Nonnegative Matrices, Brauer Characters, Normal Subsets, and Powers of Representation Modules*

David Chillag
Department of Mathematics
Technion—Israel Institute of Technology
Haifa 32000, Israel

Submitted by Robert M. Guralnick

ABSTRACT

In a previous paper it was shown that some properties of ordinary characters of finite groups are consequences of the theory of nonnegative matrices. In this article we observe that this method can be applied to Brauer characters and normal subsets (in particular conjugacy classes) of finite groups. Results (known ones and new ones) on powers and values of Brauer characters (including ordinary characters), on powers of normal subsets, on values of central characters, and on powers of representation modules are proved as consequences of results on nonnegative matrices.

INTRODUCTION

Let G be a finite group and p a prime number. By regularly representing the Brauer characters of G in characteristic p, we assign to every Brauer character θ a nonnegative matrix $M(\theta)$ with integer entries. Properties of θ correspond to properties of $M(\theta)$, so that the theory of nonnegative matrices (due to Perron, Frobenius, Wielandt, and others) can be applied to obtain results on Brauer characters. The results deal with powers and values of Brauer characters. Once found, most (if not all) the results presented here could be proved without the theory of nonnegative matrices. Our purpose

*The research was partially supported by the fund for the promotion of research at the Technion.

655 Avenue of the Americas, New York, NY 10010 0024-3795/91/$3.50

here is to show that they are, in fact, special cases or consequences of results on nonnegative matrices.

Analogously, a nonnegative integral matrix can be assigned to every normal subset of a finite group G, and results on powers of conjugacy classes and values of the central characters (the ω_χ's for χ an ordinary irreducible character of G) can be shown to be consequences of nonnegative matrix theory.

This paper is the modular and normal subsets analog of our paper [6]. It contains, among other things, generalizations of the results of [6] to Brauer characters, as well as some new results. Most of the proofs here are, in fact, observations on how properties of matrices translate to those of Brauer characters and normal subsets. Some of the results are straightforward generalizations of results from [6]; we include their proof here for completeness' sake, as we do not assume here familiarity with [6].

NOTATION 1.

(1) Let R be the full ring of algebraic integers of the complex number field $\mathbb{C}$, p a fixed prime, M a maximal ideal containing pR, and $F = R/M$. The natural homomorphism from R to F is denoted by $*$. It is well known that F is an algebraically closed field of characteristic p and $F^{\#} = F - \{0\} \cong U$, where $U = \{\epsilon \in \mathbb{C} | \epsilon^m = 1$ for some integer m which is relatively prime to $p\}$. In fact $*$ is an isomorphism from U onto $F^{\#}$ (see p. 263 of [15]).

(2) If G is a finite group and V is an FG-module, we denote the n-fold tensor product $V \otimes V \otimes \cdots \otimes V$ (n times) by V^n.

Next we indicate the type of results obtained.

Let G be a finite group, F as in Notation 1, V an FG-module, and θ the Brauer character afforded by V. It is well known that if V is faithful, then for every indecomposable projective FG-module P there exists an integer n such that P is isomorphic with a direct summand of V^n (see [1, p. 45]), and every irreducible FG-module is isomorphic with a composition factor of $1 \oplus V \oplus V^2 \oplus \cdots \oplus V^{m-1}$, where m is the number of distinct values taken on by θ. We will show (Theorem 2.7) that if a somewhat stronger condition than being faithful is imposed on V, then there exist positive integers k and l such that each indecomposable projective FG-module is isomorphic with a direct summand of V^k and each irreducible FG-module is isomorphic with a composition factor of V^l. Bounds on l will be given.

Analogous theorems are known to be true for conjugacy classes (see [2]); we will observe that they are special cases of results on so-called irreducible and primitive nonnegative matrices. Next we will use results on the graphs and eigenvalues of irreducible nonnegative matrices (which correspond to faithful Brauer characters and to normal subsets generating the group) to get further results on powers of Brauer characters (and hence on powers of their affording modules), powers of normal subsets, values of Brauer characters, and values of the central characters mentioned above.

In Section I we outline the relevant nonnegative matrix theory. Section II is devoted to Brauer characters and their modules. The correspondence of properties of Brauer characters to their matrices is in Proposition 2.5, and the consequences of this proposition are listed in Propositions 2.8, 2.9, 2.10, 2.11, and 2.13. Section III deals with the normal subsets. Here the correspondence of properties of normal subsets to their matrices is in Propositions 3.3, 3.4, and the consequences of these propositions are listed in Corollaries 3.6, 3.7, 3.8, 3.9 and Propositions 3.5, 3.10, 3.12, 3.13, and 3.14.

Our group theory notation and notions are standard and taken mainly from [15].

I. SOME RELEVANT NONNEGATIVE MATRIX THEORY

In this short section we summarize the main notation and notions of nonnegative matrix theory that will be used. Our sources are [5] and [16].

Let $A = (a_{ij})$ be a square matrix of order n with real entries. Then A is called nonnegative (denoted by $A \geqslant 0$) if all its entries are nonnegative, and it is called positive (denoted by $A > 0$) if all its entries are positive. For every positive integer q and every pair (i, j), define $a_{ij}^{(q)}$ by $A^q = \left(a_{ij}^{(q)}\right)$. The matrix A is said to be reducible if it is similar via a permutation matrix to a matrix of the type

$$\begin{pmatrix} C & 0 \\ D & E \end{pmatrix}$$

where C and E are square matrices and 0 is a zero matrix. If A is not reducible, then it is called irreducible. The following is a well-known characterization of irreducible matrices (see [5, p. 29] for a proof).

Proposition 1.1. *A nonnegative matrix $A = (a_{ij})$ is irreducible if and only if for every (i, j) there exists a natural number q such that $a_{ij}^{(q)} > 0$.*

A nonnegative matrix is called primitive if $A^p > 0$ for some positive integer p. In this case the least such p is called the index of primitivity of A, and it will be denoted by $\gamma(A)$. The relevant parts of the celebrated Perron-Frobenius theorem will be quoted next (for proofs see [5]).

THEOREM 1.2. *Let A be a nonnegative matrix. Then:*

(a) *The spectral radius of A is an eigenvalue of A; it is called the leading eigenvalue of A.*

(b) *If A is irreducible, then the leading eigenvalue is a simple root of the characteristic polynomial of A. Every other eigenvalue whose modulus is equal to the spectral radius is also simple.*

(c) *If A is primitive with leading eigenvalue ρ, then ρ is a simple eigenvalue of A and $\rho > |z|$ for any other eigenvalue z of A.*

NOTATION 1.3. The leading eigenvalue of a nonnegative matrix A is denoted by $\rho(A)$. The number of eigenvalues of a nonnegative irreducible matrix A which have modulus equal to $\rho(A)$ is called the index of cyclicity of A (or the index of imprimitivity of A, or simply the index of A).

By Theorem 1.2(a), primitive matrices have cyclicity index equal to 1.

More properties of nonnegative matrices will be introduced as we go along.

II. BRAUER CHARACTERS

NOTATION 2.1.

Let p, R, M, and F be as in Notation 1, and let G be a finite group. The set of all p-regular elements of G will be denoted by $\mathfrak{L}_p(G)$. When there is no confusion we set $\mathfrak{L}_p(G) = \mathfrak{L}(G) = \mathfrak{L}$. The algebra of all complex valued class functions on $\mathfrak{L}$ is denoted by $\mathrm{cf}_p(G)$. The collection of all Brauer characters of G defined by the F-representations of G will be denoted by $\mathrm{Br}_p(G)$ or $\mathrm{Br}(G)$, and the set of all irreducible Brauer characters will be denoted by $\mathrm{IBr}_p(G)$ or $\mathrm{IBr}(G)$. It is known that $\mathrm{IBr}(G)$ is a basis for $\mathrm{cf}_p(G)$.

NOTATION 2.2.

(1) Assume Notation 2.1. Let $\varphi_1, \varphi_2, \ldots, \varphi_k$ be some ordering of the elements of $\mathrm{IBr}(G)$; call this ordering α. For every $\theta \in \mathrm{cf}_p(G)$ let $M^\alpha(\theta) = \{m_{ij}^\alpha(\theta)\}$ be the $k \times k$ matrix whose entries are defined by the equations $\theta\varphi_i = \sum_{j=1}^{k} m_{ij}^\alpha(\theta)\varphi_j$. Then $M^\alpha(\theta)$ is a matrix with nonnegative integer entries for all $\theta \in \mathrm{Br}(G)$. If α is fixed, we write $M^\alpha(\theta) = M(\theta)$ and $m_{ij}^\alpha(\theta) = m_{ij}(\theta)$. We are using here the fact that a product of Brauer characters is a Brauer character.

