

GROUPS WITH A CHARACTER OF LARGE DEGREE

NOAH SNYDER

(Communicated by Jonathan I. Hall)

ABSTRACT. Let G be a finite group of order n and V a simple $\mathbb{C}[G]$ -module of dimension d . For some nonnegative number e , we have $n = d(d + e)$. If e is small, then the character of V has unusually large degree. We fix e and attempt to classify such groups. For $e \leq 3$ we give a complete classification. For any other fixed e we show that there are only finitely many examples.

1. INTRODUCTION

Throughout this paper we consider a finite group G of order n and a simple $\mathbb{C}[G]$ -module V with dimension d and character χ . It is well known that $d^2 \leq n$ and that $d \mid n$. Thus, there must exist a nonnegative integer e such that $d(d + e) = n$. Our approach is to fix e and consider all groups and simple modules such that $d(d + e) = n$. If e is small relative to d , then χ has large degree.

Our main result is

Theorem 1.1. *Let G be a finite group of order n with a simple $\mathbb{C}[G]$ -module V of dimension d and $d(d + e) = n$.*

- (1) *If $e = 0$, then G is trivial.*
- (2) *If $e = 1$, then G is a doubly transitive Frobenius group or a cyclic group with two elements.*
- (3) *If $e > 1$, then $n \leq ((2e)!)^2$.*

After finishing this manuscript, I discovered that for $e = 1$ and $e = 2$ this result appears in [Ber]; however, that argument does not generalize to larger e .

The $e = 0$ case is trivial. The first interesting case is $e = 1$, which we treat in section 2. In Proposition 2.1 we prove part (2) of Theorem 1.1. Doubly transitive Frobenius groups were classified by Zassenhaus [Z], so Theorem 1.1 gives a satisfactory classification.

In section 3 we show that unless d and e satisfy a certain divisibility condition, there exists a normal subgroup $N \neq \{1\}$ such that N acts trivially on each simple $\mathbb{C}[G]$ -module other than V . In section 3 we consider the former case and prove Theorem 1.1 in this case.

In section 4 we turn to the case where such a normal subgroup exists. This was studied by Gagola in [G], independently by Burtsev in [Bu], and later by Kuisch

Received by the editors May 31, 2006.

2000 *Mathematics Subject Classification.* Primary 20C15.

This material is based upon work supported under a National Science Foundation Research Fellowship.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

and van der Waall in [K-vdW1], [K], and [K-vdW2]. (For a summary of Burtsev's results in English translation see [Bel].) We adapt and strengthen a few of their results in Theorem 4.1 to give a purely group theoretic necessary and sufficient condition. No sufficient condition appeared in the earlier papers.

In section 5 we use the structure of a certain p -group to prove Theorem 1.1 for any fixed $e > 1$. First we prove a weaker version of part (3) of Theorem 1.1 with $n \leq e^{2e^2}$, and then we strengthen that result to $n \leq ((2e)!)^2$. Finally, in section 6, we give an explicit list of all groups of order n with a character of degree d such that $d(d+2) = n$ or $d(d+3) = n$.

I would like to thank Hendrik Lenstra for many long and fruitful conversations without which this paper would not exist and for his patient comments on drafts of this paper. I would also like to thank Rob van der Waall and Yakov Berkovich for sharing their knowledge of the relevant literature and Jack Schmidt whose GAP calculations first showed that the $e = 3$ case was tractable.

2. A PRELIMINARY RESULT

The first case to consider is $e = 0$. Since the sum of the squares of the dimensions of the simple modules equals the order of the group, $d^2 = n$ implies that there is only one simple module. This occurs exactly when G is trivial.

The next case is $e = 1$. This is a particularly nice case since a complete classification is possible. It is also extraordinary since it is the only e for which there are infinitely many groups. The results of this section can be derived from the more general results later, but it is helpful to see the outline in this simpler situation first. (See [Ber] for another proof which is elegant, but hard to generalize.)

Proposition 2.1. *Let G be a finite group of order n . The following two conditions are equivalent:*

- (1) *There exists a simple $\mathbb{C}[G]$ -module V of dimension d with $d(d+1) = n$.*
- (2) *G is a semidirect product of a normal subgroup N of order $d+1$ and a group H of order d which acts freely and transitively by conjugation on the set $N - \{1\}$. Also, unless $d = 1$, we have that $V \cong \text{Ind}_N^G V'$ where V' is any nontrivial 1-dimensional $\mathbb{C}[N]$ -module.*

The groups described in (2), except when $d = 1$, are called doubly transitive Frobenius groups. They were classified by Zassenhaus in [Z].

