ORBIT SIZES AND THE DIHEDRAL GROUP OF ORDER EIGHT

by

Nathan A. Jones, B.S.

A thesis submitted to the Graduate College of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Science
with a Major in Mathematics
May 2018

Committee Members:

Thomas Keller, Chair

Anton Dochtermann

Yong Yang

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

ACKNOWLEDGMENTS

I would like to thank Dr. Thomas Keller for being my advisor for this thesis. From the start Dr. Keller helped find a great problem to tackle. His work inspired new ways of thinking. During the time we spent together each week he had unparalleled patience and encouragement. In addition he taught my first year Algebra where I got to learn the real beauty and elegance of finite group theory.

I would also like to thank my committee members, Dr. Yong Yang, Dr. Anton Dochtermann. Dr. Yang has always been incredibly friendly and encouraging in our encounters. Dr. Dochtermann was gracious and helpful in learning about and preparing this thesis.

Finally, I would like to thank my dad who told me "there is no money in archeology, you'll starve", starting my journey of mathematical curiosity.

TABLE OF CONTENTS

Page

I. INTRODUCTION

Groups form one of the most basic structure available in abstract algebra, finding uses in a variety of areas in mathematics. In number theory the main object of study is the set of integers, a group. The solutions to polynomial equations give rise to a group. Well known results such as Euler's Theorem, Diophantine equations, and solvability of polynomial equations have all benefited from the understanding of groups and their structure [3, p.14].

A natural tool for studying groups is a group action on a set. Group actions provide a convenient way to study abstract groups. Seeing where a group can send a particular element of a set gives you a sense of that element's orbit. One question that arises is to study the sizes of these orbits. In this thesis we will be concerned with a lower bound for the largest orbit size. We will primarily concern ourselves with group actions where G is a finite nonabelian group acting on a finite faithful irreducible G-module V. It is known that $|G|/|G'|$, where G' is the commutator subgroup, serves as a lower bound for the largest orbit size of G acting on V [8]. It is even known that this inequality is either strict, or equal and G is abelian, or there are at least two orbits of the largest orbit size in the action of G on V when G is nonabelian. The next natural step is to consider what happens if there are exactly two orbits of size $|G|/|G'|$ in the action of G on V. In the cited paper the authors conjecture that this can only happen when the group is the dihedral group of order eight, while $V = V(2,3)$ is a two dimensional vector space over a field of 3 elements. In this thesis we will show that a slightly weaker version of this conjecture is in fact true.

Definitions

In this section we will formalize the terms used throughout this thesis. We

will also clarify notation which may vary in different sources. The definitions used in this paper have been taken from [6, 10] and the notation is consistent with literature in finite group theory.

This thesis will assume the reader is familiar with the basic concept of a group. A quick review of the properties of a group include a set G which is closed under a binary operation which is associative, contains an identity, and has inverses. In this thesis all groups will be finite. That is to say the size of set G, denoted $|G|$, is not infinite. An example of a group is the dihedral group on eight elements, denoted D_8. This group consists of the four rotational and four 'flip' symmetries of a square. These are represented by $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, where r can be considered a 90 degree rotation of a square, and s can be considered a flip over a fixed axis of symmetry of a square. This produces the multiplication rule $sr = r^{-1}s$.

The first structures on a group G we will consider are smaller groups inside G called subgroups. Subgroups provide a way to get an idea of the structure of larger groups. In this paper subgroups will be used to allow for induction on the group. In the case of D_8 we can look at only the set of rotations $\{1, r, r^2, r^3\}$ and see this forms a subgroup of D_8. We will define some more special subgroups.

Definition 1. A **normal subgroup** is a subgroup $H \leq G$ such that for all $g \in G$ we have $g^{-1}Hg = H$. This is denoted by $H \trianglelefteq G$, and $H \triangleleft G$ if and only if $H \trianglelefteq G$ and $H \neq G$.

Notice that a normal subgroup is a group that is invariant under conjugation by elements in G. These groups are also known to be characterized as the kernel of some group homomorphism.

Definition 2. A group G is **solvable** if there exists a chain of subgroups $1 = H_0 \triangleleft$

$H_1 \lhd ... \lhd H_n = G$ such that H_{i+1}/H_i is abelian for $i = 0, ..., n^{-1}$.

Notice this means that solvable groups are groups that are constructed by extensions of abelian groups. Solvable groups will be the focus of this paper.

Definition 3. The **Frattini subgroup**, $\Phi(G)$ is the intersection of all maximal proper subgroups of G.

The Frattini subgroup always exists in finite groups and possesses many useful properties. For example, the Frattini subgroup is always normal. In the case of D_8 we have three maximal subgroups $\{1, s, r^2, sr^2\}$, $\{1, r, r^2, r^3\}$, and $\{1, rs, r^2, sr^3\}$. Therefore $\Phi(D_8) = \{1, r^2\}$. One property of the Frattini subgroup we will benefit from is that it is nilpotent.

Definition 4. Let G be a finite group and p a prime. A **Sylow p-subgroup** of G is a subgroup $P \leq G$ such that $|P| = p^a$ is the full power of p dividing $|G|$. The set of all Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$

Definition 5. Let G be finite and solvable and let π be any set of prime numbers. Hall's Theorem guarantees a subgroup $H \leq G$ with order divisible only by primes in π with $|G|/|H|$ divisible by none of these primes. A subgroup $H \leq G$ satisfying these conditions is called a **Hall π-subgroup** of G.

The Sylow and Hall subgroups will provide us a natural way to 'split-up' groups into two subgroups using a free product.

Definition 6. A group G is called **nilpotent** if there exists a chain of subgroups $1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ such that $G_{i+1}/G_i \leq Z(G/G_i)$. Where $Z(G/G_i) = \{g \in G/G_i | gx = xg$ for all $x \in G/G_i\}$.

This formal definition can be replaced by another property that is equivalent to being nilpotent. A group G is nilpotent if and only if it can be written as the direct product of its Sylow subgroups for all primes p dividing $|G|$. Notice that because D_8 is a finite p-group that it must be a nilpotent group.

Definition 7. The **Fitting subgroup** of G, written as $F(G)$ is the unique largest normal nilpotent subgroup of G.

In the example of D_8, we would have $F(D_8) = D_8$, because D_8 is nilpotent. The Fitting subgroup will appear in relation to Gaschütz' Theorem which we will state in the next section.

Definition 8. Let H_1 and H_2 be subgroups of G. We define the **commutator** of these groups to be

$$[H_1, H_2] = \langle h_1^{-1} h_2^{-1} h_1 h_2 | h_1 \in H_1, h_2 \in H_2 \rangle.$$

The **commutator subgroup** of G is the group $[G, G]$ and denoted by G'.

The commutator subgroup is the smallest normal subgroup such that the quotient group of the group by its commutator is abelian. It turns out that $|G/G'|$ has a relation to the largest orbit size of a group action. In the case of D_8 the commutator subgroup is $\{1, r^2\}$.

Definition 9. Let X be a set and G be a group. We say that G **acts** on X if for every $x \in X$ and $g \in G$ there exists an element $x^g \in X$ such that $x^1 = x$ and $x^{gh} = x^{gh}$ for all $g, h \in G$. If G acts on X, we call this a right **group action**.

The group action is an abstraction that appears naturally among many objects in mathematics. Therefore they are worth studying in their own right. We will discuss a few properties of group actions next section.

Definition 10. Let G act on the set X and $x \in X$. The **orbit** containing x of this group action is the set $\{x^g | g \in G\}$

An orbit of an element x can be thought of informally as elements in the set that x can be taken to by an element in the group.

Definition 11. A group action is **faithful** if there is no $g \in G$ where $g \neq 1$ such that $x^g = x$ for all $x \in X$.

One will notice that a faithful action induces an injection from G to the symmetric group on X.

Definition 12. A group action of G on X is said to be **transitive** if for every two elements $x, y \in X$, there exists $g \in G$ with $x^g = y$. If this g is unique we say that the action is **regular**.

Definition 13. Let G be a group and V vector space over a field. Let G act on V such that $(a + b)^g = a^g + b^g$ for all $a, b \in V$ and $g \in G$. We call V a **G-module**.

Definition 14. Let D be a subgroup of G and V be a G-module. If we consider only the action of D on V we get a D-module denoted V_D.

Definition 15. Let V, W be G-modules. We say $V \cong W$ as G-modules if and only if there exists a vector space isomorphism $\phi : V \to W$ such that $\phi(v^g) = \phi(v)^g$ for all $v \in V$ and $g \in G$.

Definition 16. A G-module V is **irreducible** if V has no proper non-zero G-submodules.

Definition 17. A G-module V is **completely reducible** if it can be represented as the direct sum of irreducible G-modules.

Definition 18. Let V be a completely reducible G-module. Then $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ for irreducible G-modules V_i. One can write $V = W_1 \oplus \ldots \oplus W_m$ for some $m \leq n$ such that $V_i, V_j \leq W_k$ for some $i, j \in \{1, ..., n\}$ and some $k \in \{1, ..., m\}$ if and only if $V_i \cong V_j$ (as G-modules). Then the W_i are called the **homogeneous components** of V.

Definition 19. An irreducible G-module V is called **imprimitive** if V can be written as $V = V_1 \oplus ... \oplus V_n$ for $n > 1$ subspaces V_i that are permuted transitively by G. We say that V is *primitive* if V is not imprimitive. V is called **quasi-primitive** if V_N is homogeneous for all $N \triangleleft G$ (where V_N denotes V viewed as an N-module).

It is known that quasiprimitive is a weaker condition than primitive, that is primitive implies quasiprimitive. However the reverse implication is not true.

This concludes the formal definitions that will be required for the main result.