(2) Let $\theta \in \mathrm{Br}(G)$, T be the F-representation affording θ, and V be the corresponding FG-module. The kernel of T (or the kernel of V) is defined to be the set of all elements of G which induce the identity map on V, i.e., $\operatorname{Ker} T = \operatorname{Ker} V = \{x \in G \mid vx = v \ \ \forall v \in V\}$. We define $Z(T)$ [or $Z(V)$] to be the set of all elements of G which induce a scalar map on V, i.e., $Z(T) = Z(V) = \{x \in G \mid vx = \lambda(x)v$ for some $\lambda(x) \in F$ and $\forall v \in V$, $\lambda(x)$ depending only on $x\}$. Let $\operatorname{Ker}(\theta) = \{x \in \mathfrak{L}(G) \mid \theta(x) = \theta(1)\}$ and $Z(\theta) = \{x \in \mathfrak{L}(G) \mid |\theta(x)| = \theta(1)\}$. We say that V is faithful if $\operatorname{Ker} V = 1$ and that V is superfaithful if $Z(V) = 1$.

LEMMA 2.3. *Let G be a finite group, p and F be as in Notation* 1, *$\theta \in Br(G)$, and V be the FG-module affording θ. Then*:

(1) $\operatorname{Ker}(\theta) = \operatorname{Ker} V \cap \mathfrak{L}(G)$.
(2) $Z(\theta) = Z(V) \cap \mathfrak{L}(G)$.
(3) *If V is faithful then $Z(\theta) \subseteq Z(G)$ ($Z(G)$ is the center of G).*

Proof. The proof is as in the characteristic zero case. Let $R, U, {}^*$ be as in Notation 1, and T the F-representation affording θ. Let $x \in Z(\theta)$. Denote by $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ the eigenvalues of $T(x)$ in F^*, and let $u_i \in U$ for $i = 1, 2, \ldots, m$ be such that $(u_i)^* = \epsilon_i$. Then $\theta(x) = \sum_{i=1}^m u_i$. Next, $m = |\sum_{i=1}^m u_i| \leqslant \sum_{i=1}^m |u_i| = m$, which implies that $u_i = u_j$ for all i, j; call their common value u. It follows that all the ϵ_i's are equal. Call their common value ϵ. Note that if $x \in \operatorname{Ker}(\theta)$, then $m = \theta(x) = mu$ implies that $u = 1$, so that $\epsilon = 1$.

Let B be the Jordan canonical form of $T(x)$ over the algebraically closed field F. Then $B = \epsilon I + A$, where I is the identity matrix and A a nilpotent matrix which has all its entries zero except possibly on the superdiagonal, where we may find ones. Let n be the order of x in G; then $(p, n) = 1$. Now, $I = B^n = \epsilon^n I + n\epsilon^{n-1}A + C$, where C has a zero entry in each place that A has a nonzero entry. It follows that $nA = 0$, and as $(p, n) = 1$, we get that $A = 0$. We conclude that $T(x)$ is similar over F to ϵI, so that x induces a scalar transformation on V. So $x \in Z(T)$, and if $x \in \operatorname{Ker}(\theta)$, then, as $\epsilon = 1$, we have $T(x) = I$, so that $x \in \operatorname{Ker} T$. Thus, $\operatorname{Ker}(\theta) \subseteq \operatorname{Ker} T \cap \mathfrak{L}(G)$ and $Z(\theta) \subseteq Z(T) \cap \mathfrak{L}(G)$. The reverse inclusions are trivial.

To prove part (3), let $x \in Z(\theta)$. Then $T(x)$ is a scalar matrix by the above. Hence $T(x) \in Z(T(G))$, and so $T(x)T(y) = T(y)T(x) \ \ \forall y \in G$. Thus, $T(x^{-1}y^{-1}xy) = I$. As T is faithful, $x^{-1}y^{-1}xy = 1 \ \forall y \in G$, so that $x \in Z(G)$. ∎

Remark. It is well known that $O_p(G) \subseteq \operatorname{Ker} V$ for any irreducible FG-module V. In fact $O_p(G)$ is the intersection of all such kernels.

Notation 2.4. Assume Notation 2.2. Let $\theta \in \mathrm{cf}_p(G)$.

(1) Write $\theta = \sum_{i=1}^{k} b_i \varphi_i$ with $b_i \in \mathbb{C}$, the complex number field. Define $\mathrm{IBr}(\theta) = \{\varphi_i \mid b_i \neq 0\}$. Namely, $\mathrm{IBr}(\theta)$ is the set of all irreducible constituents of θ.

(2) If there exists a natural number s such that $\mathrm{IBr}(\theta^s) = \mathrm{IBr}(G)$, we call the smallest such s the Brauer covering number of θ and denote it by $\mathrm{bcn}(\theta)$. If no such s exists, we say that $\mathrm{bcn}(\theta)$ is infinite.

(3) The value of θ on the p-regular conjugacy class C of G will be denoted by $\theta(C)$.

(4) Let $M(G) = \{M(\theta) \mid \theta \in \mathrm{cf}_p(G)\}$.

(5) Assume that $\theta \in \mathrm{Br}(G)$. Let

$$\mathscr{Z}(\theta) = \{C \mid C \text{ is a } p\text{-regular class of } G \text{ contained in } Z(\theta)\}.$$

Note that if θ is an ordinary faithful character, then $Z(\theta) = \mathscr{Z}(\theta)$, as in this case $Z(\theta)$ lies in the center of G. The same is true for $\theta \in \mathrm{Br}(G)$ for which the affording module is faithful (by Lemma 2.3). Note that for any $\theta \in \mathrm{Br}(G)$ we have that $Z(\theta) = 1$ if and only if $\mathscr{Z}(\theta) = 1$.

The next proposition shows how properties of Brauer characters θ correspond to properties of their nonnegative matrices $M(\theta)$.

In the following, $\mathrm{diag}(a_1, a_2, \ldots, a_k)$ is the diagonal matrix whose diagonal entries are the a_i's.

Proposition 2.5. *Let G be a finite group, p a prime, and $C_1 = \{1\}, C_2, \ldots, C_k$ the collection of all conjugacy classes of p'-elements of G. Let F be as in Notation 1, corresponding to which we set $\mathrm{IBr}(G) = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, with $\varphi_1 = 1$. Let $X = X(G) = (\varphi_i(C_j))$ be the Brauer character-table of G. Let $\theta \in \mathrm{Br}(G)$. Then:*

(1) *$X^{-1}M(\theta)X = \mathrm{diag}(\theta(C_1), \theta(C_2), \ldots, \theta(C_k))$. In particular, the values of θ are the eigenvalues of the nonnegative integer matrix $M(\theta)$.*

(2) *$\rho(M(\theta)) = \theta(1)$ and $M(\varphi_1) = I$, an identity matrix.*

(3) *$M(\theta) > 0$ if and only if $\mathrm{IBr}(\theta) = \mathrm{IBr}(G)$.*

(4) *$M(\theta)$ is irreducible if and only if $\mathrm{Ker}(\theta) = 1$. In this case the index of cyclicity of $M(\theta)$ is equal to $|\mathscr{Z}(\theta)|$.*

(5) *$M(\theta)$ is primitive if and only if $Z(\theta) = 1$. In this case $\mathrm{bcn}(\theta) = \gamma(M(\theta))$. Moreover, $\mathrm{bcn}(\theta) \leqslant k^2 - 2k + 2$. Also, $\mathrm{bcn}(\theta)$ is finite if and only if $Z(\theta) = 1$.*

(6) *The map $\theta \to M(\theta)$ is linear, additive, multiplicative, and injective on $\mathrm{cf}_p(G)$. The image $M(G)$ is a commutative algebra.*

REMARKS.

(1) Part (1) is true for any $\theta \in \mathrm{cf}_p(G)$.
(2) For more on $\mathrm{bcn}(\theta)$, see further in this section.

Proof of Proposition 2.5. Let A be the commutative algebra $\mathrm{cf}_p(G)$, and consider the following two bases of A: One is $\mathrm{IBr}(G) = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ with $\varphi_1 = 1$, and the other $\mathfrak{E} = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_k\}$, consisting of the characteristic functions. That is, $\epsilon_i(C_j) = \delta_{ij}$, $1 \leqslant i, j \leqslant k$.

For each $a \in A$, let $T_a : A \to A$ be the linear transformation defined by $T_a(b) = ab$ for all $b \in A$. By the definition, $[M(a)]^t$ is the representing matrix of T_a with respect to the basis $\mathrm{IBr}(G)$ (here ^{t} means transposed). Note that $\epsilon_i \epsilon_j = \delta_{ij}\epsilon_i$ and $a\epsilon_i = a(C_i)\epsilon_i$ for all $a \in A$ and $1 \leqslant i, j \leqslant k$. Hence each ϵ_i is a common eigenvector for all the T_a's, $a \in A$. Moreover, $a(C_i)$ is the eigenvalue of T_a corresponding to the eigenvector ϵ_i. Also, the matrix $D = \mathrm{diag}(a(C_1), a(C_2), \ldots, a(C_k))$ is the representing matrix of T_a with respect to the basis $\mathfrak{E}$.