The proof of Proposition 2.1 requires two well-known lemmas. The first follows immediately from the fact that the number of irreducible representations of a group is the same as the number of conjugacy classes. The second is [R, 7.2.8i, p. 193].

Lemma 2.2. *A nontrivial normal subgroup N of a finite group G acts trivially on each of the nontrivial simple $\mathbb{C}[G]$ -modules except for one, if and only if the conjugacy classes of G are $\{1\}$, the set $N - \{1\}$, and the preimages of the nontrivial conjugacy classes of G/N .*

Lemma 2.3. *If N is a normal subgroup of a finite group G such that all nontrivial elements of N are conjugate in G , then N is elementary abelian.*

Proof of Proposition 2.1. First we show that (2) implies (1). Let χ be the character of $V = \text{Ind}_N^G V'$. Using the explicit formula for the induced character, we can

compute:

g	$\chi(g)$
1	d
$\in N - \{1\}$	-1
$\notin N$	0

Therefore, we see that $(\chi, \chi) = (d^2 + d)/n = 1$. Thus, we have that V is a simple $\mathbb{C}[G]$ -module. Notice that $\chi(1)(\chi(1) + 1) = d(d + 1) = \#G$. Thus, we see that (2) implies (1).

Now we show that (1) implies (2). Let χ be the character of V . If $d = 1$, then $n = 2$ and G is the cyclic group with two elements. If $d > 1$, note that $d^2 + d^2 > d^2 + d = n$. Therefore, G has at most one irreducible character of degree d . Thus, all the Galois conjugates of χ are equal to χ . Hence, χ is \mathbb{Z} -valued.

By character orthogonality, we see that

$$\sum_{g \in G} \chi(g)^2 = n(\chi, \chi) = n = d^2 + d$$

and

$$\sum_{g \in G} \chi(g) = n(\chi, 1) = 0.$$

Therefore, we have that $\sum_{g \neq 1} \chi(g)^2 = d$ and $\sum_{g \neq 1} \chi(g) = -d$. Adding yields

$$\sum_{g \neq 1} \chi(g)(\chi(g) + 1) = 0.$$

Since all $\chi(g) \in \mathbb{Z}$, this implies that $\chi(g)$ is 0 or -1 for any $g \neq 1$.

Let $S = \{g \in G : \chi(g) = -1\}$ and $T = \{g \in G : \chi(g) = 0\}$. Now $\sum_{g \neq 1} \chi(g) = -d$ implies that $\#S = d$ and $\#T = d^2 - 1$.

Let W be the kernel of the canonical projection $\mathbb{C}[G] \rightarrow \text{End}_{\mathbb{C}} V$. Let ψ be the character of W . Notice that $\psi = \rho_G - \chi(1)\chi$, where ρ_G is the character of the regular representation. Thus we can read off the following.

g	$\psi(g)$
1	d
$\in S$	d
$\in T$	0

Those g for which $\psi(g) = \psi(1)$ are precisely those g which act trivially on W . Thus, the map $G \rightarrow \text{Aut}(W)$ has kernel $N := S \cup \{1\}$. Further notice that $\#N = d + 1$.

Since every simple $\mathbb{C}[G]$ -module other than V is a quotient of W , the subgroup N acts trivially on each of the simple $\mathbb{C}[G]$ -modules except for one. Such simple modules shall be the main focus of the sequel.

Since the index of N is relatively prime to its order, the Schur-Zassenhaus theorem (cf. [R, p. 246]) implies that N has a complement H . Since

$$d(d + 1) = \#G = \#N\#H = (d + 1)\#H,$$

we conclude $\#H = d$. Since there are only d nontrivial elements of N and they are all in the same H -orbit under conjugation, H acts freely and transitively on $N - \{1\}$.

By Lemma 2.2 all the nonidentity elements of N are conjugate in G . So, by Lemma 2.3, we see that N is abelian. Take V' to be any 1-dimensional $\mathbb{C}[N]$ -module. By the other direction of the theorem, $\text{Ind}_N^G V'$ is a simple $\mathbb{C}[G]$ -module of dimension d , and thus the unique one V . \square

Thus, the existence of a group G of order n with a simple $\mathbb{C}[G]$ -module V of dimension d implies that n is of the form $p^k(p^k - 1)$ and $d = p^k - 1$. Conversely, if $n = p^k(p^k - 1)$, there is at least one example: $G = \mathbb{F}_q \rtimes \mathbb{F}_q^*$ and $V = \text{Ind}_{\mathbb{F}_q}^G V'$ for V' any nontrivial 1-dimensional module over the group ring of the additive group of \mathbb{F}_q .