Useful Theorems and Lemmas

The following results are all known and appear in other papers relating to group theory. Their original sources have been indicated for proofs of the following results. The first lemma will come in handy when we examine abelian subgroups in our main theorem.

Lemma 1. *[8, Lemma 2.2] Let A be an abelian finite group and let V be a finite faithful completely reducible A-module. It is well-known that A has a regular orbit on V. Write $V = V_1 \oplus ... \oplus V_n$ for irreducible A-modules V_i. Suppose that A has exactly one regular orbit on V. Then $A/C_A(V_i)$ is cyclic of order $|V_i| - 1$ for all i and $A \cong \times_{i=1}^{n} A/C_A(V_i)$ is of order $\prod_{i=1}^{n}(|V_i| - 1)$.*

The following theorem is of key importance in our paper. It is the main re-

sult of [8] and will be used throughout the paper. In particular this paper is concerned with expanding the third case, however the first two cases will also be used to show our result. The following theorem will reference modules of mixed characteristic. Mixed characteristic means that if $V = V_1 \oplus \ldots V_n$ then V_i and V_j need not have the same characteristic for all $i, j \in \{1, \ldots, n\}$

Theorem 1. *[8, Theorem 2.3] Let G be a finite solvable group and V a finite faithful completely reducible G-module, possibly of mixed characteristic. Let M be the largest orbit size in the action of G on V. Then*

$$|G/G'| \leq M$$

More precisely, we have one of the following

1. $|G/G'| < M$

2. $|G/G'| = M$ *and G is abelian; or*

3. $|G/G'| = M$, G *is nilpotent, and G has at least two different orbits of size M on V.*

The following Lemma is well-known and very useful. The reader may recognize this as a consequence of the isomorphism theorems.

Lemma 2. *[8, Lemma 2.1] Let G be a finite group and $N \trianglelefteq G$. Then*

$$|G/G'| = |G/G'N| \cdot |N : N \cap G'|;$$

and

$$|G : G'| \quad divides \quad |G/N : (G/N)'| \cdot |N : N'|.$$

7

Gaschütz' Theorem will be used in the main proof to make a reduction to nilpotent groups. This will allow us to narrow the scope of possible cases needed to prove the result.

Theorem 2 (Gaschütz' Theorem). *[10, p.37] Let G be solvable. Then $F(G/\Phi(G)) = F(G)/\Phi(G)$ is a completely reducible and faithful $G/F(G)$-module (possibly of mixed characteristic). Furthermore, $G/\Phi(G)$ splits over $F(G)/\Phi(G)$.*

Lemma 3. *Let $D_8 \leq GL(2,3)$ (invertible 2x2 matrices on the field of three elements) act on $V(2,3) = V$. Let $N \triangleleft D_8$ with N being a Klein-4 group. Then N has exactly one orbit of size four on V. If K is the other Klein-4 subgroup of D_8, then the orbit of size 4 from K acting on V is different than the orbit of size four of N acting on V.*

Proof. Let $N = \{1, r, s, sr^2\}$ and $K = \{1, r^2, sr, sr^3\}$, the two subgroups of D_8 isomorphic to the Klein-4 group. Denoting $V(2,3)$ by (i,j) where i and j are integers such that $-1 \leq i \leq 1$ and $-1 \leq j \leq 1$. Using right multiplication with

$$r = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

we can calculate the two orbits of size four. When K acts on V the orbit of size four is $\{(1,1), (1,-1), (-1,1), (-1,-1)\}$ while the orbit of size four in the action of N on V is $\{(1,0), (-1,0), (0,-1), (0,1)\}$. This concludes the proof of Lemma 3   □

II. EXAMPLES AND STATEMENT OF RESULT

The following theorem is similar to a conjecture in [8] before becoming the topic of this thesis. It will expand upon the third case of Theorem 1 in this paper by considering the case where G is nonabelian, $|G|$ is not divisible by a Mersenne prime and has exactly two orbits of size M on V and V is irreducible. Our claim is that this can only happen if and only if $G = D_8$ and $V = V(2,3)$, the vector space of dimension two over the field of three elements. These orbits can be calculated by the reader using the following matricies for r and s. The operation will be right multiplication of matrices on the elements of V. We can generate D_8 by using the following matrices to generate a subset of the general linear group $\mathrm{GL}(2,3)$.

$$r = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The orbits can also be represented in the following picture. Imagine arranging these points in a 3 by 3 grid as they appear in the familiar xy-axis. The two orbits can be seen with the connecting lines, both of size 4, while $(0,0)$ remains as a fixed point. Notice we see two squares, the symmetries of which are described by D_8.
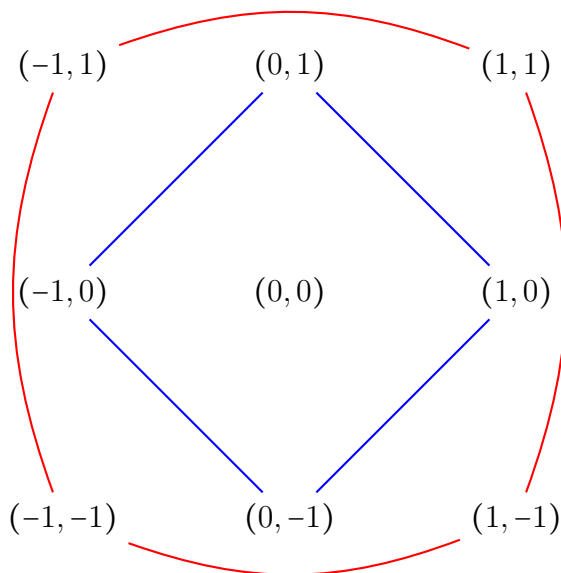
If we recall the size of D_8 and the size of D_8' we see that $|D_8 : D_8'| = 4$ and this action satisfies conditions of the next theorem.

Theorem 3. *Let G be a finite nonabelian solvable group and V a finite faithful irreducible G-module Suppose that $M = |G/G'|$ is the largest orbit size of G on V, $|G|$ is not divisible by a Mersenne prime, and that there are exactly two orbits of size M on V. Then G is dihedral of order 8, and $V = V(2,3)$.*

We note that the original conjecture did not contain the added hypothesis that $|G|$ is not divisible by Mersenne prime. We still believe that the conjecture holds without this condition, but have not found a way to dispense of the added hypothesis in one case of our proof. Further work will be done in order to remove this extra hypothesis.

III.   PROOF OF MAIN RESULT

Proof. In this proof we will use induction on the size of our group $|G|$ several times.

We begin the proof by making a reduction and showing that if G is not a nilpotent group it will not satisfy the conditions of our theorem.

If G is not nilpotent then the proof of Theorem 2.3 in [8] shows that the largest orbit size of G on V is less than M. Here we reproduce the argument for the convenience of the reader.

A Reduction to Nilpotent Groups

Suppose G is not nilpotent. Write $F = F(G)$ for the Fitting subgroup and $\Phi = \Phi(G)$ for the Frattini subgroup of G. As G is not nilpotent, we have $F < G$, and since F is normal in G, V is completely reducible as an F-module. Hence by Theorem 2.0.2 applied to the action of F on V, we have that

$$|F/F'| \le M. \tag{1}$$

Moreover, by Gaschütz' Theorem it is well-known that F/Φ is a faithful, completely reducible G/F–module (possibly of mixed characteristic). We now write $F/\Phi = W_1 \oplus W_2$, where $W_1 = (F \cap G')\Phi/\Phi$ and W_2 is G-invariant complement of W_1 in F/Φ. Hence

$$W_2 \cong (F/\Phi)/W_1 \cong F/(F \cap G'\Phi) \quad \text{as } G\text{-modules.}$$

We now claim that G/F acts trivially on W_2. For this it suffices to show that G acts trivially on $F/F \cap G'\Phi$. So let $g \in G$ and $x \in F$. Then

11

$$(x(F \cap G')\Phi)^g = x^g(F \cap G')\Phi = x[x,g](F \cap G')\Phi = x(F \cap G')\Phi,$$

the last equality being true since $[x,g] \in F \cap G'$. This proves our claim.

Now as G/F is faithful on F/Φ, but acts trivially on W_2, we see that W_1 is a faithful completely reducible G/F-module (of possibly mixed characteristic). Thus by Theorem 2.0.2 we conclude that

$$|G : FG'| = |(G/F) : (G/F)'| < |W_1|. \tag{2}$$

So altogether with (3.1) and (3.2) we conclude that

$$|G/G'| = |G : FG'||FG'/G'| < |W_1| \cdot |FG'/G'| = |(F \cap G')\Phi/\Phi||F : (F \cap G')|$$

$$= |(F \cap G')/(F \cap G' \cap \Phi)||F : (F \cap G')|$$

$$\leq |(F \cap G') : F'| \cdot |F : (F \cap G')|$$

$$= |F/F'| \leq M$$

This gives us $|G/G'| < M$ contradicting our hypothesis. Therefore we know that G must be nilpotent. This concludes the argument from [8].

