Contemporary Mathematics

Character Theory and Group Rings

D. S. Passman

Dedicated to Professor I. Martin Isaacs

Abstract. While we were graduate students, Marty Isaacs and I worked together on the character theory of finite groups, studying in particular the character degrees of finite p-groups. Somewhat later, my interests turned to ring theory and infinite group theory. On the other hand, Marty continued with character theory and soon became a leader in the field. Indeed, he has had a superb career as a researcher, teacher and expositor. In celebration of this, it is my pleasure to discuss three open problems that connect character theory to the ring-theoretic structure of group rings. The problems are fairly old and may now be solvable given the present state of the subject. A general reference for character theory is of course Marty's book [**6**], while [**10**] affords a general reference for group rings.

1. Character Regular p-Groups

As is well known, the degrees of the irreducible complex characters of a finite p-group G are all powers of p, and we write $e(G) = e$ if the largest such character degree is equal to p^e. It is presumably a hopeless task to try to characterize the p-groups G with $e(G)$ equal to a specific number e, but it is possible that certain of these groups, the ones that do not have a maximal subgroup M with $e(M) = e-1$, do in fact exhibit some interesting structure. One possible tool to study this situation is based on the following

Definition 1.1. *If $e(G) = e$, then G is said to be character regular precisely when G is faithfully embedded in the totality of its irreducible representations of degree p^e, or equivalently when*

$$\bigcap_{\chi(1)=p^e} \ker\chi = 1.$$

One can use this concept, for example, to obtain information on the center of certain subgroups of G. Specifically, we have

2000 *Mathematics Subject Classification.* 16S34, 20C15.
Research supported in part by an NSA grant.

LEMMA 1.2. *Let $H \triangleleft G$ be p-groups with $e(H) = e(G)$. If H is character regular, then $\mathbb{Z}(H) \subseteq \mathbb{Z}(G)$.*

PROOF. If $h \in \mathbb{Z}(H)$ and $g \in G$, then the commutator $x = [h, g]$ is contained in H since $H \triangleleft G$. Now let χ be any irreducible character of H of degree p^e, where $e = e(H)$, and let $\mathfrak{X}$ be its corresponding representation. Since $e(G)$ is also equal to e, it follows that χ is the restriction of a character χ' of G with corresponding representation $\mathfrak{X}'$. Now $\mathfrak{X}(h)$ is a scalar matrix, so the same is true of $\mathfrak{X}'(h)$. Hence $\mathfrak{X}'(x) = [\mathfrak{X}'(h), \mathfrak{X}'(g)] = 1$, and $x \in H \cap \ker \chi' = \ker \chi$. Since χ is an arbitrary character with $\chi(1) = p^e$, x is contained in the kernels of all characters of H of largest degree. In particular, since H is character regular, we conclude that $x = 1$ and hence that $[h, g] = 1$. But $g \in G$ is arbitrary, so $h \in \mathbb{Z}(G)$, as required. $\square$

As it turns out, not all p-groups are character regular. Indeed, we have [**8**]

LEMMA 1.3. *For any $e \geq p$, there exists a p-group G with $e(G) = e$ that is not character regular.*

PROOF. Let $H_1, H_2, \ldots, H_e$ be e nonabelian groups of order p^3 and let H be the direct product $H = H_1 \times H_2 \times \cdots \times H_e$. Since $e(H_i) = 1$, it is clear that H has character degrees p^k for $k = 0, 1, \ldots, e$, and hence $e(H) = e$. Furthermore, if W denotes the center of H, then $W = W_1 \times W_2 \times \cdots \times W_e$, where W_i is the center of H_i and has order p.

Now let Z be an elementary abelian group of order p^2, so that Z has $p + 1$ subgroups of order p, say $Z_0, Z_1, \ldots, Z_p$. Since $e \geq p$, we can define a homomorphism $\theta \colon W \to Z$ so that $\theta(W_i) = Z_i$ for $i = 1, 2, \ldots, p-1$ and $\theta(W_i) = Z_p$ for $i = p, p+1, \ldots, e$. If $N = \ker \theta$, then N is a central and hence normal subgroup of H, and we let $G = H/N$. Clearly $W/N = Z$ is the center of G, and we now show that $e(G) = e$ and that $Z_0 = \bigcap_{\chi(1)=p^e} \ker \chi$.