3. REDUCTION TO THE TWO MAIN CASES

In the proof of Proposition 2.1 we found a subgroup N which acts trivially on each simple $\mathbb{C}[G]$ -module other than V . This will be our approach to the general case as well.

Theorem 3.1. *Let G be a finite group of order n and V a simple $\mathbb{C}[G]$ -module of dimension d with character χ and $d(d + e) = n$. Then at least one of the following is true:*

- (1) $d = e$,
- (2) $d + e \mid (2e - 1)!/e$, or
- (3) *there exists some normal subgroup $N \neq \{1\}$ which acts trivially on all simple $\mathbb{C}[G]$ -modules other than V .*

Proof. If $d < e$, then $d + e \mid (2e - 1)!/e$ which is (2). If $d = e$ we are obviously in case (1). So we assume that $d > e$. Hence, we see that $d^2 + d^2 > d(d + e)$. So there can be only one irreducible representation of degree d . Thus, its character is \mathbb{Z} -valued.

Let W be the kernel of the canonical projection $\mathbb{C}[G] \rightarrow \text{End}_{\mathbb{C}} V$. Let ψ be the character of W . Let N be the kernel of the map $G \rightarrow \text{Aut}(W)$. Since every simple $\mathbb{C}[G]$ -module other than V is a quotient of W , we see that every element of N acts trivially on each simple $\mathbb{C}[G]$ -module except V . So unless $N = 1$ we have shown (3).

So assume that $G \rightarrow \text{Aut}(W)$ is an injection. Notice that $\psi(1) = ed$. For $g \neq 1$, we have that $\psi(g) = -d\chi(g)$. But, $\psi(g)$ is bounded in absolute value by $\psi(1) = ed$. Hence, we see $-e \leq \chi(g) \leq e$. For all $g \neq 1$ we have $\psi(g) \neq \psi(1) = de$; hence, $\chi(g) \neq -e$. Furthermore, since the trivial $\mathbb{C}[G]$ -module is a submodule of W , for any $g \neq 1$, we have that $\psi(g) \neq -de$. Thus, we also see that $\chi(g) \neq -e$.

Since the product of the characters of two representations is the character of the tensor product, we see that virtual characters form a ring. By the previous paragraph, the virtual character $\prod_{-e < i < e} (\chi - i)$ vanishes on any $g \neq 1$. Thus, its inner product with the trivial character is

$$\frac{1}{d(d + e)} \prod_{1 - e \leq i \leq e} (d - i).$$

Canceling the d and using that $d - i \equiv -e - i \pmod{d + e}$, we see that $d + e \mid (2e - 1)!/e$. \square

We will call the three cases in Theorem 3.1 the $d = e$ case, the *factorial case*, and the *normal subgroup case*, respectively. Theorem 1.1 is trivial in the $d = e$ case, and follows easily in the factorial case.

Proposition 3.2. *If e, d and n are integers greater than 1 such that $n = d(d + e)$ and $d = e$ or $d + e \mid (2e - 1)!/e$, then $n \leq ((2e)!)^2 \leq e^{4e^2}$.*

Proof. We see immediately that $d \leq d + e \leq (2e)!$. For $e > 1$, we see that $(2e)! \leq (2e)^{2e} \leq (e^2)^{e^2}$. Thus, $n = d(d + e) \leq ((2e)!)^2 \leq e^{4e^2}$. \square

For any e there is an example of the factorial case occurring. Take G a cyclic group of order $e + 1$ and V the trivial $\mathbb{C}[G]$ -module. However, I was unable to find any examples suggesting that the factorial bound is at all tight.

4. THE NORMAL SUBGROUP CASE

In this section we study the structure of a group G with a nontrivial normal subgroup N and a simple $\mathbb{C}[G]$ -module V such that N acts trivially on each simple $\mathbb{C}[G]$ -module other than V .

This situation is the main study of [G]. Gagola showed that the character of V vanishes on all but one nontrivial conjugacy class if and only if there exists a subgroup N of G such that N acts trivially on each simple $\mathbb{C}[G]$ -module except V .