Clearly $\varphi_i = \sum_{j=1}^{k} \varphi_i(C_j)\epsilon_j$, so that $X^t = (\varphi_i(C_j))^t$ is the transition matrix from $\mathfrak{E}$ to $\mathrm{IBr}(G)$. Consequently, $[M(a)]^t = (X^t)^{-1} D X^t$, so that $X^{-1}M(a)X = D$. Part (1) is now proved. Since all the matrices in $M(G)$ have simultaneous diagonalizations (via X), we get that the matrices in $M(G)$ commute.

The map $\theta \to M(\theta)$ is the composition of the following three algebra isomorphisms:

$$A \xrightarrow{f_1} \{T_a \mid a \in A\} \xrightarrow{f_2} M(G) \xrightarrow{f_3} M(G),$$

where the f_i's are defined as follows:

$$a \xrightarrow{f_1} T_a \xrightarrow{f_2} [M(a)]^t \xrightarrow{f_3} M(a)$$

[i.e., f_1 is the regular representation of A, and $f_2(T_a)$ is the matrix representation of T_a with respect to $\mathrm{IBr}(G)$]. Note that f_3 is multiplicative, as $M(G)$ consists of commuting matrices. This proves part (6).

For the rest of the proof let $\theta \in \mathrm{Br}(G)$. As $\theta(1) \geqslant |\theta(x)|$ for all $x \in \mathfrak{Q}(G)$ and as the values of θ are the eigenvalues of $M(\theta)$, we get that $\theta(1) = \rho(M(\theta))$. Clearly, $M(1) = I$, which proves part (2).

Next we prove part (3). If $M(\theta) > 0$ then $m_{1j}(\theta) > 0$ for $1 \leqslant j \leqslant k$. But $\theta = \theta\varphi_1 = \sum_{j=1}^{k} m_{1j}(\theta)\varphi_j$, so $\mathrm{IBr}(\theta) = \mathrm{IBr}(G)$. Conversely, assume that $\mathrm{IBr}(\theta) = \mathrm{IBr}(G)$; then $\theta = \sum_{i=1}^{k} a_i\varphi_i$, where the a_i's are positive integers. Fix an index u, $1 \leqslant u \leqslant k$. We need to show that $\mathrm{IBr}(\theta\varphi_u) = \mathrm{IBr}(G)$; this will show that $m_{ui}(\theta) > 0$ for all $1 \leqslant i, u \leqslant k$. Now, $\theta\varphi_u = \sum_{i=1}^{k} a_i\varphi_u\varphi_i$. Let $\Phi_1, \Phi_2, \ldots, \Phi_k$ be the principal indecomposable (projective) characters of G, considered as functions on $\mathfrak{L}(G)$ [outside $\mathfrak{L}(G)$ they vanish].

Suppose, by the way of contradiction, that $\varphi_v \notin \mathrm{IBr}(\theta\varphi_u)$ for some index v, $1 \leqslant v \leqslant k$. As $a_i > 0$ for all i, we get that $\varphi_v \notin \mathrm{IBr}(\varphi_u\varphi_i)$ for all $i = 1, 2, \ldots, k$. By [14, p. 145] we get that $\sum_{x \in \mathfrak{L}} \varphi_i(x)\varphi_u(x)\overline{\Phi_v(x)} = 0$ for all i. Let $\mu(x) = \overline{\varphi_u(x)}\Phi_v(x)$; then $\mu \in \mathrm{cf}_p(G)$ with $\sum_{x \in \mathfrak{L}} \varphi_i(x)\overline{\mu(x)} = 0$ for all $i = 1, 2, \ldots, k$. But μ is a linear combination of the φ_i's over $\mathbb{C}$, which implies that $\sum_{x \in \mathfrak{L}} \mu(x)\overline{\mu(x)} = 0$. Thus, $\mu(x) = 0$ $\forall x \in \mathfrak{L}$. In particular $\mu(1) = \varphi_u(1)\Phi_v(1) = 0$, a contradiction.

To prove part (4), assume first that $M(\theta)$ is irreducible. By Theorem 1.2(b), $\theta(1)$ is a simple root of the characteristic polynomial of $M(\theta)$, so that part (1) implies that $\mathrm{Ker}(\theta) = \{C \subseteq \mathfrak{L} \mid C$ a conjugacy class with $\theta(C) = \theta(1)\} = 1$. Conversely, assume that $\mathrm{Ker}(\theta) = 1$. Let m be the number of distinct values taken on by θ on $\mathfrak{L}$. By the Brauer-Burnside theorem (see Lemma 3.15, p. 148 of [14]) we know that $\mathrm{IBr}(1 + \theta + \theta^2 + \cdots + \theta^{m-1}) = \mathrm{IBr}(G)$. We note that the only assumption needed in the proof of Lemma 3.15 of [14] is that $\mathrm{Ker}(\theta) = 1$. By parts (2), (3), and (6) we obtain $I + M(\theta) + M(\theta)^2 + \cdots + M(\theta)^{m-1} = M(1 + \theta + \theta^2 + \cdots + \theta^{m-1}) > 0$. Now Proposition 1.1 implies that $M(\theta)$ is irreducible. The cyclicity index of $M(\theta)$, $c(M(\theta))$, is the number of eigenvalues of $M(\theta)$, $\theta(C_i)$, with $|\theta(C_i)| = \rho(M(\theta)) = \theta(1)$. So $c(M(\theta)) = |\{C_i \mid C_i \subseteq Z(\theta)\}| = |\mathscr{Z}(\theta)|$.

Finally, we prove part (5). If $M(\theta)$ is primitive, then by part (c) of Theorem 1.2 and our part (1), we get that $Z(\theta) = 1$. Conversely, assume that $Z(\theta) = 1$; then $\mathscr{Z}(\theta) = 1$ and $\mathrm{Ker}(\theta) = 1$. Hence, part (4) implies that $M(\theta)$ is irreducible with cyclicity index equal to $|\mathscr{Z}(\theta)| = 1$. By [5, p. 28] $M(\theta)$ is primitive.

Suppose now that $M(\theta)$ is primitive [namely that $Z(\theta) = 1$]. For a natural number n, the following statements are equivalent [by parts (3) and (6)]:

(i) $M(\theta)^n = M(\theta^n) > 0$,
(ii) $\mathrm{IBr}(\theta^n) = \mathrm{IBr}(G)$.

Thus $\mathrm{bcn}(\theta) = \gamma(M(\theta))$, the primitivity index of $M(\theta)$. The bound on $\mathrm{bcn}(\theta)$ follows from Theorem 4.14 on p. 48 of [5]. ■

Remark (Proposition 2.5 and ordinary characters). The above proposition holds for ordinary characters [replace the θ_i's by the ordinary characters,

hen $m_{1j}(\theta) > 0$ for $1 \leqslant j \leqslant k$. But
Br(G). Conversely, assume that
the a_i's are positive integers. Fix
that $\mathrm{IBr}(\theta\varphi_u) = \mathrm{IBr}(G)$; this will
k. Now, $\theta\varphi_u = \sum_{i=1}^{k} a_i \varphi_u \varphi_i$. Let
sable (projective) characters of G,
$\mathfrak{L}(G)$ they vanish].
hat $\varphi_c \notin \mathrm{IBr}(\theta\varphi_u)$ for some index
that $\varphi_c \notin \mathrm{IBr}(\varphi_u\varphi_i)$ for all $i =$
$\in \mathfrak{L}\, \varphi_i(x)\varphi_u(x)\overline{\Phi_c(x)} = 0$ for all i.
with $\sum_{x \in \mathfrak{L}} \varphi_i(x)\overline{\mu(x)} = 0$ for all
of the φ_i's over $\mathbb{C}$, which implies
$\forall x \in \mathfrak{L}$. In particular $\mu(1) =$