To this end, for $i = 0, 1, \ldots, p$, let $N_i = \theta^{-1}(Z_i)$. Then the N_i are the $p + 1$ subgroups of W of index p that contain N. Observe that $N_i = NW_i$ for $i = 1, 2, \ldots, p-1$ and that $N_p = NW_i$ for $i = p, p+1, \ldots, e$. Now suppose χ is a character of H with $W \cap \ker \chi = N_0$. Then χ is a product $\chi = \chi_1 \chi_2 \cdots \chi_e$, where χ_i is an irreducible character of H_i. Furthermore, W_i is not contained in the kernel of χ_i, since otherwise $\ker \chi$ contains $N_0 W_i = N$, a contradiction. Thus each χ_i has degree p, so χ has degree p^e. Since $\ker \chi \supseteq N$, χ corresponds to a character of $G = H/N$ and hence $e(G) = e$.

Conversely, let χ be a character of G of degree p^e and view χ as a character of H. Again χ is a product $\chi = \chi_1 \chi_2 \cdots \chi_e$ and, since $\chi(1) = p^e$, it follows that each χ_i has degree p. Thus W_i is not contained in $\ker \chi_i$ and hence W_i is not contained in $\ker \chi$. But, we know that $W \cap \ker \chi$ must be one of the $p + 1$ subgroups of W of index p that contain N. Since $\ker \chi$ cannot contain $N_1, N_2, \ldots,$ or N_p, it follows that $\ker \chi \supseteq N_0$. Viewed in G, this says that $\ker \chi \supseteq N_0/N = Z_0$ and we conclude easily that $Z_0 = \bigcap_{\chi(1)=p^e} \ker \chi$, as claimed. $\square$

This leads to the problem we pose in this section, namely

PROBLEM 1.4. *Let G be a finite p-group with $e(G) = e$. If $p > e$, must G be character regular?*

This is known to be the case at least for $e = 1$ and 2. Furthermore, one can show that if $e(G) = e$, then the subgroup $\bigcap_{\chi(1)=p^e} \ker \chi$ has order bounded by a function of p^e. Indeed, this is a special case of a result concerning arbitrary finite groups [**9**]. As will be apparent, the proof of the latter is totally ring theoretic.

PROPOSITION 1.5. *Let G be an arbitrary finite group having an irreducible character of degree $\geq n$. Then $\bigcap_{\chi(1)\geq n} \ker\chi$ has order at most $(2n-2)!$.*

PROOF. For each integer $k \geq 1$, let

$$s_k(x_1, x_2, \ldots, x_k) = \sum_{\sigma \in \mathrm{Sym}_k} (-)^{\sigma} x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(k)}$$

denote the standard polynomial over the complex numbers K in the k noncommuting variables $x_1, x_2, \ldots, x_k$. Observe that s_k is linear in each of its variables, and a result of Amitsur and Levitzki [**1**] asserts that the full matrix ring $\mathbf{M}_\ell(K)$ satisfies $s_{2k} = 0$ if and only if $\ell \leq k$. In other words, if we evaluate s_{2k} on any $2k$ elements of $\mathbf{M}_\ell(K)$, then we always obtain 0 precisely when $\ell \leq k$.

Now the complex group ring $K[G]$ is a direct sum of full matrix rings over K and, since G has an irreducible representation of degree $\geq n$, it is clear that $K[G]$ does not vanish on s_{2n-2}. In particular, by the multilinearity of the polynomial, there exist group elements $g_1, g_2, \ldots, g_{2n-2} \in G$ such that

$$0 \neq \alpha = s_{2n-2}(g_1, g_2, \ldots, g_{2n-2}) \in K[G].$$

The definition of s_{2n-2} as a sum over $\sigma \in \mathrm{Sym}_{2n-2}$ implies that α has support size $\leq (2n-2)!$. In other words, at most $(2n-2)!$ group elements have nonzero coefficients in the representation of $\alpha \in K[G]$ as a K-linear sum of group elements. Furthermore, by the Amitsur-Levitzki result, α projects to 0 in the direct summand of $K[G]$ consisting of all matrix rings of degree $< n$.