Theorem 4.1. *Let G be a group of order n and V a simple $\mathbb{C}[G]$ -module of dimension d . Define e such that $n = d(d + e)$. Assume that there exists a normal subgroup $N \neq \{1\}$ such that N acts trivially on each simple $\mathbb{C}[G]$ -module other than V . Let x be a nontrivial element of N and C be the centralizer of x in G . Then there exist a prime number p , a positive integer k and a nonnegative integer m such that*

- (1) N is elementary abelian of order p^k ,
- (2) C has order $p^k e^2$, and $d = e(p^k - 1)$, and $n = e^2 p^k (p^k - 1)$,
- (3) C is a Sylow p -subgroup of G and $e = p^m$,
- (4) if H is any group such that $N \subseteq H \subseteq C$ and $\#H > p^{k+m}$, then $N \subseteq [H, H]$.

Parts (1)–(3) and a weaker version of (4) are proved in [G, Corollary 2.3] and [K-vdW1, Corollary 1.4] using Clifford’s theorem. We give a new proof using different techniques which can be adapted to prove the converse.

Proof. By Lemma 2.2 and Lemma 2.3, we conclude that N is elementary abelian. Thus, for some p and k , we see $\#N = p^k$. This is (1).

Since all but one of the simple $\mathbb{C}[G]$ -modules are a pull-back of a simple $\mathbb{C}[G/N]$ -module, we have

$$\mathbb{C}[G] \cong \mathbb{C}[G/N] \oplus \text{End}_{\mathbb{C}} V.$$

Therefore, we see that $d(d + e) = [G : N] + d^2$. It follows that $[G : N] = de$. We also have that

$$p^k = \#N = \frac{\#G}{[G : N]} = \frac{d}{e} + 1.$$

Therefore, we see that $d = e(p^k - 1)$. Hence, we see that

$$n = [G : N]p^k = dep^k = e^2 p^k (p^k - 1).$$

Because the conjugacy class of x can be identified with G/C , we see that

$$[G : C] = \#N - 1 = \frac{d}{e}.$$

Finally, this implies that

$$[C : N] = \frac{[G : N]}{[G : C]} = e^2.$$

This completes the proof of (2).

The isomorphism $\mathbb{C}[G] \cong \mathbb{C}[G/N] \oplus \text{End}_{\mathbb{C}} V$ implies that $\rho_G = \rho_{G/N} + d\chi$ (where ρ denotes the regular character). This equation lets us read off the values of the character of V , which we denote by χ :

g	$\chi(g)$
1	d
$\in N - \{1\}$	$-e$
$\notin N$	0

Consider any subgroup H of G and φ any degree 1 character of H which is nontrivial when restricted to $H \cap N$. We have that

$$\begin{aligned} (\chi, \varphi)_H &= \frac{1}{\#H} \left(d + e - e \sum_{g \in H \cap N} \varphi(g) \right) \\ &= \frac{1}{\#H} (d + e - e\#(H \cap N)(\varphi, 1)_{H \cap N}) = \frac{d + e}{\#H}. \end{aligned}$$

So we see that

$$(*) \quad \frac{ep^k}{\#H} = (\chi, \varphi)_H \in \mathbb{Z}.$$

We will apply (*) to several different subgroups in order to prove parts (3) and (4) of Theorem 4.1. Choose q a prime different from p . Let Q be a q -Sylow subgroup of C . Let $H_q = Q \times \langle x \rangle$. Let φ be a degree 1 character of H which is trivial on Q and nontrivial on $\langle x \rangle$. Then (*) tells us that

$$\frac{ep^k}{\#H_q} \in \mathbb{Z}.$$

But the q part of $\#H_q$ is the q part of e^2 . So $\#H_q$ must be relatively prime to q . Since this is true for all $q \neq p$, we see that C is a p -group, and hence that $e = p^m$. This is (3).

