 4.2 yields $\mathbf{N}_\Gamma(\mathcal{V}(B)) \subseteq M$. Since \mathcal{V} is faithful and $B \triangleleft G$, we have $\mathcal{V}(B) \triangleleft \mathcal{V}(G)$. It follows that $\mathcal{V}(G) \subseteq \mathbf{N}_\Gamma(\mathcal{V}(B))$. Therefore $\mathcal{V}(G) \subseteq M$, as desired. \square

Acknowledgment

We thank David Pollack for providing the argument on Dirichlet's theorem on primes in arithmetic progression that appeared in the Introduction.

References

- [1] J.N. Bray, R.A. Wilson, On the orders of automorphism groups of finite groups, *Bull. Lond. Math. Soc.* 37 (2005) 381–385.
- [2] J.N. Bray, R.A. Wilson, On the orders of automorphism groups of finite groups II, *J. Group Theory* 9 (4) (2006) 537–545.
- [3] B. Eick, Automorphism groups of 2-groups, *J. Algebra* 300 (1) (2006) 91–101.
- [4] S. Fouladi, A.R. Jamali, R. Orfi, Automorphism groups of finite p -groups of coclass 2, *J. Group Theory* 10 (4) (2007) 437–440.
- [5] G.T. Helleloid, U. Martin, The automorphism group of a finite p -group is almost always a p -group, *J. Algebra* 312 (1) (2007) 294–329.
- [6] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, New York, 1967.
- [7] I.M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994.
- [8] G. Navarro, *Characters and Blocks of Finite Groups*, Cambridge Univ. Press, London, 1998.
- [9] J.M. Riedl, Automorphisms of regular wreath product p -groups, submitted for publication.
- [10] J.M. Riedl, Automorphisms of iterated wreath product p -groups, *Canad. Math. Bull.*, in press.
- [11] J.M. Riedl, Classification of the finite p -subgroups of $\mathrm{GL}(p, \mathbb{C})$ up to isomorphism, in preparation.