$M(\theta)$ is irreducible. By Theorem
ristic polynomial of $M(\theta)$, so that
a conjugacy class with $\theta(C) =$
$) = 1$. Let m be the number of
he Brauer-Burnside theorem (see
t $\mathrm{IBr}(1 + \theta + \theta^2 + \cdots + \theta^{m-1}) =$
n needed in the proof of Lemma
(3), and (6) we obtain $I + M(\theta) +$
$\cdots + \theta^{m-1}) > 0$. Now Proposi-
e. The cyclicity index of $M(\theta)$,
of $M(\theta)$, $\theta(C_i)$, with $|\theta(C_i)| =$
$\theta))| = |\mathscr{Z}(\theta)|$.
is primitive, then by part (c) of
$Z(\theta) = 1$. Conversely, assume that
ence, part (4) implies that $M(\theta)$ is
$|\mathscr{Z}(\theta)| = 1$. By [5, p. 28] $M(\theta)$ is

mely that $Z(\theta) = 1$]. For a natural
uivalent [by parts (3) and (6)]:

ex of $M(\theta)$. The bound on $\mathrm{bcn}(\theta)$
■

characters). The above proposi-
he θ_i's by the ordinary characters,

the C_i's by all the conjugacy classes, $\mathrm{IBr}(G)$ by $\mathrm{Irr}(G)$, $\mathrm{IBr}(\theta)$ by $\mathrm{Irr}(\theta)$, $\mathrm{Br}(G)$ by $\mathrm{Ch}(G)$, and $\mathrm{bcn}(\theta)$ by $\mathrm{ccn}(\theta)$, which is the smallest integer such that $\mathrm{Irr}(\theta^{\mathrm{ccn}(\theta)}) = \mathrm{Irr}(G)$]. See [6]. In the case of ordinary characters, the Brauer-Burnside theorem is not needed to show that $M(\theta)$, $\theta \in \mathrm{Ch}(G)$, is irreducible if and only if $\mathrm{Ker}(\theta) = 1$. For in this case $M(\theta) = [\theta\theta_i, \theta_j]$ where $\mathrm{Irr}(G) = \{\theta_1, \theta_2, \ldots, \theta_k\}$. Thus $M(\bar{\theta}) = M(\theta)'$, and so the first column of X, $(\theta_1(1), \theta_2(1), \ldots, \theta_k(1))'$, is a common eigenvector for both $M(\theta)$ and $M(\theta)^t$ corresponding to the eigenvalue $\theta(1)$. Then the irreducibility of $M(\theta)$ follows from Theorem 4.7, p. 18 of [16]. In fact, the Brauer-Burnside theorem can be shown to be a consequence of this irreducibility for ordinary characters (see [6] for more details). Also, in the case of ordinary characters $\mathrm{Ker}\, T = \mathrm{Ker}(\theta)$ and $Z(\theta) = Z(T)$.

Remark (Character covering numbers). In [3], the number $\mathrm{ccn}(G)$ was defined to be the smallest integer m such that $\mathrm{Irr}(\theta^m) = \mathrm{Irr}(G)$ for all $\theta \in \mathrm{Irr}(G) - \{1\}$. It was shown there (and in [6] using matrices) that this number exists if and only if G is a nonabelian simple group. The number was computed for many simple groups. We could analogously define the number $\mathrm{bcn}(G)$ to be the smallest integer m such that $\mathrm{IBr}(\theta^m) = \mathrm{IBr}(G)$ for all $\theta \in \mathrm{IBr}(G) - \{1\}$. By the previous results, clearly $\mathrm{bcn}(G)$ exists for any nonabelian simple group. In Table 1 we give some comparisons between $\mathrm{ccn}(G)$ and $\mathrm{bcn}(G)$ for a few simple groups. We note that the Janko smallest group, J_1, was characterized in [3] as the only finite group for which $\mathrm{ccn}(G) = 2$. In the case of $\mathrm{bcn}(J_1)$, the number is 2 for some primes and bigger for others; also $\mathrm{bcn}(A_5) = 2$ for one prime. It seems that the bound on $\mathrm{bcn}(\theta)$ given in Proposition 2.5 is much too big.

Notation 2.6. Let U and V be two modules. We write $U \mid V$ if U is isomorphic with a direct summand of V. If U and V are finitely generated,

TABLE 1

		bcn					
Group	ccn	$p=2$	3	5	7	11	19
A_5	3	5	3	2	—	—	—
A_6	3	3	4	3	—	—	—
A_7	4	4	3	3	4	—	—
$L(2,7)$	6	3	5	—	3	—	—
M_{11}	4	3	4	3	—	3	—
J_1	2	3	2	2	$\geqslant 3$	$\geqslant 3$	$\geqslant 3$

we write $U \leftrightarrow V$ if U and V have the same set of composition factors (with multiplicities). The Jacobson radical of a module W is denoted by $J(W)$.

The first part of the next theorem is a corollary of Proposition 2.5; the second part is due to Morton E. Harris. Recall that a superfaithful FG-module V is an FG-module such that each nonidentity element of G induces a nonscalar transformation on V.

Theorem 2.7. *Let p and F be as in Notation 1, and G a finite group. Let V be a superfaithful FG-module. Then there exist two positive integers k and l such that:*

(i) *Every irreducible FG-module is isomorphic to a composition factor of V^l. Moreover, $l \leqslant k^2 - 2k + 2$, where k is the number of p-regular classes of G.*

(ii) *Every principal indecomposable FG-module is isomorphic to a direct summand of V^k.*

Proof. Let θ be the Brauer character afforded by V. Our assumption implies that $Z(V) = 1$, so that $Z(\theta) = 1$ (by Lemma 2.3). Set $k = \mathrm{bcn}(\theta) < \infty$ (by Proposition 2.5). Thus, $\mathrm{IBr}(\theta^k) = \mathrm{IBr}(G)$. Write $\mathrm{IBr}(G) = \{\varphi_1, \varphi_2, \dots, \varphi_k\}$, and let V_i be the FG-module affording φ_i. Then $V_1, V_2, \dots, V_k$ is a complete set of representatives of isomorphism classes of irreducible FG-modules. As $\theta^k = \sum_{i=1}^k a_i \varphi_i$ with $a_i > 0\ \forall i$, we get that $V^k \leftrightarrow \bigoplus_{i=1}^k (a_i V_i)$ (see Lemma 3.5 on p. 146 of [14]). Now part (i) follows.

To prove part (ii), let Q be the projective cover of the trivial FG-module. As V is faithful, Theorem 1 on p. 45 of [1] implies that $Q \mid V^m$ for some nonnegative integer m. Let $l = m + k$, and A be an FG-module such that $V^m \cong Q \oplus A$.

Let L be any irreducible FG-module, and $P(L)$ its projective cover. We have to show that $P(L) \mid V^l$. As $V^k \leftrightarrow \bigoplus_{i=1}^k (a_i V_i)$, Lemma 2.7 on p. 99 of [14] (taking $T = 1$ and $U = Q$) implies that $Q \otimes V^k \cong \bigoplus_{i=1}^k a_i (Q \otimes V_i)$. Since L is isomorphic to one of the V_i's, we get that $Q \otimes L \mid Q \otimes V^k$. Let B be an FG-module such that $Q \otimes V^k \cong (Q \otimes L) \oplus B$, and set $C = A \otimes V^k$. Consequently

$$V^l \cong V^m \otimes V^k \cong (Q \oplus A) \otimes V^k \cong (Q \otimes V^k) \oplus C \cong (Q \otimes L) \oplus B \oplus C,$$

so that $Q \otimes L \mid V^l$. Therefore it suffices to show that $P(L) \mid Q \otimes L$.

First note that since Q is projective, $Q \otimes L$ is projective as well (see e.g. Lemma 4 of [1, p. 47]). Let $J = J(FG)$, and write $Q \otimes L = \bigoplus_{i=1}^s Q_i$, where the Q_i are projective indecomposable FG-modules. The radical of $Q\otimes L$ is $(Q\otimes L)J=\oplus_{i=1}^{s}Q_iJ$. It follows that

$$\frac{Q\otimes L}{(Q\otimes L)J}\cong\frac{\oplus_{i=1}^{s}Q_i}{\oplus_{i=1}^{s}Q_iJ}\cong\bigoplus_{i=1}^{s}W_i,\qquad \text{where } W_i\cong\frac{Q_i}{Q_iJ}\quad \text{for } i=1,2,\dots,s.$$

It follows that each of the W_i's is irreducible.

Now, as Q is the projective cover of 1_G, we get that

$$\frac{Q\otimes L}{(QJ)\otimes L}\cong\frac{Q}{QJ}\otimes L\cong 1_G\otimes L=L,$$

which is irreducible. But $(Q\otimes L)J$ is the smallest submodule of $Q\otimes L$ with a semisimple quotient; hence $(Q\otimes L)J\subseteq(QJ)\otimes L$. Finally,

$$L\cong\frac{Q\otimes L}{(QJ)\otimes L}\cong\frac{(Q\otimes L)/(Q\otimes L)J}{[(QJ)\otimes L]/(Q\otimes L)J}\cong\frac{\oplus_{i=1}^{s}W_i}{[(QJ)\otimes L]/(Q\otimes L)J}.$$

As both L and the W_i's are irreducible, we get that $L\cong W_j\cong Q_j/Q_jJ$ for some j and consequently $P(L)\cong Q_j\mid Q\otimes L$. ∎

The next five propositions are a long list of consequences of Proposition 2.5. The first four have the same assumption, namely:

Assumption $(*)$. Let G be a finite group, p a prime, and F the field as in Notation 1. Set $\mathrm{IBr}(G)=\{\varphi_1=1,\varphi_2,\dots,\varphi_k\}$, and let $C_1=\{1\},C_2,\dots,C_k$ be all the p-regular conjugacy classes of G. Let $\theta\in\mathrm{Br}(G)$ be such that $\mathrm{Ker}(\theta)=1$.