A Reduction to p-groups

We can further make a reduction to p-groups. Assume that $|G|$ is divisible by at least two distinct primes, one of which we will call p. Let $P \in \mathrm{Syl}_p(G)$ and $H \in \mathrm{Hall}_{p'}(G)$. It is known that because G is nilpotent, $P \lhd G$ [6, p.89]. Moreover we can write $G = P \times H$ [6, Theorem 8.11]. V is a finite G-module over a field, call

it K. By [11, Lemma 10] there exists a field extension L of K such that if U is an irreducible summand of V viewed as an LG-module, then the permutation actions of G on V and U are permutation isomorphic. We may consider the action of G on U instead. With relabeling we can assume that V is absolutely irreducible. By [1, (3.6)] we may assume $V = X_1 \otimes X_2$, where X_1 is a faithful irreducible P-module and X_2 is a faithful irreducible H-module. By Theorem 2.0.2 we can choose $x_1 \in X_1$ and $x_2 \in X_2$ such that

$$|P/P'| \le |x_1^P|,$$

$$|H/H'| \le |x_2^H|.$$

Clearly we may assume that $|x_1^P|$ is the largest orbit size of P on X_2, and $|x_2^H|$ is the largest orbit size of H on X_2. Using [9, Lemma 3.3] if $g \in P$ and $h \in H$ such that $gh \in C_G(x_1 \otimes x_2)$ then $x_1 g = \alpha x_1$ and $x_2 h = \beta x_2$ where α, β are scalars in the field with $\alpha\beta = 1$. Now g and h have coprime orders so we have that $\alpha = \beta = 1$ which gives

$$C_G(x_1 \otimes x_2) = C_P(x_1) \times C_H(x_2).$$

This gives the following

$$|G/G'| = M \ge |(x_1 \otimes x_2)^G| = |G : C_p(x_1) \times C_H(x_2)| \tag{3}$$

$$= |P : C_P(x_1)||H : C_H(x_2)|$$

$$= |x_1^P||x_2^H| \ge |P/P'||H/H'| = |G/G'|.$$

This shows that we have equality everywhere in 3, and so $|x_1^P| = |P/P'|$, and $|x_2^H| = |H/H'|$. Therefore $|P/P'|$ is the largest orbit size of P on X_1 and $|H/H'|$ is the largest orbit size of H on X_2.

Suppose that P and H have exactly one maximal orbit of size $M_1 = |P/P'|$ and $M_2 = |H/H'|$ on X_1 and X_2 respectively. By Theorem 1 P and H would be abelian groups. Then $G = P \times H$ would be abelian, a contradiction. Therefore, one of the following holds, P has at least two orbits of size M_1 on X_1, or H has at least two orbits size M_2 on X_2.

We will now show that P has no more than two orbits of size M_1 on X_1 and H has no more than two orbits of size M_2 on X_2. The argument will be the same in both cases. We assume P has three orbits of maximal size on X_1. Let $y_1, y_2 \in X_1$ be the representatives of the remaining two orbits. Then as in (3.3)

$$|(x_1 \otimes x_2)^G| = |(y_1 \otimes x_2)^G| = |(y_2 \otimes x_2)^G| = M,$$

making three orbits of size M when G acts on V contradicting our hypothesis. Using a similar argument we see that H cannot have more than two orbits of size M_2 on X_2.

We now will show that either P cannot have two orbits of size M_1 on X_1 or H cannot have two orbits of size M_2 on X_2. If P and H both have two orbits of maximal size we have $y_1 \in X_1$ as a second representative of an orbit size M_1 and $y_2 \in X_2$ a second representative of an orbit of size M_2 of P and H, respectively. Whenever it is assumed that P and H have a second orbit we will call upon these elements to represent the second orbit. Then, again proceeding as in (3.3), we see that

$$|G/G'| = |(x_1 \otimes x_2)^G| = |(x_1 \otimes y_2)^G| = |(y_1 \otimes x_2)^G| = |(y_1 \otimes y_2)^G| = M$$

creating four orbits of size M in the action of G on V, a contradiction. Therefore P has exactly two orbits of maximal size on X_1 or H has exactly two orbits of maxi-

mal size on X_2 but not both. Next we consider what happens in these two cases.

First we consider the case where P has two orbits of size $|P/P'|$ on X_1. H must have exactly one orbit of size $|H/H'|$ on X_2. Notice that $(x_1 \otimes x_2)^G$ and $(y_1 \otimes x_2)^G$ are two distinct orbits of G of size M. By part 2 of Theorem 1 H must be abelian. Thus $|H/H'| = |H| = |x_2^H|$, by Lemma 1 $H \cong H/C_H(X_2)$ and H is a cyclic group of order $|X_2| - 1$. We know that P is not abelian, since if it were, then $G = P \times H$ would be abelian. Therefore we can use induction, $P = D_8$ and $X_1 = V(2,3)$. This makes char$(X_1) = 3$ so char$(X_2) = 3$. Therefore $|H| = 3^n - 1$ for some $n \in \mathbb{N}$ making $|H|$ even. This contradicts that $P \in \mathrm{Syl}_2(G)$. Therefore P cannot have two orbits size $|P/P'|$ on X_2.

We now consider the case that H has two orbits of size $|H/H'|$ on X_2. Then P has one orbit of size $|P/P'|$ on X_1. By Theorem 1 part 2 P is an abelian group and by Lemma 1 P is cyclic of order $|X_1| - 1$. We can see that H is not abelian, if it were $G = H \times P$ would be abelian. Using induction we see that $H = D_8$ and $X_2 = V(2,3)$. This means $|H| = 8$ and char$(X_1) =$char$(X_2) = 3$ and $|P| = |X_1| - 1 = 3^n - 1$, for some $n \in \mathbb{N}$. Therefore $|P|$ is even contradicting $\gcd(|H|,|G|) = 1$. This shows that G must be a p-group.

The Case Where V is Quasiprimitive

Consider the case where V is quasiprimitive. Using the proof of Theorem 3.3 in [10] we know $G = S \times T$ where T is cyclic of odd order and S a 2-group. There also exists a $U \lhd G$ where U is cyclic, $|G : U| \leq 2$ and U has a regular orbit on V. This gives the inequality $M \geq |U| \geq |G|/2$. Because G is a nonabelian p-group we have $|T| = 1$ and $G = S$, and $p = 2$. By Corollary 1.3 in [10] G is cyclic, quaternion, dihedral, or semi-dihedral and $G \ncong D_8$. G is not abelian so $|G| > 4$ and $8 \| |G|$. It is also known that the derived subgroup of the quaternion,

15

dihedral, and semi-dihedral 2-groups have index 4 [7, proof of Theorem A]. That is $|G/G'| = 4 \leq |G|/2 \leq M$. Here we have equality so $|G'| = 2$, $|G| = 8$. This makes G the quaternion group. It is known that the quaternion group has a regular orbit on V [10, Lemma 4.2(a)] contradicting $M = 4$. Therefore V can not be quasiprimitive.

The Case Where V is Quasiprimitive

From now on we may assume that V is not quasiprimitive. In particular, V is imprimitive. By Corollary 0.3 in [10] there exists a $D \trianglelefteq G$ with $|G : D| = p$ where p is prime and $V_D = V_1 \oplus \ldots \oplus V_p$ for irreducible D-modules V_i of V_D. We will consider two cases, $D' < G'$ and $D' = G'$.

The Case Where $D' < G'$

For the first case suppose that $D' < G'$, that is, $p|D'| \leq |G'|$. Using Theorem 1 we have the following inequality

$$M \geq |D : D'| = \frac{|D|}{|D'|} = \frac{p|D|}{p|D'|} \geq \frac{|G|}{|G'|} = M.$$

Therefore $|D : D'| = M$. Because $\cap_{i=1}^{p} C_G(V_i) = 1$ we have that D is isomorphic to a subgroup of $D/C_D(V_1) \times \ldots \times D/C_D(V_p)$ [8, equation (4)]. We will use the symbol $H \lesssim G$ to denote that H is isomorphic to a subgroup of G. Then

$$D \lesssim D/C_D(V_1) \times \ldots \times D/C_D(V_p) = \bigtimes_{i=1}^{p} D/C_D(V_i) =: T. \tag{4}$$

Notice that the above equation tells us that if $D/C_D(V_i)$ is abelian for any $i = 1, \ldots, p$ then $D/C_D(V_i)$ is abelian for all $i = 1, \ldots, p$ and D must be abelian. We will use this fact several times in the following arguments.

From Theorem 1, having $|D : D'| = M$ shows that D is abelian or has exactly two orbits of size M on V_D. We know D cannot have more than two orbits of size

16

M on V_D, otherwise G would have more than two orbits of size M on V or an orbit larger than size M.

Recall that $V_D = V_1 \oplus V_2 \oplus ... \oplus V_p$, with V_i irreducible faithful D-modules. Let $W_i = \oplus_{j=1, j \neq i}^p V_j$. Write M_1 for the largest orbit of size D on V_1 and M_2 for the largest orbit of size $C_D(V_1)$ on W_1. Also let M_D be the largest orbit size of D on V. Let $x \in V_D$ be in a largest orbit of D on V_D. Write $x = x_1 + x_2$ for some $x_1 \in V_1$ and $x_2 \in W_1$. Observe that

$$M_D = |D : C_D(x)| = |D : C_D(x_1) \cap C_D(x_2)| =$$

$$|D : C_D(x_1)||C_D(x_1) : C_D(x_1) \cap C_D(x_2)| = |x_1^D||x_2^{C_D(x_1)}|.$$

If $|x_1^D| < M_1$, then the same calculation would show that if $y_1 \in V_1$ with $|y_1^D| = M_1$, then $|D : C_D(y_1 + x_2)| > M_D$, contradicting the definition of M_D. Thus we have $|x_1^D| = M_1$. Moreover, since $|x_2^{C_D(x_1)}| \geq |x_2^{C_D(V_1)}|$. We also can conclude that $|x_2^{C_D(x_1)}| \geq M_2$, because if $|x_2^{C_D(x_1)}| < M_2$, then let $y_2 \in W_1$ such that $|y_2^{C_D(V_1)}| = M_2$, and then

$$M_D = |(x_1 + y_2)^D| = |D : C_D(x_1) \cap C_D(y_2)| = |D : C_D(x_1)||C_D(x_1) : C_D(x_1) \cap C_D(y_2)|$$

$$M_1|y_2^{C_D(x_1)}| = M_1 M_2 > M_1|x_2^{C_D(x_1)}| = |D : C_D(x)| = M_D,$$

a contradiction. Thus altogether we get $M \geq M_D \geq M_1 M_2$. Then

$$M \geq |x^D| = |D : C_D(x)| = |D : C_D(x_1) \cap C_D(x_2)|$$

$$= |D : C_D(x_1)||C_D(x_1) : C_D(x_1) \cap C_D(x_2)| = M_1|x_2^{C_D(x_1)}| \geq M_1|x_2^{C_D(W_1)}| = M_1 M_2.$$