Now write $N = \bigcap_{\chi(1)\geq n} \ker\chi$. If $x \in N$, then by definition, $1-x$ projects to 0 in the direct summand of $K[G]$ consisting of all matrix rings of degree $\geq n$. In particular, $\alpha(1-x) = 0$ and hence $\alpha = \alpha x$. It follows that if $S \subseteq G$ denotes the support of α, then $S = Sx$ and hence N permutes the elements of S via right multiplication. But this multiplication action is semiregular, so we conclude that $|N| \leq |S| \leq (2n-2)!$ and the proposition is proved. □

At this point, it is not clear how or if the above argument can be extended. One could look for a multilinear polynomial identity for $\mathbf{M}_n(K)$ with a small number of monomials, but these do not exist. On the other hand, if we are willing to increase the number of monomials, we could replace s_{2n-2} by a central polynomial for $\mathbf{M}_n(K)$. This is a polynomial in noncommuting variables that maps $\mathbf{M}_n(K)$ nontrivially to its center, and as a consequence is a polynomial identity for all matrix rings of smaller degree. With such a central polynomial, we would then be able to find an element α as above that is central in $K[G]$, but this centrality does not seem to be of use here. Presumably, Problem 1.4 will require a character-theoretic proof of some sort assuming the conjecture turns out to be correct.

2. Simple Twisted Group Algebras

Let G be a finite group and let K be a field. Then a twisted group algebra K^tG is an associative K-algebra having basis $\overline{G} = \{\overline{g} \mid g \in G\}$ and with multiplication given by $\overline{x}\,\overline{y} = \mu_{x,y}\,\overline{xy}$ for all $x, y \in G$, where $\mu_{x,y} \in K^\bullet$. For example, if all $\mu_{x,y} = 1$, then $K^tG = K[G]$ is the ordinary group algebra. It is easy to check that the associativity of K^tG is equivalent to the map $\mu\colon G\times G\to K^\bullet$ being a 2-cocycle on G, but associativity is the more natural condition to work with.

Twisted group algebras are of course related to projective representations of groups. Indeed, if $\mathfrak{X}\colon K^tG\to \mathbf{M}_n(K)$ is an irreducible representation, then the formula $\mathfrak{X}(\overline{x})\,\mathfrak{X}(\overline{y})=\mu_{x,y}\,\mathfrak{X}(\overline{xy})$ describes a projective representation of G. Alternatively, suppose H is a group with a cyclic central subgroup Z and suppose $\lambda\colon Z\to K^\bullet$ is a faithful linear character of Z. Then we can use λ to identify Z with the subgroup $\lambda(Z)\subseteq K^\bullet$. Indeed, if I is the ideal of $K[H]$ generated by all $z-\lambda(z)$, with $z\in Z$, then $K[H]/I$ is easily seen to be a twisted group algebra of $G=H/Z$. The converse, however, is not true in general unless we assume K to be algebraically closed.

Lemma 2.1. *Let K^tG be a twisted group algebra of the finite group G over an algebraically closed field K. Then there exists a finite group H, with central cyclic subgroup Z, such that $G\cong H/Z$. Furthermore, there is a faithful linear character $\lambda\colon Z\to K^\bullet$ such that $K^tG\cong K[H]/I$, where I is the ideal of $K[H]$ generated by the elements $z-\lambda(z)$ for all $z\in Z$.*

Proof. Let $\mathfrak{G}=\{k\overline{x}\mid x\in G,\ k\in K^\bullet\}$ be the group of trivial units of K^tG. Then the map $\mathfrak{G}\to G$ given by $k\overline{x}\mapsto x$ is a group epimorphism with kernel $\mathfrak{Z}=K^\bullet$. In other words, $\mathfrak{G}/\mathfrak{Z}\cong G$ and, since $\mathfrak{Z}$ is central in $\mathfrak{G}$, the group $\mathfrak{G}$ is center-by-finite. A result of Schur [**11**] now implies that the commutator subgroup $\mathfrak{G}'$ is finite. To proceed further, we need K to be algebraically closed.