Finally we apply (*) to a group H such that $N \subseteq H \subseteq C$ and $\#H > p^{k+m}$ and any degree 1 character φ of H . Since

$$\frac{p^{k+m}}{\#H} \notin \mathbb{Z},$$

(*) implies that φ must be trivial when restricted to N . Thus, $N \subseteq [H, H]$. This is part (4). □

Corollary 4.2. *Let e be a positive integer which is not a power of a prime. Let G be a finite group of order n and V a simple $\mathbb{C}[G]$ -module of V of dimension d . Suppose that $d(d + e) = n$, then $n \leq ((2e)!)^2 \leq e^{4e^2}$.*

Proof. By Theorem 4.1, the group G does not have a normal subgroup $N \neq \{1\}$ which acts trivially on each simple $\mathbb{C}[G]$ -module except for one. Therefore, by Theorem 3.1, we know that $d + e \mid (2e)!$. Thus, by Proposition 3.2, we conclude that $n \leq ((2e)!)^2 \leq e^{4e^2}$. □

Conditions (1)–(4) of Theorem 4.1 are also sufficient. (The reader interested only in the proof of Theorem 1.1 is encouraged to skip to section 5.)

Theorem 4.3. *Let G be a finite group of order $n = p^{k+2m}(p^k - 1)$ with $m \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}_{>0}$. Let N be an elementary abelian normal subgroup of G of order p^k . Let $d = (p^k - 1)p^m$. Let x be a nontrivial element of N and let C be the centralizer of x in G . Suppose that C is a Sylow p -subgroup of G of order p^{k+2m} . Suppose that if H is any group such that $N \subseteq H \subseteq C$ and $\#H > p^{k+m}$, then $N \subseteq [H, H]$.*

Then there exists a simple $\mathbb{C}[G]$ -module V such that $\mathbb{C}[G] \cong \mathbb{C}[G/N] \oplus \text{End}_{\mathbb{C}} V$. Furthermore, $\dim V = d$.

The crucial step in the proof of Theorem 4.1 was that for any virtual character χ of G and for any subgroup H of G and any character φ of H we know that $(\chi, \varphi) \in \mathbb{Z}$. Brauer’s theorem gives a converse to this fact.

Proposition 4.4 (cf. [Se, p. 82]). *Let χ be a class function on G . χ is a virtual character if and only if, for every elementary subgroup H and for every 1-dimensional character φ of H , we have $(\chi, \varphi)_H \in \mathbb{Z}$.*

In order to prove Theorem 4.3, we will build a class function χ and use Proposition 4.4 to show that χ is a character of a simple $\mathbb{C}[G]$ -module V satisfying the required properties.

Proof of Theorem 4.3. Let χ be the class function such that $d\chi$ is the character of the virtual $\mathbb{C}[G]$ -module $\mathbb{C}[G] - \mathbb{C}[G/N]$. We can read off the values of χ :

g	$\chi(g)$
1	d
$\in N - \{1\}$	$-p^m$
$\notin N$	0

If H is an elementary subgroup of G and φ is a degree 1 character of H , then we define

$$\begin{aligned}
 f(H, \varphi) &:= (\chi, \varphi)_H = \frac{1}{\#H} \left(p^m(p^k - 1) - p^m \sum_{g \in H \cap N - \{1\}} \varphi(g) \right) \\
 &= \frac{p^m}{\#H} (p^k - \#(H \cap N)(\varphi, 1)_{H \cap N}).
 \end{aligned}$$

Since C is the centralizer of x in G , the conjugacy class of x has $(G : C) = p^k - 1 = \#N - 1$ elements. So all nontrivial elements of N are conjugate. Thus, any other nontrivial element $y \in N$ has a Sylow p -group of G as its centralizer. Thus, no nontrivial element of N commutes with any element of order prime to p . In particular, if H is an elementary group, then H is a p -group or H intersects N trivially or both.

Suppose that H is a p -group. Since $f(H, \varphi)$ does not change under conjugation, we can assume that $H \subseteq C$. Let $H' = H \cdot N$. Since $N \subseteq H' \subseteq C$, we know that one of $\#H' \mid p^{m+k}$ and $N \subseteq [H', H']$ holds. On the one hand, if $\#H' \mid p^{m+k}$, then

we also have that $\#H \mid p^{m+k}$. Thus, we see that

$$\begin{aligned} f(H, \varphi) &= \frac{p^{m+k}}{\#H} - \frac{p^m \#(H \cap N)}{\#H} (\varphi, 1)_{H \cap N} \\ &= \frac{p^{m+k}}{\#H} - \frac{p^m \#N}{\#H'} (\varphi, 1)_{H \cap N} \\ &= \frac{p^{m+k}}{\#H} - \frac{p^{m+k}}{\#H'} (\varphi, 1)_{H \cap N} \in \mathbb{Z}. \end{aligned}$$