By applying Theorem 2 $|D : D'|$ divides $|D/C_D(V_1) : D/C_D(V_1)'||C_D(V_1)/C_D(V_1)'|$

and we have

$$M \geq M_1 M_2 \geq |D/C_D(V_1) : (D/C_D(V_1)')||C_D(V_1) : C_D(V_1)'| \geq |D : D'| = M.$$

This shows $M_1 M_2 = M_D = M$. It also follows that $M_1 = |D/C_D(V_1) : (D/C_D(V_1))'|$ and $M_2 = |C_D(V_1) : C_D(V_1)'|$. Suppose there exists $y_1, z_1 \in V_1$ where y_1 and z_1 are representatives of two new orbits of size M_1 of $D/C_D(V_1)$ acting on V_1, then arguing as we have previously $x_1 + y_2, y_1 + x_2$ and $z_1 + x_2$ are three representatives of orbits of size M of D on V_D. This contradicts our hypothesis. So $D/C_D(V_1)$ has at most two orbits of size M_1 on V_1. We also know that if $D/C_D(V_1)$ has exactly one orbit of size M_1 on V_1 then $D/C_D(V_1)$ is abelian by Theorem 1, and by (4) D is abelian. Therefore if D is abelian, then $D/C_D(V_1)$ has exactly two orbits of size M_1 on V_1.

First we will consider the case that D is nonabelian.

The case where D is nonabelian.

We know by (4) that $D/C_D(V_1)$ is not abelian, for the reason listed above. As argued before $C_D(V_1)$ must have exactly one orbit of size M_2 on W_1, otherwise G would have too many orbits of size M. By induction $D/C_D(V_1) = D_8$, $V_1 = V(2,3)$, and $p = 2$ so $|W_1| = |V_1| = |V_2|$. We have $D \lesssim D/C_D(V_1) \times D/C_D(V_2) \cong D_8 \times D_8$ making $C_D(V_1) \lesssim D_8$. If $C_D(V_1) \cong D_8$ then $C_D(V_1)$ has two orbits of size M_2 on V_2. Contradicting $C_D(V_1)$ having exactly one orbit of size M_2 on $W_1 = V_2$. Therefore $C_D(V_1)$ is of order one, two or four. This makes $C_D(V_1)$ abelian which gives it at least two regular orbits (i.e, two orbits of size $M_2 = |C_D(V_1)|$) unless $C_D(V_1)$ is the Klein four-group.

Since $C_D(V_1)$ has only one orbit of size M_2 on V_2, we conclude that $C_D(V_1)$ is the Klein four-group. Since $C_D(V_1)$ and $C_D(V_2)$ are conjugate under the action

of G, then $C_D(V_2)$ is also a Klein four-group. Let $v_1 \in V_1$ be in an orbit of size $M_1 = 4$ of $D/C_D(V_1)$ on V_1, such that v_1 is in a regular orbit of $C_D(V_2)$ on V_1 by Lemma 3. Now $|C_D(v_1)| = 8$, $C_D(v_1) \cap C_D(V_2) = 1$, therefore

$$C_D(v_1) \cong C_D(v_1)/(C_D(v_1) \cap C_D(V_2)) \cong C_D(v_1)C_D(V_2)/C_D(V_2) \cong D/C_D(V_2) \cong D_8$$

where the third isomorphism comes from the isomorphism theorems. Hence we have $C_D(v_1) \cong D_8$. Therefore $C_D(v_1)$ acts faithfully on V_2 and if $z_1, z_2 \in V_2$ are representatives of the the two orbits of size four in the action fo $C_D(v_1)$ on V_2, then $v_1 + z_1$ and $v_1 + z_2$ are representatives of two orbits of size $16 = M_D = M$ of D on V_D. Now let $w_1 \in V_1$ be in an orbit of D of size $M_1 = 4$ such that w_1 is not in a regular orbit of $C_D(V_2)$ on V_1. Let $z_3 \in V_2$ be in the (unique) regular orbit of $C_D(V_1)$ on V_2 (so it is of size $M_2 = 4$). Then clearly $w_1 + z_3$ is a representative of an orbit of size $16 = M$ of D on V, and this orbit is different from this orbit containing $v_1 + z_1$ and $v_1 + z_2$. Thus we have found three orbits of size $16 = M$ of D on V which contradicts our hypothesis. This concludes the case where D is nonabelian.

<div align="center">

The Case Where D is Abelian.

</div>

We will consider two possibilities, that D has exactly one orbit of size M or D has exactly two orbits of size M on V.

<div align="center">

The Case Where D has Exactly One Orbit Size M.

</div>

In the proof of Theorem 1 in [8] it is shown that this results in $G = D_8$ and $|V| = 9$. The following argument has been reproduced for completeness.

Since D is abelian, D has regular orbits, so $M = |D|$. Hence, D has exactly one regular orbit on V, therefore by Lemma 1 we have $D = \bigtimes_{i=1}^{p} C_D(W_i)$. Notice that G/D cycles these direct factors around, therefore we see that $|G : G'| =$

$p|C_D(W_1)|$ (see [5]). Additionally, $|G/G'| = |D| = |C_D(W_1)|^p$ which implies that $|C_D(W_1)|^{p-1} = p$. This forces $p = 2$ and $|C_D(W_1)| = 2$. It follows that $|D| = 4$, D is elementary abelian, $|G| = 8$, and G is nonabelian. Because $M = |D| = 4$, G does not have a regular orbit on V, making G the dihedral group of order 8. D is elementary abelian and has exactly one regular orbit on V so we conclude that $|V| = 9$. This is a second verification that D_8 satisfies our hypothesis and ends the case from [8].

The Case Where D has Exactly Two Orbits of Size M.

Assume that D has exactly two regular orbits on V. As before we will denote the largest orbit size of the action of $D/C_D(V_1)$ on V_1 as M_1, and M_2 will denote the largest orbit size of $C_D(V_1)$ acting on W_1. Recall that $D/C_D(V_1)$ has at most two orbits of size M_1 on V_1. So the $D/C_D(V_i)$ for $i = 1, \ldots, p$ are all isomorphic and $D/C_D(V_i)$ has either one or two orbits of size M_1 acting on V_i.

Suppose we have two orbits of size M_1 in the action of $D/C_D(V_1)$ on V_1, then as argued before $C_D(V_1)$ has exactly one orbit of size M_2 on W_1. Using Theorem 1 part (2) we see that $C_D(V_1)$ is abelian. Using induction we see that $D/C_D(V_1) \cong D_8$, however the quotient of an abelian groups must be abelian creating a contradiction.

Hence we know that $D/C_D(V_1)$ has only one orbit of size M_1 in the action of $D/C_D(V_1)$ on V_1 and $C_D(V_1)$ has exactly two orbits of size M_2 on W_1. Hence we have $|D/C_D(V_1)| = |V_1| - 1$, and $D/C_D(V_1)$ is cyclic. Now by (3.4) we have $D \lesssim \bigtimes_{i=1}^{p} D/C_D(V_i) =: T$ and T has exactly one regular orbit on V. Every regular orbit of T on V splits into $\frac{|T|}{|D|}$ regular orbits of D. Since D has no more than two orbits of size $M = M_D(= |D|)$, we see that $\frac{|T|}{|D|} \le 2$. If $\frac{|T|}{|D|} = 1$, then $T = D$ and so $C_D(V_1) \cong \bigtimes_{i=1}^{p} D/C_D(V_i)$ has only one regular orbit (i.e., of size M_2) on W_1, a contradiction.

Therefore we know that $\frac{|T|}{|D|} = 2$. From Lemma 1 we have that $|T| = (|V_i| - 1)^p$,

thus

$$(|V_1| - 1)^p = 2|D| = 2p^k \tag{5}$$

for appropriate k. Hence 2 divides the right hand size, so 2^p divides the left hand size, this forces $p = 2$ and $V = V_1 \oplus V_2$. We wish to show that $|C_D(V_1)| = 2$. Observe that $C_D(V_1) \cap C_D(V_2) = 1$ and so $C_D(V_1) \times C_D(V_2) = C_D(V_1)C_D(V_2) \leq D$. Let $g \in G - D$ and $(1, a) \in C_D(V_1) \times C_D(V_2)$, then G' contains the element

$$[(1, a), g] = (1, a)^{-1}g^{-1}(1, a)g = (1, a)^{-1}(1, a)^g = (1, a^{-1})(a^*, 1) = (a^*, a^{-1})$$

for suitable $a^* \in C_D(V_1)$. If there are more than two choices for $a \in C_D(V_2)$ then $|G'| \geq 3$. On the other hand, $\frac{|G|}{|G'|} = |D|$ and $\frac{|G|}{|D|} = 2$ so $|G'| = |G|/|D| = 2$. We conclude that $|C_D(V_1)| \leq 2$. If $|C_D(V_1)| = 1$ then $D = D/C_D(V_1)$, but we know that D has exactly two orbits of size M_1 on V_1 while $D/C_D(V_1)$ has only one orbit of size M_1 on V_1. Therefore we can say $|C_D(V_1)| = 2$.