For each $x\in G$, we know that $\overline{x}^{o(x)}\in\mathfrak{Z}$, where $o(x)$ is the order of x. Hence, since K is algebraically closed, we can choose $a\in K$ with $a^{o(x)}=\overline{x}^{o(x)}$. It follows that $\tilde{x}=a^{-1}\overline{x}\in\mathfrak{G}$ has finite order $o(x)$, and we let H be the subgroup of $\mathfrak{G}$ generated by all $\tilde{x}$, one for each $x\in G$. Then H is finitely generated by elements of finite order and, since $H'\subseteq\mathfrak{G}'$ is finite, it follows that H is a finite subgroup of $\mathfrak{G}$. Furthermore, H maps onto G via the map of the preceding paragraph, and hence $H/Z\cong G$ where $Z=H\cap\mathfrak{Z}$.

Certainly Z is cyclic, since it is a finite subgroup of $K^\bullet$, and indeed the embedding $\lambda\colon Z\to K^\bullet$ is a faithful linear character of Z. Furthermore, the embedding $H\to\mathfrak{G}$ gives rise to an epimorphism $K[H]\to K^tG$, and the kernel I of this map contains the elements $z-\lambda(z)$ for all $z\in Z$. In fact, I is generated by all $z-\lambda(z)$ since any transversal for Z in H has a linearly independent image in K^tG. $\square$

Some version of the algebraically closed assumption is certainly needed in the above. To see this, suppose $G=\langle g\rangle$ is cyclic of order $n>1$ and let K be the field of rational numbers. Then $K[x]/(x^n-2)$ is isomorphic to a twisted group algebra of G, with $\overline{g}$ corresponding to the image of the variable x. Note that $\overline{g}^n=2$ so, since K is the rational field, no scalar multiple of $\overline{g}$ can have finite order in $\mathfrak{G}$. In particular, K^tG cannot be a natural homomorphic image of the group ring $K[H]$ for any finite group H.

While we have the above notation in mind, let us point out the following observation that is usually proved by cohomological considerations.

Lemma 2.2. *If K is an algebraically closed field of characteristic p and if G is a finite p-group, then any twisted group algebra K^tG is naturally isomorphic to $K[G]$.*

Proof. Notice that $H/Z\cong G$, so H is also nilpotent. In particular, we can write $H=P\times Q$, where P is its Sylow p-subgroup and Q its p-complement.

Obviously P maps onto G, so we can assume that $H = P$. But then Z is isomorphic to a p-subgroup of $K^\bullet$, so $Z = 1$ and $K^tG \cong K[H] \cong K[G]$. $\square$

Of course, ordinary group algebras are never simple since they always have a proper augmentation ideal. But twisted group algebras can be simple and the question of interest here is

Problem 2.3. *When is a twisted group algebra K^tG simple? In particular, is G necessarily a solvable group?*

If K is an algebraically closed field of characteristic 0, then Lemma 2.1 and its notation imply that K^tG is simple if and only if the group H is of central type. In other words, this occurs if and only if H has a unique irreducible character χ whose restriction χ_Z to Z has λ as a constituent. From a ring-theoretic point of view, this is why groups of central type are so interesting. Furthermore, we know from the fundamental paper [**5**] of Howlett and Isaacs that groups of central type are necessarily solvable. Thus $G = H/Z$ is also solvable.

Recall that a K-algebra A is said to be central simple if A is simple and has center K. As is well known, if A is central simple, then so is any F-algebra $F \otimes_K A$, where F is a field extension of K. In particular, if K^tG is central simple and if $\overline{K}$ is the algebraic closure of K, then $\overline{K} \otimes_K K^tG = \overline{K}^tG$ is also simple and the above yields

Proposition 2.4. *If K is a field of characteristic 0 and K^tG is central simple, then G is solvable.*

So the real problem in extending [**5**] to arbitrary characteristic 0 fields is the presence of additional central elements. Now it is easy to describe the center of any twisted group algebra. To this end, given K^tG and $x \in G$, we define

$$\mathbb{C}^t_G(x) = \{y \in G \mid \bar{x}\,\bar{y} = \bar{y}\,\bar{x}\}.$$

Then it is clear that $\mathbb{C}^t_G(x)$ is a subgroup of G contained in the centralizer $\mathbb{C}_G(x)$. Indeed, if $g \in \mathbb{C}_G(x)$, then $\bar{g}\,\bar{x} = \tau(g)\,\bar{x}\,\bar{g}$, where $\tau\colon \mathbb{C}_G(x) \to K^\bullet$ is a linear character with kernel $\mathbb{C}^t_G(x)$. If $\mathbb{C}^t_G(x) = \mathbb{C}_G(x)$, then the conjugacy class of x is said to be special, and it is easy to see that the center of K^tG is the K-linear span of the class sums of all such special classes.