Remark. All the propositions below are valid for ordinary characters as well. All we have to do is replace in the assumptions and statements the field F by $\mathbb{C}$, $\mathrm{cf}_p(G)$ by $\mathrm{cf}(G)$, $\mathscr{Z}(\theta)$ by $Z(\theta)$, $\mathrm{Br}(G)$ by $\mathrm{ch}(G)$, $\mathrm{IBr}(G)$ by $\mathrm{Irr}(G)$, and the p-regular classes by all the conjugacy classes. The proofs remain the same.

We now list all the propositions; the proofs will follow.

Proposition 2.8. *Assume Assumption $(*)$. Then:*

(i) *For every $\psi\in\mathrm{IBr}(G)$ we have that* $|\mathscr{Z}(\theta)|=\gcd\{m\mid\psi\in\mathrm{IBr}(\psi\theta^m)\}$.

(ii) $|\mathscr{Z}(\theta)|=\gcd\{m\mid 1_G\in\mathrm{IBr}(\theta^m)\}$.

PROPOSITION 2.9. *Assume Assumption* $(*)$, *and suppose that one of the following holds*:

(i) $\varphi_i \in \mathrm{IBr}(\theta\varphi_i)$ *for some* i, *or*
(ii) $\varphi_i \in \mathrm{IBr}(\theta\varphi_j) \cap \mathrm{IBr}(\theta^2\varphi_j)$ *for some* i *and* j, *or*
(iii) $\varphi_i \in \mathrm{IBr}(\theta^q\varphi_j) \cap \mathrm{IBr}(\theta^{q+1}\varphi_j)$ *for some* i, j *and* q, *or*
(iv) $1_G \in \mathrm{IBr}(\theta^m) \cap \mathrm{IBr}(\theta^{m+1})$ *for some* m.

Then $Z(\theta) = 1$.

PROPOSITION 2.10. *Assume Assumption* $(*)$, *and set* $h = |\mathcal{Q}(\theta)|$. *Let* $s_1(\theta), s_2(\theta), \ldots, s_k(\theta)$ *be the elementary symmetric functions in the* $\theta(C_i)$'s, *namely*, $s_1(\theta) = \sum_{i=1}^{k}\theta(C_i)$, $s_2(\theta) = \sum_{i<j}\theta(C_i)\theta(C_j)$, $s_3(\theta) = \sum_{i<j<r}\theta(C_i)\theta(C_j)\theta(C_r), \ldots$, $s_k(\theta) = \prod_{i=1}^{k}\theta(C_i)$. *Then*:

(i) *For all* $i \leq k+1-h$, *at least* $h-1$ *of the following* h *integers are zero*:

$$s_i(\theta), s_{i+1}(\theta), \ldots, s_{i+h-1}(\theta).$$

(ii) *If* $h \neq 1$ *then* $s_i(\theta)s_{i-1}(\theta) = 0$ *for all* $i < k$.
(iii) *For each* $r \leq k$ *there exists a* j, $0 < j \leq k$, *such that* $\theta(C_r) = e^{2\pi i/h}\theta(C_j)$ (*where* $i = \sqrt{-1}$).
(iv) *The* h *elements of* $\{\theta(C_i) \mid C_i \subseteq Z(\theta)\}$ *are the distinct* h*th roots of* $\theta(1)^h$.

REMARK. The $s_i(\theta)$'s are always integers [even when $\mathrm{Ker}(\theta) \neq 1$], because they are the coefficients (up to a sign) of the characteristic polynomial of $M(\theta)$ [by part (1) of Proposition 2.5] which has integer entries. Also note that $\sum_{i=1}^{k}\theta(C_i)$ is a nonnegative integer, being equal to the trace of $M(\theta)$.

PROPOSITION 2.11. *Assume that Assumption* $(*)$ *holds and that* $h = |\mathcal{Q}(\theta)| > 1$. *Then there is a partition* $\mathrm{IBr}(G) = A_1 \cup A_2 \cup \cdots \cup A_h$ *into pairwise disjoint subsets* $A_1, A_2, \ldots, A_h$ *with the following properties*:

(i) *If* $\psi \in A_i$, *then*

$$\mathrm{IBr}(\theta\psi) \subseteq \begin{cases} A_{i+1} & \text{if} \quad i < h, \\ A_1 & \text{if} \quad i = h \end{cases} \quad \text{and} \quad \mathrm{IBr}(\theta^h\psi) \subseteq A_i.$$

(ii) *For every* $i = 1, 2, \ldots, h$, *there exists a positive integer* $m(i)$ *such that for every* $\psi \in A_i$ *we have that* $\mathrm{IBr}(\theta^{hm(i)}\psi) = A_i$.

m $(*)$, and suppose that one of the

ne i and j, or
some i, j and q, or
me m.

tion $(*)$, and set $h = |\mathcal{Z}(\theta)|$. Let
symmetric functions in the $\theta(C_i)$'s,
$) = \sum_{i<j} \theta(C_i)\theta(C_j)$, $s_3(\theta) =$
$_1 \theta(C_i)$. Then:

-1 of the following h integers are

$, s_{i+h-1}(\theta)$.

all $i < k$.
j, $0 < j \leqslant k$, such that $\theta(C_r) =$

$Z(\theta)\}$ are the distinct hth roots of

egers [even when $\mathrm{Ker}(\theta) \neq 1$], be-
gn) of the characteristic polynomial
vhich has integer entries. Also note
being equal to the trace of $M(\theta)$.

sumption $(*)$ holds and that $h =$
$G) = A_1 \cup A_2 \cup \cdots \cup A_h$ into pair-
he following properties:

and $\mathrm{IBr}(\theta^h\psi) \subseteq A_i$.

sts a positive integer $m(i)$ such that
$\psi) = A_i$.

(iii) *Set* $\mu = \min_i\{|A_i|\}$. *Then the number of* C_i*'s such that* $\theta(C_i) = 0$ *is at least* $k - h\mu$.

(iv) *Let* $z \in Z(\theta) - \{1\}$. *For every* $j = 1, 2, \ldots, k$ *set* $\varphi_j(z) = |\varphi_j(z)|e^{i\delta_j}$ (*where* $i = \sqrt{-1}$). *Then*

$$\left\{\delta_j \middle| 1 \leqslant j \leqslant k\right\} = \left\{\frac{2\pi}{h} j \middle| j = 0, 1, \ldots, h-1\right\}$$

and for $j = 0, 1, \ldots, h-1$ *we have that* $A_{j+1} = \{\psi \in \mathrm{IBr}(G) \mid \psi(z) = |\psi(z)|e^{i(2\pi j/h)}\}$.

(v) *If* $\theta(C_j) \neq 0$ *for all* $j = 1, 2, \ldots, k$, *then* $|A_j| = k/|\mathcal{Z}(\theta)|$ *for all* $j = 1, 2, \ldots, h$. *In particular* $|\mathcal{Z}(\theta)|$ *divides* k. *Furthermore, let* $z \in Z(\theta)$. *Then for all* $j = 0, 1, \ldots, h-1$, *the set* $\{\varphi_r(z) \mid 1 \leqslant r \leqslant k\}$ *has exactly* $k/|\mathcal{Z}(\theta)|$ *elements of argument* $2\pi j/|\mathcal{Z}(\theta)|$. *In particular, there are exactly* $k/|\mathcal{Z}(\theta)|$ *positive real (and, if* h *is even, exactly* $k/|\mathcal{Z}(\theta)|$ *negative real) elements in this set.*

Notation 2.12. Let $\theta \in \mathrm{Br}(G)$. Denote by $\mathbb{Q}(\theta)$ the smallest subfield of $\mathbb{C}$ containing the rationals, $\mathbb{Q}$, and $\{\theta(x) \mid x \in \mathfrak{L}_p(G)\}$. Let $\mathbb{Q}(G)$ be the smallest subfield of $\mathbb{C}$ containing $\bigcup\{\mathbb{Q}(\theta) \mid \theta \in \mathrm{IBr}(G)\}$.

Proposition 2.13. *Let* G *be a finite group,* p *a prime, and* F *as in Notation* 1. *Set* $k = |\mathrm{IBr}(G)|$, *and let* $\theta \in \mathrm{Br}(G)$.

(i) *Let* $\alpha_1, \alpha_2, \ldots, \alpha_s$ *be all the distinct values taken on by* θ *on* $\mathfrak{L}_p(G)$, *with* $\alpha_1 = \theta(1)$. *Then*

$$|\mathrm{Ker}(\theta)| \prod_{i=2}^{s} \theta(1)\left[\theta(1) - \alpha_i\right] \equiv 0 \pmod{|G|_{p'}},$$

and if $\alpha_i = 0$ *for some* i, *then*

$$|\mathrm{Ker}(\theta)| \prod_{i=2}^{s} \left[\theta(1) - \alpha_i\right] \equiv 0 \pmod{|G|_{p'}}.$$

(*Here* $|G|_{p'}$ *is the* p' *part of* $|G|$.)