We can now determine $|D|$ using (5) we have that $\frac{|T|}{|D|} = \frac{|D/C_D(V_1)||D/C_D(V_2)|}{|D|} = 2$. This implies $2|D| = \frac{|D|}{2}\frac{|D|}{2} = \frac{|D|^2}{4}$, or $|D| = 8$ and $|G| = 16$. From Lemma 1 $|D/C_D(V_1)| = |V_1| - 1$ giving us $|V_1| = 5, i = 1, 2$. So we can identify V_i with $\mathrm{GF}(5)$, and thus $V = \mathrm{GF}(5)^2$. Then $\{(1, 0), (2, 0), (3, 0), (4, 0)\}$ and $\{(0, 1), (0, 2), (0, 3), (0, 5)\}$ are both orbits of D on V (as $D/C_D(V_1)$ has an orbit of size 4 on V_i), and their union is an orbit of size 8 of G on V. Moreover, if $a, b \in \mathrm{GF}(5) - \{0\}$, then $(a, b)^D$ will contain $(a, -b)$, since $C_D(V_1)$ acts as $x \to -x$ on V_2. Since $D/C_D(V_1)$ has an orbit of size 4 on V_1, we also see that $(a, b)^D$ will contain elements of the form $(1, *), (2, *), (3, *)$, and $(4, *)$. Altogether we see that $|(a, b)^D| = 8 = M$. Putting this together shows that, since $8 = M$, G has three orbits of size 8 on V, contradicting the hypothesis.

This concludes the case where $D' < G'$.

The Case where $D' = G'$

We will consider the action of $D/C_D(V_1)$ on V_1 and $C_D(V_1)$ acting on W_1. Using Theorem 1, we have the following inequalities

$$|D : D'C_D(V_1)| \leq M_1 \tag{6}$$

$$|C_D(V_1) : C_D(V_1)'| \leq M_2 \tag{7}$$

where M_1 is the largest orbit size of $D/C_D(V_1)$ on V_1 and M_2 is the largest orbit size of $C_D(V_1)$ on W_1. There are now four cases to consider; strict inequality in (6) and (7), strict inequality in (6) or (7) but not both, and equality in (6) and (7).

First we consider the case where we have strict inequality in (6) and (7). Because G is a p-group we know that $p|D : D'C_D(V_1)| \leq M_1$ and $p|C_D(V_1) : C_D(V_1)'| \leq M_2$. Therefore

$$M \geq M_1 M_2 \geq p^2 |D : D'C_D(V_1)||C_D(V_1) : C_D(V_1)'|.$$

Recall $|G : D| = p$ and notice that $|D : D'| \leq M_D \leq pM_1M_2$ so

$$p^2|D : D'C_D(V_1)||C_D(V_1) : C_D(V_1)'| \geq p|G : D||D : D'| = p|G : D'| = p|G : G'| > |G : G'|.$$

Putting the above equations together we have $|G : G'| < M$. This contradicts our hypothesis that $|G : G'| = M$, and therefore either (6) or (7) must be an equality.

Suppose that (6) is equal, that is $|D : D'C_D(V_1)| = M_1$. If $D/C_D(V_1)$ is abelian then by (4) we have D is abelian. If D is abelian then $1 = D' = G'$ and G

22

is abelian, a contradiction. Therefore we note that $D/C_D(V_1)$ cannot be abelian for the rest of the paper. By Theorem 1 we have that $D/C_D(V_1)$ has at least two orbits of size M_1 on V_1. Let $v_1, v_2 \in V_1$ be representatives of two different orbits of size M_1 in the action of $D/C_D(V_1)$ on V_1. Let $w \in W_1$ be in an orbit of size M_2 in the action fo $C_D(V_1)$ on W_1.

Because (7) is strict, we have $p|C_D(V_1) : C_D(V_1)'| \leq M_2$. This gives us the following,

$$M \geq |(v_i + w)^G| \geq |v_i^{D/C_D(V_1)}||w^{C_D(V_1)}| = M_1 M_2$$

$$\geq p|D : D'C_D(V_1)||C_D(V_1) : C_D(V_1)'| \geq |G : G'| = M$$

for $i = 1, 2$. This gives equality everywhere. By hypothesis G has exactly two orbits of size M on V. This means $D/C_D(V_1)$ has exactly two orbits of size M_1 on V_1. By induction $D/C_D(V_1) \cong D_8$, $|V_1| = 9$ and $p = 2$. Thus $M_1 = 4$, and clearly $M_2 \leq 4$. This gives us $C_D(V_1) \leq D_8$. If $C_D(V_1) \cong D_8$ then $|C_D(V_1) : C_D(V_1)'| = 4$ contradicting (7) is strict. Therefore $C_D(V_1)$ is size one, two, or four. This makes $C_D(V_1)$ abelain. That means $M_2 = |C_D(V_1)| = |C_D(V_1) : C_D(V_1)'|$ which contradicts (7) is strict. Therefore we know that (7) cannot be strict when (6) is equal.

We now consider the case that (6) and (7) are equalities. That is $|D : D'C_D(V_1)| = M_1$ and $|C_D(V_1) : C_D(V_1)'| = M_2$. Then

$$M = |G : G'| = p|D|/|D'| = p|C_D(V_1) : D'C_D(V_1)|C_D(V_1) : C_D(V_1) \cap D'| \leq pM_1 M_2$$

also,

$$M \geq M_D \geq M_1 M_2,$$

so $M_1 M_2 \leq M_D \leq M \leq pM_1 M_2$. We know that exactly one of these inequalities is strict because $|D|/|D'| < p|D|/|D'| = |G|/|G'| = M$. We now have three cases to

23

consider.

In all of these cases we know that $D/C_D(V_1)$ has at least two orbits of size M_1 on V_1, otherwise $D/C_D(V_1)$ would be abelian, making $D' < (\bigtimes_{i=1}^{p} D/C_D(V_i))' = 1$. Then we would have $D' = G' = 1$, contradicting that G is not abelian. Throughout the following arguments we will let $v_1, v_2 \in V_1$ be representatives of two orbits of size M_1 on V_1.

We consider that $M_1 M_2 = M_D = M < pM_1 M_2$. Assume that $v_3 \in V_1$ is a third orbit of size M_1 in the action of $D/C_D(V_1)$ on V_1. Then let $w_1 \in W_1$ be a representative of an orbit of size M_2 in the action of $C_D(V_1)$ on W_1. This gives us $(v_1 + w_1)^D, (v_2 + w_1)^D$, and $(v_3 + w_1)^D$; three orbits of size $M_D = M$ on V. Thus we have three orbits are of size M in the action of G on V, a contradiction. Therefore $D/C_D(V_1)$ has exactly two orbits of size M_1 on V_1. Let $w_1, w_2 \in W_1$ be representatives of distinct orbits of size M_2 in the action of $C_D(V_1)$ on W_1. We see $(v_1 + w_1)^D, (v_1 + w_2)^D, (v_2 + w_1)^D$, and $C_D(v_2 + w_2)^D$ are four orbits of size $M_D = M$ on V, a contradiction. Therefore we know that $C_D(V_1)$ has exactly one orbit of size M_2 on W_1. By Theorem 1 we see that $C_D(V_1)$ is abelian. By induction we have that $D/C_D(V_1) \cong D_8, p = 2$, and $V_1 = V_2 = V(2,3)$. Therefore we have $C_D(V_1) \times C_D(V_2) \lesssim D \lesssim D/C_D(V_1) \times D/C_D(V_2)$ and $C_D(V_1) \leq D/C_D(V_1) \cong D_8$.

If $|C_D(V_1)| = 8$, then $C_D(V_1) \cong D_8$, contradicting $C_D(V_1)$ is abelian. If $|C_D(V_1)| = 4$, then $C_D(V_1)$ must be the Klein-4 which we have previously shown to be a contradiction. If $|C_D(V_1)| = 2$, then $C_D(V_1)$ is Z_2, the cyclic group of order two. If we examine the table above we see that all subgroups of D_8 of order two have at least three orbits of size two in the action on V_2. This is a contradiction. If $|C_D(V_1)| = 1$, then $D/C_D(V_1)$ has two orbits of size four in the action of $D/C_D(V_1)$ on V_1 and $D/C_D(V_2)$ has two orbits of size four in the action of $D/C_D(V_2)$ on V_2. Therefore D has either four orbits of size four or an orbit of size eight. This contra-

dicts that G has exactly two orbits of size $M = M_1 M_2 = 4$ in the action of G on V. Therefore we know that $M_1 M_2 = M_D = M$ cannot occur.

Suppose that $M_1 M_2 < M_D = M = p M_1 M_2$. This gives us $|D|/|D'| < M_D$ and we know $D/C_D(V_1)$ has at least two orbits of size M_1 in the action of $D/C_D(V_1)$. We claim that $D/C_D(V_1)$ must have exactly two orbits of size M_1 on V_1. Let $w \in W_1$ be such that $|(v_1 + w)^D| = M_D = M$. Then any $g \in G - D$ will stabilize the orbit $(v_1 + w)^D$. In particular, there is a $g \in G - D$ such that $(v_1 + w)^g = v_1 + w$. Assume that $g \in G - D$ also fixes $(v_2 + w)^D$; then $(v_2 + w)^g = (v_2 + w)^{d_0} = v_2^{d_0} + w^{d_0}$ for some $d_0 \in D$. Recall that $g \in G - D$ cycles around the elements of the components $V = V_1 \oplus \ldots \oplus V_p$. The first component of $(v_1 + w)^g$ and $(v_2 + w)^g$ are therefore the same, they are also v_1 and $v_2^{d_0}$ respectively. This means $v_1 = v_2^{d_0}$ contradicting v_1, v_2 are from different $D/C_D(V_1)$–orbits on V_1. Hence g cannot fix the orbit $(v_2 + w)^D$. Therefore

$$M \geq |(v_2 + w)^G| \geq p|(v_2 + w)^D| \geq p M_1 M_2 = M.$$

Thus $(v_1 + w)^G$ and $(v_2 + w)^G$ are two orbits of size M in the action of G on V. We can then repeat this argument to show $(v_3 + w)^D$ must be a third distinct orbit of size $M_D = M$, a contradiction. Therefore $D/C_D(V_1)$ has exactly two orbits of size M_1 on V_1. By induction we have $D/C_D(V_1) \cong D_8, p = 2, V_1 = V_2 = V(2, 3)$. We also know $C_D(V_1) \times C_D(V_2) \lessapprox D \lessapprox D/C_D(V_1) \times D/C_D(V_1) \cong D_8 \times D_8$, and $C_D(V_1) \leq D_8$. This tells us $|C_D(V_1)| \in \{1, 2, 4, 8\}$.