Of course, if K^tG is simple, then its center F is a finite field extension of K, and the behavior of F under further field extensions of K is well known. We offer a quick proof below.

Lemma 2.5. *Let F/K be a finite separable extension of fields and let $L \supseteq F$ contain the Galois closure of F. Then $L \otimes_K F = L_1 \oplus L_2 \oplus \cdots \oplus L_n$, a direct sum of $n = |F : K|$ copies of L. Furthermore, the embedding of F into this direct sum is given by $a \mapsto \sigma_1(a) \oplus \sigma_2(a) \oplus \cdots \oplus \sigma_n(a)$, where $\sigma_1, \sigma_2, \ldots, \sigma_n \colon F \to L$ are the n distinct K-linear embeddings of F into L.*

Proof. The primitive element theorem tells us that $F = K[\alpha]$, and we let $g(x)$ be the minimal monic polynomial of α over K. Then $F \cong K[x]/(g(x))$, so $L \otimes_K F \cong L[x]/(g(x))$. But $g(x)$ splits in L as $\prod_{i=1}^n (x - \alpha_i)$, so $L[x]/(g(x)) \cong L_1 \oplus L_2 \oplus \cdots \oplus L_n$, as required. Furthermore, since the image of x in L_i is α_i, the embedding of F is determined by $\alpha \mapsto \alpha_1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_n$. $\square$

As a consequence, we see that if K^tG is simple, with $\operatorname{char} K = 0$, and if $\overline{K}$ is the algebraic closure of K, then $\overline{K}^t G = \overline{K} \otimes_K K^tG$ is a direct sum of full matrix rings over $\overline{K}$ that correspond to a full set of Galois conjugate projective representations of G. In terms of the lifted group H, where $H/Z \cong G$, this says that the irreducible characters of H that extend the linear character $\lambda\colon Z \to K^\bullet$ are all Galois conjugate. So one wonders whether the methods of [**5**] can be extended to handle this situation.

We briefly mention what happens in characteristic p. To start with, any simple algebra is certainly semisimple, so the following is relevant.

Lemma 2.6. *Let K^tG be a semisimple twisted group algebra.*

i. If H is a subgroup of G, then K^tH is semisimple.

ii. If K has characteristic $p > 0$ and if P is a Sylow p-subgroup of G, then K^tP is a purely inseparable field extension of K. It follows that G has a normal p-complement.

Proof. (i) First note that there is a K-linear projection map $\theta\colon K^tG \to K^tH$ given by $\theta(\overline{x}) = \overline{x}$ if $x \in H$ and $\theta(\overline{x}) = 0$ if $x \in G \setminus H$. It is easy to see that θ is a (K^tH, K^tH)-bimodule homomorphism. Next, observe for a finite dimensional K-algebra A, semisimplicity is equivalent to von Neumann regularity. The latter, of course, asserts that for all $\alpha \in A$, there exists $\alpha' \in A$ with $\alpha\alpha'\alpha = \alpha$. Finally, let $\alpha \in K^tH$. Since K^tG is semisimple, there exists $\alpha' \in K^tG$ with $\alpha\alpha'\alpha = \alpha$. Applying the bimodule map θ now yields $\alpha = \theta(\alpha) = \theta(\alpha\alpha'\alpha) = \alpha\,\theta(\alpha')\,\alpha$, and consequently K^tH is semisimple.

(ii) In view of (i), we know that K^tP is semisimple. Furthermore, by Lemma 2.2, $\overline{K}^t P \cong \overline{K}[P]$, where $\overline{K}$ is the algebraic closure of K. If I denotes the copy of the augmentation ideal of $\overline{K}[P]$ in K^tP, then $\overline{K}^t P/I \cong \overline{K}$ and I is nilpotent. Thus, since K^tP is semisimple, we have $K^tP \cap I = 0$ and consequently K^tP embeds in $\overline{K}^t P/I \cong \overline{K}$. It follows that K^tP is isomorphic to a subfield of $\overline{K}$ containing K. Since it is generated by the various $\overline{x}$, with $x \in P$, and since $\overline{x}^{o(x)} \in K$, we see that K^tP is purely inseparable over K.