(ii) *Assume that* θ *takes on exactly* k *values on* $\mathfrak{L}_p(G)$. *Then every Brauer character of* G *is a polynomial in* θ *with rational coefficients. In particular* $\mathbb{Q}(G) \subseteq \mathbb{Q}(\theta)$, *so that the Brauer character table is realized in* $\mathbb{Q}(\theta)$.

(iii) *Assume that* $\theta(1) > 1$. *Set* $\mathrm{IBr}(G) = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ *with* $\varphi_1 = 1_G$. *Let* η *be one of the* φ_i*'s. Then* $\eta(1)$ *does not divide at least* $\log_{\theta(1)} \eta(1)$ *of the* $\varphi_j(1)$*'s.*

Proof of Propositions 2.8 and 2.9. For each $\eta \in \mathrm{IBr}(G)$, let $G(M(\eta))$ be the directed graph with k vertices $P_1, P_2, \ldots, P_k$ with an edge leading from P_i to P_j if and only if $m_{ij}(\eta) \neq 0$. In fact the vertices can be labeled by $\varphi_1, \varphi_2, \ldots, \varphi_k$, where an edge leads from φ_i to φ_j if and only if $\varphi_j \in \mathrm{IBr}(\eta\varphi_i)$ [i.e. $m_{ij}(\varphi) \neq 0$].

Let θ be our given Brauer character, and $\psi \in \mathrm{IBr}(G)$. As $\mathrm{Ker}(\theta) = 1$, we know that $M(\theta)$ is irreducible with cyclicity index $|\mathscr{P}(\theta)|$ [Proposition 2.5(4)]. Now, a circuit of length m through ψ exists in $G(M(\theta))$ if and only if a loop (i.e. a circuit of length 1) exists through ψ in the graph $G([M(\theta)]^m) = G(M(\theta^m))$ [recall that $\theta \to M(\theta)$ is multiplicative]. We have used here Corollary 3.1 on p. 78 of [16]. Now, a loop through ψ exists in $G(M(\theta^m))$ if and only if $\psi \in \mathrm{IBr}(\psi\theta^m)$. We now use Theorem (2.30) on p. 34 of [5] to conclude that

$$|\mathscr{P}(\theta)| = \gcd\{m \mid \text{there is a loop in } G(M(\theta^m)) \text{ through } \psi\}$$

$$= \gcd\{m \mid \psi \in \mathrm{IBr}(\psi\theta^m)\}.$$

This proves Proposition 2.8(i). Part (ii) is a special case of part (i).

Part (i) of Proposition 2.9 implies that trace $M(\theta) > 0$, Part (iii) implies that $m_{ji}^{(q)}(\theta) m_{ji}^{(q+1)}(\theta) > 0$. Each of these implies that $M(\theta)$ is primitive (see Corollary 2.28 on p. 34 and Problem 6.20 on p. 55 of [5]), which in turn implies that $|Z(\theta)| = 1$. Finally, part (ii) is a special case of part (iii), and part (iv) follows from part (ii) of Proposition 2.8. ∎

Proof of Proposition 2.10. For $h = 1$ the proposition is trivial, so we may assume that $h > 1$. Since $\mathrm{Ker}(\theta) = 1$, we conclude that $M(\theta)$ is irreducible but not primitive. The index of cyclicity of $M(\theta)$ is h [by Proposition 2.5(4)]. For $i = 1, 2, \ldots, k$, $s_i(\theta)$ is, up to sign, the coefficient of x^{k-i} in the characteristic polynomial $p_\theta(x)$ of $M(\theta)$ (here k is the number of p-regular classes of G). Let x^{m_1} and x^{m_2} be two consecutive powers of x in $p_\theta(x)$ with nonzero coefficients. Theorem 2.27 on p. 34 of [5] implies that h divides $m_1 - m_2$. So $m_1 - m_2 \geqslant h$ and part (i) follows. Part (ii) follows from part (I). Parts (iii) and (iv) follow from Theorems 1.1 and 1.2 on pp. 47 and 48 of [16] and our Proposition 2.5. ∎

$= \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ *with* $\varphi_1 = 1_G$. *Let*
t divide at least $\log_{\theta(1)} \eta(1)$ *of the*

r each $\eta \in \mathrm{IBr}(G)$, let $G(M(\eta))$ be
$, \ldots, P_k$ with an edge leading from
ict the vertices can be labeled by
φ_i to φ_j if and only if $\varphi_j \in \mathrm{IBr}(\eta\varphi_i)$

and $\psi \in \mathrm{IBr}(G)$. As $\mathrm{Ker}(\theta) = 1$, we
ty index $|\mathscr{Z}(\theta)|$ [Proposition 2.5(4)].
its in $G(M(\theta))$ if and only if a loop
h ψ in the graph $G([M(\theta)]^m) =$
ltiplicative]. We have used here
p through ψ exists in $G(M(\theta^m))$ if
Theorem (2.30) on p. 34 of [5] to

n $G(M(\theta^m))$ through $\psi\}$

a special case of part (i).
t trace $M(\theta) > 0$, Part (iii) implies
mplies that $M(\theta)$ is primitive (see
:0 on p. 55 of [5]), which in turn
a special case of part (iii), and part
■

he proposition is trivial, so we may
conclude that $M(\theta)$ is irreducible
$M(\theta)$ is h [by Proposition 2.5(4)].
oefficient of x^{k-i} in the character-
the number of p-regular classes of
powers of x in $p_\theta(x)$ with nonzero
mplies that h divides $m_1 - m_2$. So
ollows from part (I). Parts (iii) and
n pp. 47 and 48 of [16] and our
■

Proof of Proposition 2.11. Note that if Q is a $k \times k$ permutation matrix, then Q is a transition matrix from one ordering, α, of $\mathrm{IBr}(G)$ to another ordering, β. In fact, if α is the ordering $\varphi_1, \varphi_2, \ldots, \varphi_k$ and σ is the permutation corresponding to Q, then β is the ordering $\varphi_{\sigma(1)}, \varphi_{\sigma(2)}, \ldots, \varphi_{\sigma(k)}$. It follows that $QM^\alpha(\eta)Q^t = M^\beta(\eta)$ for all $\eta \in \mathrm{cf}_p(G)$.

Let α be the given ordering of $\mathrm{IBr}(G)$. Set $M(\eta) = M^\alpha(\eta)$ for all $\eta \in \mathrm{cf}_p(G)$. As $\mathrm{Ker}(\theta) = 1$, we know that $M(\theta)$ is irreducible with cyclicity index $h > 1$. Let $X = (\varphi_i(C_j))$. By Proposition 2.5, $M(\theta)X = X\,\mathrm{diag}(\theta(C_1), \theta(C_2), \ldots, \theta(C_k))$.

Let $z \in Z(\theta) - \{1\}$; then $z \in C_r \in \mathscr{Z}(\theta)$ for some r. Set $v = (\varphi_1(C_r), \varphi_2(C_r), \ldots, \varphi_k(C_r))^t$. Then $M(\theta)v = \theta(C_r)v$, so that v is an eigenvector of $M(\theta)$ corresponding to the eigenvalue $\theta(C_r)$. By Theorem 1.2, $\theta(C_r)$ is a simple root of the characteristic polynomial of $M(\theta)$, and so every eigenvector corresponding to $\theta(C_r)$ is of the form λv for some $\lambda \in \mathbb{C}$. Write $\varphi_j(C_r) = |\varphi_j(C_r)|e^{i\delta_j}$, $1 \leqslant j \leqslant k$. Note that $\varphi_1(C_r) = 1$, so that we can take the matrix $D = \mathrm{diag}(e^{i\delta_1}, e^{i\delta_2}, \ldots, e^{i\delta_k})$ as the matrix D of the proof of Theorem (2.20) on p. 32 of [5] (this D goes back to the proof of Theorem 2.14 on p. 31 of [5]); note that n_0 of the proof of Theorem 2.20 of [5] should be 0, and not positive as written mistakenly there).