If $|C_D(V_1)| = 8$, then $C_D(V_1) \cong D_8$. This means $D \cong D_8 \times D_8$, $|D| = 64$, and $|G| = 128$. By [10, Lemma 2.8] we have $G < D_8 \wr Z_2$, where Z_2. Because $|D_8 \wr Z_2| = 128$ we have that $G = D_8 \wr Z_2$, which is known to be not metabelian [4, Satz 15.3 (d)], that is $G'' \neq 1$. However we have that $G' = D' = (D_8 \times D_8)'$ which is size four. This makes G' abelian and $G'' = 1$, a contradiction.

If $|C_D(V_1)| = 4$ we have that $|D| < |D/C_D(V_1) \times D/C_D(V_1)| = |D|^2/16 = 64$.

That is $|D| = 32$. We also have $D' \leq (D_8 \times D_8)'$ so $|D'| \leq 4$. Suppose $|D'| = 4$ then

$\frac{|D|}{|D'|} = \frac{32}{4} = 8$, so $M_D = 16 = M_1 M_2$ a contradiction. Suppose that $|D'| = 2$. Notice

$C_D(V_1) \cap C_D(V_2) = 1$ so $C_D(V_1) \times C_D(V_2) = 1$ so $C_D(V_1) \times C_D(V_2) = C_D(V_1)C_D(V_2)$.

Let $g \in G - D$ and $(1, a) \in C_D(V_1) \times C_D(V_2)$. Then

$$[(1, a), g] = (1, a)^{-1}g^{-1}(1, a)g = (1, a)^{-1}(1, a)^g = (1, a^{-1})(a^*, 1) = (a^*, a^{-1})$$

for some $a^* \in C_D(V_1)$, and we have four choices for $a \in C_D(V_1)$. Thus $2 = |D'| = |G'| \geq$

4, a contradiction.

If $|C_D(V_1)| = 2$, then $\frac{|D|^2}{4} = 64$ or $|D| = 16$. As before, we know that $|D'| \in$

$\{2, 4\}$. Suppose $|D'| = 4$, then $\frac{|D|}{|D'|} = \frac{16}{4} = 4$, and $M_D = 8$. We know $(v_1, 0)$ and $(v_2, 0)$

are both in D-orbits of size four on V. Let $w \in V_2$ be a regular orbit. Then $(v_1 + w)$

would be in an orbit of size eight, contradicting $M_1 M_2 < M_D$. Suppose that $|D'| = 2$,

then $\frac{|D|}{|D'|} = 8$ and $M_D = 16$. Thus $C_D(V_1)$ must have four orbits of size two on V_2.

Let $w_i \in V_2$ for $i = 1, 2, 3, 4$ be representatives of these four orbits. Then we know

by the table above that $C_D(V_1) = \{1, r\}$, because all other subgroups of D_8 with

size two have only three orbits of size two on V_2. We also know there must exist a

$d_i \in D, i = 1, 2, 3, 4$ where $w_1^{d_1} = w_2, w_2^{d_2} = w_3, w_3^{d_3} = w_4, w_4^{d_4} = w_1$. Without loss let

$w_1 = (1, 0)$ and $w_2 = (1, -1)$. Then there exists a $d \in D$ where $(1, 0)^d = (1, -1)$ in

the action of D on V_2, a contradiction. If $C_D(V_1) = 1$ then $D \cong D_8$, but $D_8/D_8' = 4 =$

M_D, a contradiction.

Suppose that $|D|/|D'| = M_1 M_2 = M_D < M$. We know that $D/C_D(V_1)$ has at

least two orbits of size M_1 in the action of V_1. Recall that v_1 and v_2 are representa-

tives of these orbits.

Let us first assume that $C_D(V_1)$ has exactly one orbit of size M_2 on W_1.

26

By Theorem 1 $C_D(V_1)$ is abelian. Therefore $C_D(V_i)$ is abelian for all $i = 1, \ldots, p$, and it follows that for each i, $C_D(W_i)$ is abelian. We further claim that for each i, $C_D(W_i)$ has exactly one regular orbit of V_i. To see this, observe that $C_D(V_1)$ has exactly one regular orbit on W_1. Hence $C_D(V_1)/(C_D(V_1) \cap C_D(V_2))$ has exactly one regular orbit on V_2, and $(C_D(V_1) \cap C_D(V_2))/(C_D(V_1) \cap C_D(V_2) \cap C_D(V_3))$ has exactly one regular orbit on V_3. We can repeat this until we finally get

$$(\cap_{j=1}^{p-1} C_D(V_j))/(\cap_{j=1}^{p} C_D(V_i)) \cong C_D(W_p)$$

has exactly one regular orbit on V_p. Since the actions of $C_D(W_i)$ on V_i are equivalent for all i, the claim is true. Let $A := \prod_{i=1}^{p} C_D(W_i)$. We see that $A \trianglelefteq G$, and $A = \bigtimes_{i=1}^{p} C_D(W_i)$ is an internal direct product because $C_D(W_i) \cap \prod_{j \in \{1,\ldots,p\}-\{i\}} C_D(W_j)) = 1$, for $i = 1, \ldots, p$ (all elements in $\prod_{j \in \{1,\ldots,p\}-\{i\}} C_D(W_j))$ act trivially on V_i). Applying Lemma 2.2 to the action of $C_D(W_i)$ on V_i for all i. Putting this together thus shows that if we write $V_A = X_1 \oplus \ldots \oplus X_m$ for some $M \in \mathbb{N}$ and irreducible A-modules such that $V_1 = X_1 \oplus \ldots \oplus X_k$ for some $k \in \mathbb{N}$, then $m = kp$ and

$$|A| = \prod_{i=1}^{m}(|X_i| - 1) = (|X_1| - 1)^m \leq M$$

and

$$M_1 \geq \prod_{i=1}^{k}(|X_i| - 1) = (|X_1| - 1)^k.$$

Now recall that $v_1, v_2 \in V_1$ are representatives of two orbits of size M_1 of $D/C_D(V_1)$ on V_1. Write $v_i = x_{i1} + \ldots + x_{ik}$ with $x_{ij} \in X_j$ for $j = 1, \ldots, k$, $i = 1, 2$. We may assume that v_1 is in a regular orbit of $A/C_A(V_1)$, and thus $x_{1j} \neq 0$ for $j = 1, \ldots, k$. But then $v_1^D = v_1^A = \{y_1 + \ldots + y_k | 0 \neq y_i \in X_i \text{ for } i = 1, \ldots, k\}$, and this forces that $x_{2j} = 0$ for at least one $j \in \{1, \ldots, k\}$. If we let $g \in G - D$ and put $z_i = v_i + \sum_{j=1}^{p-1} v_1^{g^j}$ for $i = 1, 2$, then

27

it is clear that both z_1 and z_2 are in different orbits of size greater than or equal to $|A|$ of G. Hence $|G/G'| \geq |A|$.

Now let q be the characteristic of V and write $|X_1| = q^s$. Write $|A/C_A(X_1)| = p^t$. Then $p^t = q^s - 1$ and hence with [10, Proposition 3.1] we know that either $s = 1$, $p = 2$, and q is a Fermat prime; or $t = 1$, $q = 2$, and p is a Mersenne prime; or $s = 2$, $t = 3$, $p = 2$, and $q = 3$. Moreover, by [10, Theorem 2.1] we know that $N_G(X_1)/C_G(X_1)\Gamma(X_1)$ and since G is a p-group, altogether we conclude that

$$N_G(X_1)/C_G(X_1) \cong A/C_A(X_1)$$

unless possibly in the third case, when $|V_1| = 9$ and $N_G(X_1)/C_G(X_1) \cong \Gamma(3^2)$ is possible (in the first case this is clear, in the second it follows by Fermat's Little Theorem). For the moment suppose that $N_G(X_1)/C_G(X_1) \cong A/C_A(X_1)$. Because of the size of A with [10, Lemma 2.8] we conclude that $G \cong A/C_A(X_1) \wr G/A$ where G/A transitively and faithfully permutes the X_i $(i = 1, \ldots, m)$. Now with arguments similar to the one in the proof of [6, Lemma 2] we see that

$$|[A, G]| \geq |A/C_A(X_1)|^{m-1} = (|X_1| - 1)^{m-1}.$$

Moreover, by [2, Theorem 2.3] we have $|G : G'A| = |G/A : (G/A)'| \leq p^{m/p}$. Hence altogether we have

$$
\begin{aligned}
(|X_1| - 1)^m = |A| \leq |G/G'| &= |G : G'A||G'A : G'| \\
&\leq p^{m/p}|A : A \cap G'| \\
&\leq p^{m/p}|A : [A, G]| \\
&= p^{m/p}(|X_1| - 1)
\end{aligned}
$$

Now clearly $|X_1| - 1 \geq p$, and so it follows that

$$p^{m-1} \leq (|X_1| - 1)^{m-1} \leq p^{\frac{m}{p}}.$$

So $m - 1 \leq m/p$, and since $m \geq p$, we get that $p = m = 2$, $|X_1| = 3$, $k = 1$, $V_1 = X_1$, $|V| = 9$, $M = |G/G'| = 4$ and thus G is dihedral of order 8 acting on the nine elements of V. But then D is abelian, and since $G' = D'$, G is also abelian. This is a contradiction.