Finally, let $g \in \mathbb{N}_G(P)$. Then conjugation by $\overline{g}$ induces a field automorphism of K^tP fixing K. But K^tP is purely inseparable over K, so this automorphism must be trivial. Clearly this implies that $\mathbb{N}_G(P) = \mathbb{C}_G(P)$ and hence that G has a normal p-complement. $\square$

It is a well known character-theoretic result that Hall subgroups of groups of central type are also of central type. Since the proof of this fact merely uses dimensions of modules, it carries over to twisted group algebras over any field. We include the simple argument.

Lemma 2.7. *Let K^tG be a simple twisted group algebra and let H be a Hall π-subgroup of G. Then K^tH is also simple.*

Proof. Since K^tG is simple, its regular module $R(G)$ is equal to aV, where the simple module V occurs with multiplicity a. Furthermore, since K^tH is semisimple, we have $R(H) = bW + U$, where the simple K^tH-module W occurs with multiplicity b and where U denotes a sum of other simple modules. The goal is to show that $U = 0$. Now K^tG is a free K^tH-module of rank $|G : H|$, so restricting to K^tH yields $|G : H|\,(bW + U) = |G : H|\,R(H) = R(G)_H = aV_H$. It follows that a divides $|G : H|\,b$, so $|a|_\pi$ divides b, since $|G : H|$ is a π' number.

Next, module induction tells us that $W^G = cV$ for some multiplicity c. Thus, by dimension considerations, we have $c \dim V = \dim W^G = |G : H| \dim W$, so $\dim V$ divides $|G : H| \dim W$ and hence $|\dim V|_\pi$ divides $\dim W$. We conclude that $|H| = |G|_\pi = |a \dim V|_\pi$ divides $b \dim W$. But $b \dim W + \dim U = |H|$, so we must have $U = 0$ and hence $K^t H$ is simple. □

Finally, if $K^t G$ is simple and K has characteristic $p > 0$, then we know that G has a normal complement N. Furthermore, the preceding lemma implies that $K^t N$ is also simple. Since the ordinary and modular character theory of N agree, modular simplicity of $K^t N$ surely lifts to the characteristic 0 case. Thus, there may be nothing new to say in characteristic p.

3. The Number of Irreducible Representations

If K is the field of complex numbers, or any algebraically closed field of characteristic 0, then we know that the number n of irreducible representations of $K[G]$ is equal to the dimension of the center of the algebra and hence equal to the number of conjugacy classes of the group G. Furthermore, the class equation then yields

$$1 = \frac{1}{c_1} + \frac{1}{c_2} + \cdots + \frac{1}{c_n}$$

where c_i is the order of the centralizer of an element in the ith conjugacy class. In particular, if the first class corresponds to the identity element, then $c_1 = |G|$. As Landau [**7**] pointed out, if we are given n, then equations as above have only finitely many positive integer solutions $c_1, c_2, \ldots, c_n$, and as a consequence one has

Proposition 3.1. *If K is the field of complex numbers and if $K[G]$ has precisely n irreducible representations, then $|G|$ is bounded by a function of n.*

The above proof is elementary, but it is an accident of number theory. On the other hand, it can presumably be replaced by a very much harder argument using the classification of the finite simple groups [**3**]. For example, suppose that $G \neq 1$ has precisely n conjugacy classes, and let us further assume that G has no nonidentity finite solvable normal subgroup. Then the socle H of G is a finite direct product $H = H_1 \times H_2 \times \cdots \times H_k$ of nonabelian simple groups H_i, and G permutes these factors by conjugation. In particular, if $1 \neq h_i \in H_i$, then the k elements $h_1, h_1h_2, h_1h_2h_3, \ldots$ cannot be G-conjugate and hence $k \leq n$. Furthermore, if x and y are nonidentity elements of the same H_i and if $x^g = y$, then g must normalize H_i and hence this conjugation corresponds to the action of an element of $\mathrm{Aut}(H_i)$.

In other words, if we can use the classification of finite simple groups to bound the order of a simple group in terms of the number of conjugacy classes it contains in its automorphism group, then we can bound each $|H_i|$ and hence $|H|$. Since G acts faithfully by conjugation on H, this therefore bounds $|G|$. Furthermore, solvable normal subgroups of G can be handled using the following simple observation.