On the other hand, suppose that $N \subseteq [H', H']$. Thus, we see that

$$H' = H \cdot N \subseteq H \cdot [H', H'] \subseteq H'.$$

Hence, we have that $H' = H \cdot [H', H']$. By the Burnside basis theorem, *cf.* [R, p. 135], any set of elements of H' which generates $H'/[H', H']$ also generates all of H' . Therefore, we see that $H = H'$. Thus, we know that $N \subseteq [H, H] \subseteq H$. Since $N \subseteq [H, H]$, all degree 1 characters of H are trivial on N . Thus, for any p -group H we see that

$$f(H, \varphi) = \frac{p^m}{\#H} (p^k - p^k) = 0 \in \mathbb{Z}.$$

Now we suppose that $N \cap H = \{1\}$. Let H_p be a Sylow p -subgroup of H . Let r be the index $[H : H_p]$. Thus,

$$\begin{aligned} f(H, \varphi) &= \frac{p^m(p^k - 1)}{\#H} = \frac{p^m}{\#H_p} \frac{p^k - 1}{r} \\ &= f(H_p, \text{Res}\varphi) \frac{p^k - 1}{r}. \end{aligned}$$

Since the part of n relatively prime to p is $(p^k - 1)$, we see that $r \mid p^k - 1$. We already saw that $f(H_p, \varphi) \in \mathbb{Z}$. Thus, we know that $f(H, \varphi) \in \mathbb{Z}$ for any elementary subgroup H and any degree 1 character φ of H .

Therefore, by Proposition 4.4, χ is a virtual character. Since $(\chi, \chi) = 1$ and $\chi(1) > 0$ we see that χ is the character of a simple $\mathbb{C}[G]$ -module V . Finally, since $\chi(1)\chi$ is the character of the virtual module $\mathbb{C}[G] - \mathbb{C}[G/N]$, we conclude that $\mathbb{C}[G] \cong \mathbb{C}[G/N] \oplus \text{End}_{\mathbb{C}} V$. \square

Here is one family of groups which satisfies the conditions of Theorem 4.3. Let k be a finite field over the prime field \mathbb{F}_p , let W be a finite-dimensional vector space over k , and let W^\vee be its dual space over k . Let

$$G = k \times W \times W^\vee \times k^\times$$

with the multiplication

$$(a, v, f, c) \cdot (b, w, g, d) = (a + cb + f(w), v + cw, f + g, cd).$$

Let $N = k \subseteq G$. Here C is $k \times W \times W^\vee$. Subgroups H , such that $N \subseteq H \subseteq C$, are of the form $k \times U$ for U an \mathbb{F}_p -subspace of $W \times W^\vee$. We compute the commutator:

$$[(a, v, f, 1), (b, w, g, 1)] = (f(w) - g(v), 0, 0, 1).$$

Thus, condition (4) of Theorem 4.1 reduces to proving that if $\#U > \#W$, then the antisymmetric \mathbb{F}_p -bilinear map $U \times U \rightarrow k$ given by $[(v, f), (g, w)] = f(w) - g(v)$ is surjective. It is sufficient to prove that the \mathbb{F}_p -bilinear form $[(v, f), (g, w)] = \pi(f(w) - g(v))$ on the \mathbb{F}_p -vector space U is nonzero for every \mathbb{F}_p -linear surjection $\pi : k \rightarrow \mathbb{F}_p$. Thus, condition (4) follows from the well-known fact that isotropic

subspaces of a symplectic space have dimension at most half the dimension of the space.

5. THE STRUCTURE OF THE p -GROUP C

In order to prove Theorem 1.1 we need to get a bound on n in terms of e in the normal subgroup case. To do this we will use the Schreier subgroup lemma to study the structure of C .

Theorem 5.1 (Schreier cf. [R, 6.1.8]). *Let G be a group generated by n elements. Let H be a subgroup of G of finite index i . Then N is generated by $i(n - 1) + 1$ elements.*

Theorem 5.2. *Let G be a group of order n and V a simple $\mathbb{C}[G]$ -module of dimension d such that $n = d(d + e)$. If $e > 1$, then we have that $n \leq e^{4e^2}$.*

Proof. In view of Theorem 3.1 and Proposition 3.2 we need only consider the case where G and V satisfy the conditions of Theorem 4.1. Thus, we see that $e = p^m$, there exists a p -group H with order p^{k+m+1} , and H has an elementary abelian subgroup N of order p^k , and $N \subseteq [H, H]$.