In the exceptional case $s = 2$, $t = 3$, $p = 2$, $q = 3$ above we have that the kernel K/A of the permutation action of G/A on the X_i is of order at most 2^m. So we see that $G/\Omega_2(A)$ has A as an abelian normal subgroup, and so similarly as above

$$\begin{aligned}
|G/G'| &\leq |G : G'K||G'K : G'| \\
&\leq 2^{\frac{m}{2}} |K : K \cap G'| \\
&\leq 2^{\frac{m}{2}} |K/\Omega_1(A) : (K \cap G')\Omega_1(A)/\Omega_1(A)| \cdot |\Omega_1(A)|
\end{aligned}$$

Now $|[K/\Omega_1(A), G/\Omega_1(A)]| \geq 4^{m-1}$, and thus altogether

$$\begin{aligned}
2^{3m} = 8^m = (|X_1| - 1)^m = |A| \leq |G/G'| &\leq 2^{\frac{m}{2}} |K/\Omega_1(A) : [K/\Omega_1(A), G/\Omega_1(A)]| \cdot 2^m \\
&\leq 2^{\frac{m}{2}} \cdot \frac{8^m}{4^{m-1}} \cdot 2^m \\
&= 2^{\frac{3}{2}m + m - 1} \cdot 8 = 2^{\frac{5}{2}m + 2}
\end{aligned}$$

Hence $3m \leq \frac{5}{2}m + 2$ or, equivalently, $m \leq 4$. Since $m = kp = 2k$, we have that $m = 2$ or $m = 4$.

If $m = 2$, then $k = 1$ and thus $X_i = V_i$ for $i = 1, 2$. But then $M_1 = 8 = |V_1| - 1$, and $D/C_D(V_1)$ has exactly one orbit of size M_1 on V_1, contradicting our observation

29

above that $D/C_D(V_1)$ has at least two orbits of size M_1 on V_1.

If $m = 4$, then $k = 2$ and $|V_1| = 3^4$. Hence G is isomorphic to a subgroup of $\mathrm{GL}(8,3)$ and thus $|G| \leq 2^{19}$. As above, we know that $|G'| \geq |[A,G]| \geq (|X_1| - 1)^{m-1} = 8^3 = 2^9$, and hence $|G/G'| \leq 2^{10} < 2^{12} = |A| \leq M$, contradicting $|G|/|G'| = M$.

Therefore we know that $C_D(V_1)$ has at least two orbits of size M_2 on W_1. Let w_1 and w_2 be representatives of such orbits. If there exists a $d \in C_D(v_1)$ such that $w_1^d = w_2$ we see that

$$M \geq M_D \geq M_1 p M_2 \geq p|D : D'| = |G/G']$$

contradicting that $M_D < M$. Therefore, no such d exists. This tells us that $(v_1 + w_1)$ and $(v_1 + w_2)$ lie in different D-orbits on V. Similarly $v_2 + w_1$ and $v_2 + w_1$ are in different D-orbits on V.

Now identify D with a subgroup of $\bigtimes_{i=1}^{p} D/C_D(V_i)$. Also let $g \in G - D$ and put

$$L_i = \sum_{j=0}^{p-1} (v_i^{g^j})^D := \{\sum_{j=0}^{p-1} x_j | x_j \in (v_i^{g^j})^p \text{ for } j = 0, \dots, p-1\} \subset V$$

for $i = 1, 2$. The L_i are clearly G-invariant subsets, and $L_1 \cap L_2 = \emptyset$. For any $x \in V_2 \oplus \dots \oplus V_p$ it follows that if the orbit $(v_i + x)^D \subset L_i$ $(i \in \{1, 2\})$.

We now have several cases to consider. The D-orbits $(v_1 + w_1)^D$ and $(v_1 + w_2)^D$ are both G–invariant. The D-orbits $(v_2 + w_1)^D$ and $(v_2 + w_2)^D$ are both G-invariant. Lastly, one of the D-orbits $(v_1 + w_1)^D$ or $(v_1 + w_2)^D$ is not G-invariant, and at least one of the orbits D-orbits $(v_2 + w_1)^D$ or $(v_2 + w_2)^D$ is not G-invariant.

Suppose that the D-orbits $(v_1 + w_1)^D$ and $(v_1 + w_2)^D$ are both G-invariant. Then $v_1 + w_1 \in L_1$ and $v_1 + w_2 \in L_1$, and thus $v_2 + w_1 \notin L_2$ and $v_2 + w_2 \notin L_2$, that is

$(v_2 + w_1)^D$ and $(v_2 + w_2)^D$ are not G-invariant, so that

$$M \geq |(v_2 + w_i)^G| \geq p|(v_2 + w_i)| \geq pM_1 M_2 \geq p|D/D'| = |G/G'|$$

for $i = 1, 2$. This tells us that $C_D(V_1)$ has exactly two orbits of size M_2 in the action on W_1.

Suppose that we have three orbits of size $D/C_D(V_1)$ on V_1, let v_3 be a representative of this orbit. We know that $(v_3 + w_1)^D$ and $(v_3 + w_2)^D$ are not G–invariant. That means $(v_2 + w_1)^D = (v_3 + w_2)^D$, so there exists a $g \in G - D$ with $(v_1 + w_2)^g = v_2^g + w_2^g = v_3 + w_1$ and $w_1 = v_2^g + x$ for some $x \in W_2$. Therefore $w_1 \in L_1$ so $v_2^g \in (v_1^{g^j})^D$ for some j. We can choose g so that $j = 1$ giving us that $v_2^g \in (v_1^g)^D$ but $(v_1^g)^D \cap (v_2^g)^D = \varnothing$, a contradiction.

Therefore we have that $D/C_D(V_1)$ has exactly two orbits of size M_1 in the action of V_1. By induction $D/C_D(V_1) \cong D_8$, $p = 2$, and $V_1 = V(2,3)$. We know that $C_D(V_1) \times C_D(V_2) \leq D \leq D/C_D(V_1) \times D/C_D(V_2) \cong D_8 \times D_8$ and $C_D(V_1) \leq D/C_D(V_1) \cong D_8$. Then $|C_D(V_1)| \in \{2, 4, 8\}$. If $|C_D(V_1)| = 8$ then $D = D_8 \times D_8$, so $|D| = 64$, $|D'| = 4 = |G'|$ and $|G| = 128$. By [10, Lemma 2.8] we have $G \leq D_8 \wr Z_2$ is metabelian, but $|G'| = 4$ a contradiction.

If $|C_D(V_1)| = 4$, then $C_D(V_1) \cong Z_4$ (because $C_D(V_1)$ has two orbits of size M_2 on V_2, therefore it is not the Klein-4). Thus $Z_4 \times Z_4 \leq D \leq D_8 \times D_8$, $|D| > 16$, and $Z_4 \times Z_4 < D$ so $|D| = 32$ and $|D'| = 2$. Because $D' < (D_8 \times D_8)'$ we have that $|D'| \in \{2, 4\}$. If $|D'| = 4$ then $\frac{|D|}{|D'|} = \frac{32}{4} = 8$, contradicting that $Z_4 \times Z_4$ has a regular orbit (size 16) on V. Therefore $|D'| = |G'| = 2$, but $C_D(V_1) = 4$ which we have shown makes $|G'| \geq 4$, a contradiction.

If $|C_D(V_1)| = 2$, then $C_D(V_1) \cong Z_2$. This means that $C_D(V_1)$ has at least three orbits of size M_2 on V_2, a contradiction.

The case where $(v_2 + w_1)^D$ and $(v_2 + w_2)^D$ are both G-invariant will follow the same proof as in case 1 if we replace v_1 with v_2.

Suppose that at least one of the orbits $(v_1 + w_1)^D$ or $(v_1 + w_2)^D$ is not G-invariant and at least one of the orbits $(v_2 + w_1)^D$ and $(v_2 + w_2)^D$ is not G-invariant. Without loss we may assume that $(v_1 + w_1)^D$ is not G-invariant. If $(v_2 + w_1)^D$ is also not G-invariant, we see that $(v_1 + w_1)^G$ and $(v_2 + w_1)^G$ are two distinct orbits of size M, because

$$M \geq (v_i + w_1)^G \geq pM_1 M_2 = |G/G'|$$

for $i = 1, 2$ and if we write $w_1 = (x_2, \ldots, x_p) \in V_2 \oplus \ldots \oplus V_p$ then $v_1 + w_1 = (v_1, x_2, \ldots, v_p)$ and $v_2 + w_2 = (v_2, x_2, \ldots, x_p)$ have a different number of components in the corresponding component of L_1 and cannot be conjugate in G.

By induction we have that $D/C_D(V_1) \cong D_8$, $V_1 = V(2,3)$, $p = 2$, and $V = V_1 \times V_2$. As shown above, this leads to a contradiction.

Hence $(v_2 + w_1)^D$ is G-invariant and thus $(v_2 + w_2)^D$ is not G-invariant. A similar argument then shows that $(v_1 + w_2)^D$ must be G-invariant otherwise $(v_1 + w_2)^G$ and $(v_2 + w_2)^G$ would be in two different orbits of size M, and we could use induction as above to show $D/C_D(V_1) \cong D_8$, a contradiction.

Thus $(v_1 + w_1)^D$ and $(v_2 + w_2)^D$ are both G-invariant. If $(v_1 + w_2)^D$ and $(v_2 + w_2)^D$ are G-conjugate then $v_2 + w_1 \in L_2$ and $v_1 + w_2 \in L_1$. This shows that $v_1 + w_1$ and $v_2 + w_2$ can only be conjugate in G if $p = 2$, so now let $p = 2$.