Lemma 3.2. *Let G have precisely n conjugacy classes and let $1 \neq A \triangleleft G$. Then G/A has at most $n-1$ classes. Furthermore, if A is abelian, then $|A| \leq n\,|G/A|$.*

Proof. We have $G = \bigcup_{i=1}^n C_i$, a union of n conjugacy classes and hence $\overline{G} = G/A = \bigcup_{i=1}^n \overline{C}_i$. Of course, in the latter union there may be overlap and indeed any class contained in A is merged with the identity class. Finally, if A is abelian, then the classes contained in A are precisely the orbits in A under the conjugation action of G/A. Since each orbit has size $\leq |G/A|$ and since there are at most n classes in A, we have $|A| \leq n\,|G/A|$, as required. $\square$

A priori, there seems to be little virtue in the latter argument. But if we change the problem to deal with fields of characteristic p, then the simple number-theoretic observation no longer applies. As was proved by Brauer [**2**], if K is an algebraically closed field of characteristic $p > 0$, then the number of irreducible representations of $K[G]$ is precisely the number of p-regular classes in G. So we pose the following

Problem 3.3. *Let G have precisely n irreducible representations over an algebraically closed field of characteristic $p > 0$. How much of the structure of G can be bounded by a function of n, possibly depending upon p?*

Note that the irreducible representations of G in characteristic p are precisely the irreducible representations of $G/\mathbb{O}_p(G)$. Thus, we cannot hope to bound $|\mathbb{O}_p(G)|$ in the above context. But there are more examples of interest. To start with, let q be a Fermat prime, so that $q = 1 + 2^m$. Then the cyclic group Z_{2^m} of order 2^m acts on Z_q, and we can form the semidirect product $G = Z_q \rtimes Z_{2^m}$. Here, we are taking $p = 2$, and it is easy to see that there are just $n = 2$ classes in G that are 2-regular. Thus, $n = 2$, $p = 2$ and $\mathbb{O}_2(G) = 1$. But the order of G is big and so is the order of $\mathbb{O}_{2'}(G) = Z_q$. In particular, if there exist infinitely many Fermat primes, then we cannot hope to bound $|\mathbb{O}_{p'}(G)|$ as a function of n and p, when $\mathbb{O}_p(G) = 1$.

We can use other prime equations to get similar examples for all primes p. To this end, fix the integer d and suppose q is a prime power of the form $q = 1 + dp^m$. Then Z_{p^m} acts faithfully on E_q, an elementary abelian group of order q, and we can form the semidirect product $G = E_q \rtimes Z_{p^m}$. Here, it is easy to see that there are just $n = d + 1$ classes in G that are p-regular, and of course $\mathbb{O}_p(G) = 1$. Again the order of G is big and so is the order of $\mathbb{O}_{p'}(G) = E_q$. Thus, if the equation $q = 1 + dp^m$ has infinitely many solutions with q a prime power, then we cannot hope to bound $|\mathbb{O}_{p,p'}(G)/\mathbb{O}_p(G)|$ as a function of n and p.

Now, let us return to positive results and a consideration of nonabelian simple groups. For example, if $G = \mathrm{Alt}_m$ with $m > 6$, then we know that $\mathrm{Aut}(G) = \mathrm{Sym}_m$, and consequently elements of G are conjugate in $\mathrm{Aut}(G)$ if and only if they have the same cycle structure. In particular, cycles of odd length $1, 3, 5, \ldots$ are contained in G and are not conjugate in $\mathrm{Aut}(G)$. Furthermore, if we account for the relatively sparse number of cycles with length divisible by p, we see that G contains at least $m/4$ conjugacy classes in $\mathrm{Aut}(G)$ consisting of p-regular elements. The following result is due to Guralnick [**4**]. Part of its proof uses the obvious fact that elements of different order in G cannot be conjugate in $\mathrm{Aut}(G)$.

Theorem 3.4. *Let G be a finite nonabelian simple group and let p be a prime. Suppose G contains at most n conjugacy classes of* $\mathrm{Aut}(G)$ *that are p-regular. Then $|G|$ is bounded by a fixed function of n that does not depend upon p.*

Proof. (Sketch) We can of course ignore the finitely many sporadic groups, so we need only assume that G is alternating or a Chevalley group. We already discussed the alternating groups, but it is best to mention another approach here. Indeed, if $G = \mathrm{Alt}_m$, then there can be at most n primes that are less than or equal to m. Hence the prime number theorem bounds m and $|G|$.