By the proof of Theorem 2.20(c) on p. 33 of [5] we get that $\{\delta_j \mid 1 \leqslant j \leqslant k\} = \{(2\pi/h)j \mid j = 0, 1, \ldots, h-1\}$. Let $A_{j+1} = \{\psi \in \mathrm{IBr}(G) \mid \psi(z) = |\psi(z)|e^{i(2\pi j/h)}\}$ for $j = 0, 1, \ldots, h-1$. We now rename the elements of A_t as follows: $A_t = \{\varphi_{t,1}, \varphi_{t,2}, \ldots, \varphi_{t,m_t}\}$ for all $t = 1, 2, \ldots, h$. Clearly, $\mathrm{IBr}(G) = \bigcup_{i=1}^{h} A_i$. Let P be the permutation matrix corresponding to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & k \\ 1,1 & 1,2 & 1,3 & \cdots & 1,m_1 & 2,1 & 2,2 & \cdots & 2,m_2 & 3,1 & \cdots & h,m_h \end{pmatrix}.$$

Again, the proof of Theorem 2.20(c) of [5] shows that

$$PM(\theta)P^t = \begin{pmatrix} 0_1 & M_{12} & 0 & \cdots & 0 \\ 0 & 0_2 & M_{23} & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0_{h-1} & M_{h-1,h} \\ M_{h1} & 0 & \cdots & 0 & 0_h \end{pmatrix} = M^\beta(\theta)$$

for some ordering β of $\mathrm{IBr}(G)$, where each 0_j is a square zero matrix whose order is $|A_j|$, and $M_{12}, M_{23}, \ldots, M_{h-1,h}, M_{1h}$ are nonnegative matrices. The definition of $M^\beta(\theta)$ now implies that the first parts of part (i) and part (iv) hold. Part (iii) is a consequence of Theorem 4.4 on p. 60 of [16]. By Problem

6.10 on p. 54 of [5] we get that $M^{\beta}(\theta^{h}) = [M^{\beta}(\theta)]^{h} = \mathrm{diag}(N_1, N_2, \ldots, N_h)$, where each N_i is a primitive square matrix. Let $m(j)$ be the primitivity index of N_j; then $N_j^{m(j)} > 0$. Now the second statement of (i) and all of (ii) follow from the definitions of $M^{\beta}(\theta^{h})$ and $M^{\beta}(\theta^{hm(j)})$ respectively. Part (v) follows from the previous parts and Corollary 4.2 on p. 61 of [16]. ■

Proof of Proposition 2.13. By Proposition 2.5(1), the characteristic polynomial of $M(\theta)$ is $f(x) = \prod_{i=1}^{k}[x - \theta(C_i)]$, where the C_i's are the p-regular classes of G. If $\theta(C_i) \neq \theta(C_j)$ for all i and j, then $f(x)$ is also the minimal polynomial of $M(\theta)$. By [11, p. 232] every matrix over the rational number field, $\mathbb{Q}$, that commutes with $M(\theta)$ is a polynomial in $M(\theta)$ with coefficients in $\mathbb{Q}$. Let $\psi \in \mathrm{Br}(G)$. By Proposition 2.5(6) we know that $M(\psi)$ commutes with $M(\theta)$, so that $M(\psi) = \sum_{i=1}^{n} a_i [M(\theta)]^{i}$, with $a_i \in \mathbb{Q}$ and n a positive integer. Part (6) of Proposition 25 now implies that $\psi = \sum_{i=1}^{n} a_i \theta^{i}$. This proves (ii).

To prove part (iii), consider the group $\overline{G} = G/\mathrm{Ker}\,V$, where V is the module affording θ. Then $\theta \in \mathrm{Br}(\overline{G}) \subseteq \mathrm{Br}(G)$. As $\mathrm{Ker}(\theta) = 1$ on $\overline{G}$, we get that $M(\theta)$ is irreducible on $\overline{G}$. The leading eigenvalue of $M(\theta)$ is $\theta(1)$, and $(\varphi_1(1), \varphi_2(1), \ldots, \varphi_u(1))^{t}$, [where $\mathrm{IBr}(\overline{G}) = \{\varphi_1 = 1, \varphi_2, \ldots, \varphi_u\} \subseteq \mathrm{IBr}(G)$] is an eigenvector corresponding to $\theta(1)$ (by Proposition 2.5). Now part (iii) follows from a result of Ashley [4].

We now prove part (i). Let

$$\bar{\theta}(x) = \begin{cases} |G|_p \theta(x) & \text{if } x \text{ is a } p'\text{-element}, \\ 0 & \text{if } x \text{ is } p\text{-singular}. \end{cases}$$

It is well known that $\bar{\theta}$ is a generalized character of G (see for example Problem 15.3 on p. 285 of [15], which clearly holds for any $\theta \in \mathrm{Br}(G)$). If $(|G|, p) = 1$, then θ is an ordinary character of G and the result follows from [7]. Thus we may assume that p divides $|G|$, so that the distinct values of $\bar{\theta}$ are either $|G|_p\alpha_1, |G|_p\alpha_2, \ldots, |G|_p\alpha_s$ (if one of the α_i's is zero) or $|G|_p\alpha_1, |G|_p\alpha_2, \ldots, |G|_p\alpha_s, 0$ (if $\alpha_i \neq 0$ for all i). We now use Corollary 3 of [7] (this corollary assumes that the θ there is a character, but the same proof holds for generalized characters). Note that $\bar{\theta}(1) = \theta(1)|G|_p$, so that $\mathrm{Ker}(\theta) = \mathrm{Ker}(\bar{\theta}) = \{x \in G \mid \bar{\theta}(x) = \bar{\theta}(1)\}$. Therefore, either

$$|\mathrm{Ker}(\theta)| \prod_{i=2}^{s} \left[\bar{\theta}(1) - |G|_p\alpha_i\right] \equiv 0 \pmod{|G|} \qquad \text{if some } \alpha_i \text{ is zero},$$

$=[M^{\beta}(\theta)]^h = \mathrm{diag}(N_1, N_2, \ldots, N_h)$,
trix. Let $m(j)$ be the primitivity
ond statement of (i) and all of (ii)
$M^{\beta}(\theta^{h\,m(j)})$ respectively. Part (v)
ry 4.2 on p. 61 of [16]. ∎

ion 2.5(1), the characteristic poly-
. where the C_i's are the p-regular
l j, then $f(x)$ is also the minimal
matrix over the rational number
ynomial in $M(\theta)$ with coefficients
5) we know that $M(\psi)$ commutes
$]^i$, with $a_i \in \mathbb{Q}$ and n a positive
implies that $\psi = \sum_{i=1}^{n} a_i\theta^i$. This

p $\overline{G} = G/\mathrm{Ker}\,V$, where V is the
(G). As $\mathrm{Ker}(\theta) = 1$ on $\overline{G}$, we get
g eigenvalue of $M(\theta)$ is $\theta(1)$, and
$\varphi_1 = 1, \varphi_2, \ldots, \varphi_u\} \subseteq \mathrm{IBr}(G)]$ is an
osition 2.5). Now part (iii) follows

is a p'-element,
is p-singular.

character of G (see for example
arly holds for any $\theta \in \mathrm{Br}(G)$). If
of G and the result follows from
$G|$, so that the distinct values of $\bar{\theta}$
one of the α_i's is zero) or
ll i). We now use Corollary 3 of
is a character, but the same proof
$\bar{\theta}(1) = \theta(1)|G|_p$, so that $\mathrm{Ker}(\theta) =$
ither

d $|G|$) if some α_i is zero,

or

$$|\mathrm{Ker}(\theta)|\prod_{i=2}^{s}\left[\bar{\theta}(1) - |G|_p\alpha_i\right]\left[\bar{\theta}(1) - 0\right] \equiv 0 \pmod{|G|} \qquad \text{if no } \alpha_i \text{ is zero.}$$

Consequently,

$$|\mathrm{Ker}(\theta)|(|G|_p)^{s-1}\prod_{i=2}^{s}\left[\theta(1) - \alpha_i\right] \equiv 0 \pmod{|G|}$$

in the first case, and

$$|\mathrm{Ker}(\theta)|(|G|_p)^{s}\prod_{i=2}^{s}\left[\theta(1) - \alpha_i\right]\theta(1) \equiv 0 \pmod{|G|}$$

in the second case. Now the result follows. ∎

III. NORMAL SUBSETS AND NONNEGATIVE MATRICES

We start with definitions and notation analogous to the ones in Section II.

NOTATION 3.1. Let G be a finite group.

(1) Let $\alpha: C_1, C_2, \ldots, C_k$ be an ordering of the conjugacy classes of G. Let $\mathrm{Con}(G) = \{C_1, C_2, \ldots, C_k\}$.

(2) If A is a normal subset of G, we define $\mathrm{Con}(A) = \{C \in \mathrm{Con}(G) \mid C \subseteq A\}$. Clearly $A = \bigcup\{C \mid C \in \mathrm{Con}(A)\}$.

(3) If A is a normal subset of G, we denote by $\hat{A}$ the sum of the elements of A in the group algebra $\mathbb{C}G$; that is, $\hat{A} = \sum_{a \in A} a$. Clearly, $\hat{A} = \sum_{C \in \mathrm{Con}(A)} \hat{C}$.

(4) We define a matrix $M^{\alpha}(A) = (m_{ij}^{\alpha}(A))$ by $\hat{A}\hat{C} = \sum_{j=1}^{k} m_{ij}^{\alpha}(A)\hat{C}_j$. We use here the fact that $\hat{A} \in Z(\mathbb{C}G)$ and that the $\hat{C}_j$'s form a basis of $Z(\mathbb{C}G)$. If the ordering α is fixed, we set $M^{\alpha}(A) = M(A)$ and $m_{ij}^{\alpha}(A) = m_{ij}(A)$.

(5) If A is a normal subset of G, we denote $A^{-1} = \bigcup\{C^{-1} \mid C \in \mathrm{Con}(A)\}$. Here C^{-1} is the conjugacy class consisting of the inverses of the elements of C.