Since N is contained in the Frattini subgroup of H and $\#H/N = p^{m+1}$, we see, by the Burnside basis theorem, that H is generated by $m + 1$ elements. Thus, by Theorem 5.1, we see that N is generated by $p^{m+1}m + 1$ elements. Since N is elementary abelian of rank k , we see that $k \leq p^{m+1}m + 1$. To get the explicit bound we calculate

$$\begin{aligned} \log_p(n) &= \log_p(p^{2m+k}(p^k - 1)) \leq 2m + 2k \\ &\leq 2m + 2(p^{m+1}m + 1) = 2(m + 1) + 2p^{m+1}m \leq 4p^{2m}m = \log_p(e^{4e^2}). \quad \square \end{aligned}$$

Using a result of Gagola's we can strengthen the bound in Theorem 5.2.

Theorem 5.3. *Let N , C and e be as in Theorem 4.1, and further assume that $e > 1$ and is not a power of 2. The centralizer of N in C is strictly larger than N .*

Proof. This is Theorem 6.2 in [G]. When $p > 2$, Gagola gave an elegant two-paragraph proof on the bottom of page 379 (the second paragraph together with the paragraph beginning "Suppose then that G/N is nonsolvable. If $p > 2...$ ", where the assumption that G/N is nonsolvable is not used.) For $p = 2$, Gagola gave a much longer proof of Theorem 5.3 using the classification of finite simple groups. As the rest of this paper is elementary, we avoid reliance on the $p = 2$ case. □

Theorem 5.4. *Let e , k , and m be as in Theorem 4.1. If $e > 1$ and is not a power of 2, then we have that $k < 2m$.*

Proof. By Theorem 5.3, there exists an element $y \in C - N$ such that N is a proper subgroup of the centralizer of y in G , denoted $Z_y(G)$. Let $[y]$ be the conjugacy class of y in G . By Lemma 2.2, we see that $[y]$ is the inverse image of the conjugacy class of the image of y in G/N . In particular we see that $\#N \mid \#[y]$. Therefore, we know that

$$p^k = \#N \mid \#[y] = \frac{\#G}{\#Z_y(G)} \mid \frac{\#G/N}{p} = p^{2m-1}(p^k - 1).$$

Thus, we see that $k < 2m$. □

Theorem 5.4 tightens the bound significantly in the normal subgroup case of Theorem 5.2; however, this gives only a marginal improvement in general, since the factorial bound will dominate.

Theorem 5.5. *Let G be a finite group of order n with a simple $\mathbb{C}[G]$ -module V of dimension d and $d(d+e) = n$. Suppose that $e > 1$ is not a power of 2. Then, $n \leq ((2e)!)^2$.*

Proof. In the $d = e$ case or the factorial case, $(d+e) \mid (2e)!$, so this follows immediately. In the normal subgroup case, since e is not a power of 2, by Theorem 5.4 we see that, for $e \geq 3$,

$$n = p^{k+2m}(p^k - 1) < p^{6m} = e^6 \leq ((2e)!)^2. \quad \square$$

Notice that we do not know of any examples of the factorial case with $d > e$. This leaves open the possibility of much stronger results. In particular it is still conceivable that $2d^2 > n$ implies the normal subgroup case or that the polynomial bound in Theorem 5.4 holds in general.

The bounds which we have already proved in Theorems 3.1 and 5.4 are enough to completely classify all groups and all simple modules with $e = 2$ or $e = 3$. However, for $e = 2$, recall that Theorem 5.4 depends on the classification of finite simple groups. To avoid this dependence we will use a result of Taussky [T].

6. CLASSIFICATION FOR $e = 2$ AND $e = 3$

Theorem 6.1 (cf. [H, Chapter III, Satz 11.9(a)]). *Suppose that C is a 2-group and that $[C, C]$ has index 4 in C . Then $[C, C]$ is cyclic.*

Theorem 6.2. *Let G be a finite group of order n with a simple $\mathbb{C}[G]$ -module V of dimension d such that $d(d+2) = n$. Then G is a cyclic group of order 3, or G is a nonabelian group of order 8.*

Proof. If $d = 1$, then $n = 3$. Thus, $d = 1$ implies that G is the cyclic group of order 3. If $d = 2$, then $n = 8$. If G were abelian, then it would have no irreducible degree 2 characters. Therefore, $d = 2$ implies that G is a nonabelian group of order 8. Thus, it is enough to show that $d \leq 2$.