Now let G be a Chevalley group of rank r over a field of size q. To start with, we bound the rank r. For this, note that if $r \geq 8$, then the Weyl group of G involves

Sym_m, where $m = r$ or $r+1$. But then $m!$ divides $|G|$, so there can be at most n primes that are $\leq m$. Again, the prime number theorem bounds m and hence r. Since r can now be fixed, it suffices to consider a specific family of simple groups of specific rank and bound the field size q. Here we note that $|\mathrm{Aut}(G)|/|G|$ is at most $c\cdot \log q$, for some constant c, so it suffices to show that the number of p-regular classes of G grows, as a function of q, more quickly than $\log q$.

To this end, suppose first that G contains a copy of $\mathrm{SL}_2(q)$ or of $\mathrm{PSL}_2(q)$. If q is even, then it follows that G contains cyclic subgroups of relatively prime orders $q-1$ and $q+1$. On the other hand, if q is odd, then G contains cyclic subgroups of relatively prime orders $(q-1)/2$ and $(q+1)/2$. We conclude that G has a cyclic subgroup C of order prime to both p and q, and with $|C| \geq (q-1)/2$. Now embed C in a maximal torus T of G. Then the number of $\mathbb{N}_G(T)$-conjugacy classes contained in C is at least $(q-1)/2|W|$, where $W = \mathbb{N}_G(T)/T$ has order bounded by the size of the Weyl group of G. Furthermore, it follows from the BN-pair description of G that any two semisimple elements in a given maximal torus T are conjugate in G if and only if they are conjugate in $\mathbb{N}_G(T)$. We conclude that G contains at least $(q-1)/2|W|$ classes of p-regular elements, and this linear function of q certainly increases more quickly than a logarithmic function.

Finally, using Dynkin diagrams, it is easy to verify that the only groups that do not contain a copy of $\mathrm{SL}_2(q)$ or of $\mathrm{PSL}_2(q)$ are the Suzuki groups. Indeed, since $|\mathrm{Sz}(q)|$ is prime to 3, these groups cannot possibly contain such linear groups. Nevertheless, one can check that the Suzuki groups have tori of relatively prime orders and of size linear in q. Thus the result follows in this case also. $\square$

As a consequence of the above and the methods discussed previously, we obtain the following partial answer to Problem 3.3. Here, of course, $S/\mathbb{O}^{p'}(S)$ is the largest homomorphic image of S that is a p'-group.

COROLLARY 3.5. *Let the finite group G have precisely n irreducible representations over an algebraically closed field of characteristic $p > 0$. If S is the largest normal solvable subgroup of G, then $|G/\mathbb{O}^{p'}(S)|$ is bounded by a fixed function of n, independent of p.*

It remains to be seen whether this result can be improved. Finally, I would like to thank Prof. Guralnick for allowing me to include his Theorem 3.4 in this paper.

References

[1] S. A. Amitsur and J. Levitzki, *Minimal identities for algebras*, Proc. AMS **1** (1950), 449–463.

[2] R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher Ordnung*, Math. Z. **63** (1956), 406–444.

[3] D. Gorenstein *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, New York, 1982.

[4] R. M. Guralnick, *private communication*, 2010.

[5] R. B. Howlett and I. M. Isaacs, *On groups of central type*, Math. Z. **179** (1982), 555–569.

[6] I. M. Isaacs, *Character Theory of Finite Groups*, AMS Chelsea Publishing, Providence, RI, 2006.

[7] E. Laudau, *Klassenzahl binarer quadratischer Formen von negativer Discriminante*, Math. Annalen **56** (1903), 674–678.

[8] D. S. Passman, *Groups whose irreducible representations have degrees dividing p^2*, Pacific J. Math. **17** (1966), 475–496.

[9] ———, *Character kernels of discrete groups*, Proc. AMS **17** (1966), 487–492.

[10] ———, *The Algebraic Structure of Group Rings*, Krieger Publishing, Malabar, Florida, 1985.
[11] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **127** (1904), 20–50.

Department of Mathematics, University of Wisconsin-Madison, Madison, Wisconsin 53706, USA
E-mail address: passman@math.wisc.edu