Suppose there are three orbits of size M_2 in the action $C_D(V_1)$ on V_2. Let $w_3 \in W_1 = V_2$ be a representative of such an orbit. As above it follows that $v_1 + w_1, v_1 + w_2$ and $v_1 + w_3$ all lie in different D-orbits on V and so do $v_2 + w_1, v_2 + w_2$, and $v_2 + w_3$, and as above, with w_3 in place of w_2 we see the following version of case 3 must be true.

At least one of the orbits $(v_1 + w_1)^D$ or $(v_1 + w_3)^D$ is not G-invariant, and at least one of the orbits $(v_2 + w_1)^D$ or $(v_2 + w_3)^D$ is not G-invariant. We already know that $(v_2 + w_1)^D$ is G-invariant, it follows that $(v_2 + w_3)^D$ is not G-invariant. The argument from an earlier shows $(v_2 + w_2)^G$ and $(v_2 + w_3)^G$ are different G-orbits. Assume that there is third orbit of size M_1 in the action of $D/C_D(V_1)$ on V_1, let v_3 be a representative of this orbit. Then at least two or the three orbits $(v_3 + w_1)^D, (v_3 + w_2)^D$, and $(v_3 + w_3)^D$ are not G-invariant. If $(v_3 + w_1)^D$ is G-invariant, then $(v_3 + w_2)^G, (v_3 + w_1)^G$, and $(v_2 + w_2)^G$ are three G-orbits of size M, a contradiction. If $(v_3 + w_2)^D$ is G-invariant, then $(v_2 + w_3)^G, (v_2 + w_2)^G$, and $(v_3, w_3)^G$ are three G-orbits of size M, a contradiction. Lastly, if $(v_3 + w_3)^D$ is G-invariant, the $(v_3 + w_1)^G, (v_2 + w_2)^G$, and $(v_3 + w_2)^G$ are three G-orbits of size M, a contradiction. We see that $D/C_D(V_1)$ has exactly two orbits of size M_1 on V_1. By induction we have that $D/C_D(V_1) \cong D_8$, a contradiction. This concludes equality in (6) and (7).

Suppose we have equality in (7) and strict inequality in (6). That is

$$M \geq M_1 M_2 \geq p|D : D'C_D(V_1)||C_D(V_1) : C_D(V_1)'| \geq p|D/D'| = |G : G'|.$$

Because $|G : G'| = M$ we have equality everywhere, and $M = M_1 M_2, M_1 > |D : D'C_D(V_1)|, M_2 = |C_D(V_1) : C_D(V_1)'|$. Again let M_D denote the largest orbit size of D on V, then $M_D \geq M_1 M_2$ so $M_D = M$. By Theorem 1 $C_D(V_1)$ is abelian or has at least two orbits of size M_2 of D on W_1.

Suppose $C_D(V_1)$ has at least two orbits of size M_2 on W_1, and let $w_1, w_2 \in W_1$ be representatives of these orbits. Let $D/C_D(V_1)$ have at least two orbits of size M_1 on V_1. Because $M = M_1 M_2$ we have that $(v_1 + w_1)^D, (v_1 + w_2)^D$, and $(v_2 + w_2)^D$ and $(v_2 + w_1)^D$ are all (not necessarily distinct) orbits of size $M_D = M$. This means that $(v_1 + w_1)^D$ is G-invariant, meaning that $(v_2 + w_1)^D$ is not G-invariant. That is

$|(v_2 + w_1)^G| > M_1 M_2 = M$, a contradiction.

Therefore we have that $D/C_D(V_1)$ has exactly one orbit of size M_1 on V_1. If $(v_1 + w)$ is not G–invariant then $|(v_1 + w)^G| = M$, but D has two orbit of size M on V, different from $(v_1 + w)^D$ giving G three G-orbits of size M on V, a contradiction. Therefore $(v_1 + w)^D$ is G-invariant. If $C_D(V_1)$ has two orbits of size M_2 on W_1, then $(v + w_1)^D$ and $(v + w_2)^D$ are two D–orbits of size M. Thus $C_D(V_1)$ has exactly two orbits of size M_2 on W_1. If $M_2 > M_1$, then $C_D(V_1) < D$ would give us an orbit of size M_2 on V_1 contradicting that M_1 was the size of the largest orbit of D on V_1. If $M_2 = M_1$ then $C_D(V_1)$ would have two orbits of size M_1 on V_1 contradicting that D has exactly one orbit of size M_1 on V_1. If $p = 2$ then $M_1 > M_2$. Let $g \in G - D$ which permutes the elements of the components $V_1 \to V_2 \to \ldots \to V_p \to V_1$. Let $v^g = x \in V_2$ and $w_1^g = y \in W_2$. We claim that $(x + y) \notin (v + w_1)^D$. Suppose not, then $(x + y)^D = (v + w_1)^D$. The V_2 component of the left hand side has M_1 choices for this element. However, the right hand side has M_2 choices for elements in V_2 Therefore $(x + y)^D$ is a third orbit of size M in the action of D on V, a contradiction. This means $p \ne 2$.

Using [10][Theorem 4.4] we know that p would have to be a Mersenne prime, contradicting the original hypothesis that $|G|$ is not divisible by a Mersenne prime.

Suppose that $C_D(V_1)$ has exactly one orbit of size M_2 on W_1, then $C_D(V_1)$ is abelian by Theorem 1. As argued above and using Lemma 1 we conclude that there is an irreducible normal subgroup of G such that if we write $V_A = X_1 \oplus \ldots \oplus X_m$ for some $m \in \mathbb{N}$ and irreducible A-modules X_i, then $|A| = (|X_i| - 1)^m \le M$. Without loss we may assume that $V_1 = X_1 \oplus \ldots \oplus X_k$ for some $k \in \mathbb{N}$ (which divides m), and then $M_1 \ge (|X_1| - 1)^k = |A/C_A(V_1)|$. Now $C_A(V_1) \cong A/C_A(W_1)$ is isomorphic to a maximal abelian subgroup of $D/C_D(V_1)$. If there was a larger abelian subgroup, call in V, this subgroup would still act on each $X_j, (j = k + 1, \ldots, m)$ where for

$Y_i = \bigtimes_{\ell \in \{1,\dots,m\}-\{i\}} X_\ell$ we put

$$C_j = X_{i\in\{1,\dots,m\}-\{j\}} C_A(Y_i) \le A = \bigtimes_{i=1}^{m} C_A(Y_i).$$

Hence there would exist a $j \in \{k+1,\dots,m\}$ such that $|BC_B(X_j)| > |A/C_A(X_j)| = |X_j|-1$, a contradiction. Hence $C_A(V_1) \cong A/C_A(W_1)$ is self centralizing in $D/C_D(W_1)$. But as $D/C_D(V_1)$ is nonabelian, clearly $D/C_D(W_1)$ is nonabelian, and thus there exists a $d \in D$ and $a \in C_D(V_1)$ such that $1 \ne [d,a]$. Hence $D' \cap C_A(V_1) > 1$. On the other hand, we have, as $C_D(V_1)' = 1$ and $G' = D'$, that

$$M = pM_1|C_D(V_1)| = |G/G'| = p|D/D'|$$

$$= p|D : D'C_D(V_1)||D'C_D(V_1) : D'|$$

$$= pM_1|D'C_D(V_1) : D'|$$

$$= p|M_1 C_D(V_1) : (D' \cap C_D(V_1))|.$$

This forces $D' \cap C_D(V_1) = 1$, and we have a contradiction. This concludes our proof.

□

IV.   The Open Case

In this section we will reiterate the conditions under which we use the Mersenne prime condition. Let the action of G on V be imprimitive where $D' = G'$. Let M_1 be the size of the largest orbit of $D/C_D(V_1)$ on V_1 and M_2 be the largest orbit size of $C_D(V_1)$ on M_2. If $|D : D'C_D(V_1)| < M_1$, $|C_D(V_1) : C_D(V_1)'| = M_2$ and $M_1 M_2 = M_D = M = p|D|/|D'| = |G|/|G'|$, $D/C_D(V_1)$ has exactly one orbit of size M_1 on V_1 and $C_D(V_1)$ has exactly two orbits of size M_2 on W_1 then we know that p is a Mersenne and $q = 2$. However we are almost certain this case cannot happen.

REFERENCES

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

[2] M. Aschbacher and R. M. Guralnick, *On abelian quotients of primitive groups*, Proc. Amer. Math. Soc. (1989), 89–95.

[3] D. S. Dummit and R. M. Foote, *Abstract algebra*, Wiley, Hoboken, New Jersey, 2004.

[4] B. Huppert, *Endliche gruppen i*, Springer-Verlag, Berline, Hiddleberg, New York, 1967.

[5] I. M. Isaacs, *Commutators and the commutator subgroup*, Amer. Math. Monthly **84** (1977), 720 – 722.

[6] I. M. Isaacs, *Algebra: A graduate course*, American Mathematical Society, Providence, RI, 2009.

[7] I.M. Isaacs, G. Navarro, and J. Sangroniz, *p-groups having few almost-rational irreducible characters*, Israel J. of Math. **189** (2012), 65–96.

[8] T. M. Keller and Y. Yang, *Abelian quotients and orbit sizes of solvable linear groups*, Israel J. of Math. **2011** (2016), 23–44.

[9] M. W. Liebeck and A. Shalev, *Bases of primitive linear groups*, J. of Algebra **252** (2002), 95–113.

[10] O. Manz and T. R. Wolf, *Representations of solvable groups*, London Mathematical Society Lecture Notes Series, vol. 185, Cambridge University Press, Cambridge, MA, 1993.

[11] G. R. Robinson and J. G. Thompson, *On Brauer's k(b)-problem*, J. Algebra **184** (1996), 95–113.