The argument splits up according to the three cases of Theorem 3.1. Case (1) states that $d = 2$. Case (2) states that $d+2 \mid 3$. Hence, $d = 1$. Case (3) states that G satisfies the assumptions of Theorem 4.1. Thus, there exists a nontrivial elementary abelian subgroup N of G and a Sylow 2-subgroup C of G , such that N has index 4 in C , and $N \subseteq [C, C]$. Since C/N has order 4, it must be abelian. Thus, we see that $N = [C, C]$. So, by Theorem 6.1, we see that N is cyclic. Since it is also nontrivial and elementary abelian it must have order 2. But $d = 2(\#N - 1)$, so we see that d must be 2. \square

There is a nice consequence of Theorem 6.2. For $d > 1$, we have that $d(d+3) > (d+1)^2$. Thus, if G is a group and V is a simple $\mathbb{C}[G]$ -module such that $\dim V = \lfloor \sqrt{\#G} \rfloor$, then G is cyclic of order at most 3, or G is nonabelian of order 8, or G is a doubly transitive Frobenius group.

Theorem 6.3. *Let G be a finite group of order n with a simple $\mathbb{C}[G]$ -module V of dimension d such that $d(d+3) = n$. Then G is one of the two abelian groups of order 4, or G is the dihedral group of order 10, or G is one of two groups of order 54 satisfying the conditions of Theorem 4.1.*

Proof. Again we split into cases based on Theorem 3.1. The key additional ingredient is [Se, Cor. to Prop. 8.1], which states that the degree of any irreducible representation divides the index of any abelian normal subgroup. Case (1) states that $d = 3$. Thus, $n = 18$. Clearly, the Sylow 3-subgroup is abelian, normal, and of index 2. Thus, $3 \mid 2$, which is a contradiction.

Now consider case (2). If $d = 1$, then $n = 4$. Thus, $d = 1$ implies that G is an abelian group of order 4. If $d = 2$, then $n = 10$. If G were abelian, then it would have no degree 2 irreducible characters. Therefore, $d = 2$ implies that G is the nonabelian group of order 10. If $d > 3$ and $d + 3 \mid 5!/3$, it is easy to see that d is prime and that the Sylow d -subgroup is normal and cyclic. Thus, $d \mid d + 3$, which contradicts the assumption that $d > 3$.

Finally consider case (3). By Theorem 5.4, we see that G must be a group of order 54 satisfying the conditions of Theorem 4.1. The fact that there are exactly two such groups is left as an exercise for the reader. \square

REFERENCES

- [Ber] Berkovich, Y., "Groups with few characters of small degrees." *Israel J. Math.* 110 (1999), 325–332. MR1750431 (2001a:20013)
- [Bel] Belonogov, V. A., "Recovery of an erased row or column in a table of characters of a finite group." *Algebra Logika* 41 (2002), no. 3, 259–275, 386. MR1934536 (2003i:20011)
- [Bu] Burtsev, A. I., "Groups with arithmetic restrictions for conjugacy classes of elements," *Dep. VINITI*, No. 3011–82 (1982).
- [G] Gagola, S., "Characters vanishing on all but two conjugacy classes." *Pacific J. Math.* 109 (1983), no. 2, 363–385. MR721927 (85e:20009)
- [H] Huppert, B., "Endliche Gruppen 1." Springer-Verlag (1967). MR0224703 (37:302)
- [K] Kuisch, E., "Sylow p -subgroups of solvable Camina pairs." *J. Algebra* 156 (1993), no. 2, 395–406. MR1216476 (94e:20030)
- [K-vdW1] Kuisch, E., and van der Waall, R., "Homogeneous character induction." *J. Algebra* 149 (1992), no. 2, 454–471. MR1172440 (93f:20012)
- [K-vdW2] Kuisch, E., and van der Waall, R., "Homogeneous character induction. II." *J. Algebra* 170 (1994), no. 2, 584–595. MR1302857 (95i:20013)
- [R] Robinson, D., "A Course in the Theory of Groups." Springer-Verlag (1996). MR1357169 (96f:20001)
- [Se] Serre, J-P., "Linear Representations of Finite Groups." Springer-Verlag (1977). MR0450380 (56:8675)
- [T] Taussky, O., "A remark on the class field tower." *J. London Math. Soc.* 12 (1937), 82–85.
- [Z] Zassenhaus, H., "Über endliche Fastkörper." *Abhandl. Hamburg* 11 (1935), 187–220.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720
E-mail address: nsnyder@math.berkeley.edu