(6) Let $\mathrm{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$ be the set of all ordinary irreducible characters of G, and as usual denote by $\theta(C)$ the value of the character θ on the conjugacy class C. We define $\mathrm{Ker}(\theta)$ and $Z(\theta)$ for a character θ as in

Notation 2.2. Here $\mathrm{Ker}(\theta)$ and $Z(\theta)$ are both normal subgroups of G. The central character corresponding to $\chi \in \mathrm{Irr}(G)$ is denoted by ω_χ. That is, $\omega_\chi(C) = |C|\chi(C)/\chi(1)$ for all $C \in \mathrm{Con}(G)$. If A is a normal subset of G, we write $\omega_\chi(A) = \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C)$ for all $\chi \in \mathrm{Irr}(G)$.

(7) Let A and B be two subsets of G. Set $AB = \{ab \mid a \in A,\, b \in B\}$. This extends to products of any finite number of subsets. Note that if A and B are normal subsets, then $AB = BA$.

(8) Let A be a normal subset of G. If there exists a natural number m such that $A^m = G$, we call the least such m the covering number of A and denote it by $\mathrm{cn}(A)$. If no such m exists, we say that $\mathrm{cn}(A)$ is infinite.

(9) Let $M = (m_{ij})$ and $N = (n_{ij})$ be two square matrices of the same size over some field. We say that M and N are equivalent (denoted by $N \approx N$) if for all (i, j) we have that $m_{ij} = 0$ if and only if $n_{ij} = 0$. Clearly, $\approx$ is an equivalence relation.

The first lemma contains some well-known and some obvious consequences of these definitions.

LEMMA 3.2. *Let G be a finite group, A a normal subset of G, and α a fixed ordering of* $\mathrm{Con}(G)$. *Then*:

(1) $m_{ij}^\alpha(A) = \sum_{C \in \mathrm{Con}(A)} m_{ij}^\alpha(C)$ *and* $M^\alpha(A) = \sum_{C \in \mathrm{Con}(A)} M^\alpha(C)$.

(2) $M^\alpha(A)$ *is a nonnegative matrix with integer entries which can be computed from the character table of* G.

(3) $m_{ij}^\alpha(A) \neq 0$ *if and only if each element of C_j can be written as a product uv with $u \in A$ and $v \in C_i$.*

(4) $m_{ij}^\alpha(A) \neq 0$ *if and only if* $C_j \subseteq AC_i$.

(5) *Let* $\chi \in \mathrm{Irr}(G)$. *If* $|\omega_\chi(A)| = |A|$ *then* $A \subseteq Z(\chi)$.

(6) *Let* $\chi \in \mathrm{Irr}(G)$. *If* $\omega_\chi(A) = |A|$ *then* $A \subseteq \mathrm{Ker}(\chi)$.

Proof. (1): Recall that

$$\sum_{j=1}^{k} m_{ij}^\alpha(A)\hat{C}_j = \hat{A}\hat{C}_i = \sum_{C \in \mathrm{Con}(A)} \hat{C}\hat{C}_i = \sum_{C \in \mathrm{Con}(A)} \sum_{j=1}^{k} m_{ij}^\alpha(C)\hat{C}_j$$

$$= \sum_{j=1}^{k} \sum_{C \in \mathrm{Con}(A)} m_{ij}^\alpha(C)\hat{C}_j,$$

so that part (1) follows.

(2) It is well known that $m_{ij}^\alpha(C)$ is a nonnegative integer that can be computed from the character table of G for all conjugacy classes C (see [15,

oth normal subgroups of G. The
(G) is denoted by ω_χ. That is,
If A is a normal subset of G, we
$\mathrm{Irr}(G)$.
et $AB = \{ab \mid a \in A, b \in B\}$. This
subsets. Note that if A and B are

there exists a natural number m
the covering number of A and
say that $\mathrm{cn}(A)$ is infinite.
square matrices of the same size
equivalent (denoted by $N \approx N$) if
nly if $n_{ij} = 0$. Clearly, $\approx$ is an

nown and some obvious conse-

A a normal subset of G, and α a

$(A) = \Sigma_{C \in \mathrm{Con}(A)} M^\alpha(C)$.
ith integer entries which can be

ment of C_j can be written as a

n $A \subseteq Z(\chi)$.
$A \subseteq \mathrm{Ker}(\chi)$.

$$_i = \sum_{C \in \mathrm{Con}(A)} \sum_{j=1}^{k} m_{ij}^\alpha(C)\hat{C}_j$$

$$C)\hat{C}_j,$$

nonnegative integer that can be
r all conjugacy classes C (see [15,

pp. 15, 45]). By part (1) we get that the same is true for $m_{ij}^\alpha(A)$, so that part (2) holds.

Parts (3) and (4): If $A = C \in \mathrm{Con}(G)$, then part (3) is well known (see the proof of Theorem 2.4 of [15]). For a general A, assume that $m_{ij}(A) \neq 0$. Part (1) implies that $m_{ij}(C) \neq 0$ for some $C \in \mathrm{Con}(A)$. Hence each element of C_j can be written as a product uv with $u \in C \subseteq A$ and $v \in C_i$, as needed. Conversely, if an element $b \in C_j$ can be written as a product $b = uv$ with $u \in A$ and $v \in C_i$, then $u \in C$ for some $C \in \mathrm{Con}(A)$, so that $m_{ij}(C) \neq 0$. Part (1) implies now that $m_{ij}(A) \neq 0$. So part (3) is proved. Part (4) is a restatement of part (3).

(5): Assume that $|\omega_\chi(A)| = |A|$. Then

$$|A| = \sum_{C \in \mathrm{Con}(A)} |C| = \left| \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C) \right| \leqslant \sum_{C \in \mathrm{Con}(A)} |\omega_\chi(C)| \leqslant \sum_{C \in \mathrm{Con}(A)} |C| = |A|, \qquad (*)$$

so that the two inequalities are in fact equalities. As $|\omega_\chi(C)| \leqslant |C|$ for all $C \in \mathrm{Con}(G)$ [this fact was used in $(*)$], we get that $|\omega_\chi(C)| = |C|$ $\forall C \in \mathrm{Con}(A)$. This implies that $\chi(1) = |\chi(C)|$ $\forall C \in \mathrm{Con}(A)$. Hence $C \subseteq Z(\chi)$ $\forall C \in \mathrm{Con}(A)$, which implies that $A \subseteq Z(\chi)$.

(6): Assume that $\omega_\chi(A) = |A|$. Then

$$|A| = \sum_{C \in \mathrm{Con}(A)} |C| = \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C) = \left| \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C) \right| \leqslant \sum_{C \in \mathrm{Con}(A)} |\omega_\chi(C)| \leqslant \sum_{C \in \mathrm{Con}(A)} |C| = |A|. \qquad (**)$$

As above, this implies that $|\omega_\chi(C)| = |C|$ for all $C \in \mathrm{Con}(A)$ and that $(**)$ is an equality throughout. But then the arguments of the $\omega_\chi(C)$'s are all the same. Call the common value of the arguments β, $0 \leqslant \beta < 2\pi$. Then

$$|A| = \sum_{C \in \mathrm{Con}(A)} |C| = \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C) = e^{i\beta} \sum_{C \in \mathrm{Con}(A)} |\omega_\chi(C)|$$

is a real number, forcing $\beta = 0$. Thus for each $C \in \mathrm{Con}(A)$ we have that $|C| = |\omega_\chi(C)| = \omega_\chi(C)$, which implies that $C \subseteq \mathrm{Ker}(\chi)$. Consequently, $A \subseteq \mathrm{Ker}(\chi)$. ∎

Now come the two propositions that relate properties of A to those of $M(A)$. These are the normal subset analogs of Proposition 2.5. We first state both and then prove them.

PROPOSITION 3.3. *Let G be a finite group, $C_1, C_2, \ldots, C_k$ a fixed ordering of the conjugacy classes of G, and $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \ldots, \chi_k\}$, where $C_1 = \{1\}$ and $\chi_1 = 1_G$. Let $Y = Y(G)$ be the matrix $Y = \left(\omega_{\chi_i}(C_j)\right)^t$. Let A be a normal subset of G. Then:*

(1) $Y^{-1}M(A)Y = \mathrm{diag}(\omega_{\chi_1}(A), \omega_{\chi_2}(A), \ldots, \omega_{\chi_k}(A))$. *In particular, the $\omega_{\chi_i}(A)$'s are the eigenvalues of the nonnegative integer matrix $M(A)$.*

(2) $\rho(M(A)) = |A|$ *and* $M(C_1) = I$, *an identity matrix.*

(3) $[M(A)]^t = \left(m_{ij}(A^{-1})|C_j|/|C_i|\right)$.

(4) *If A_1 and A_2 are two normal subsets of G, then $M(A_1 \cup A_2) = M(A_1) + M(A_2)$ and $M(A_1A_2) = M(A_1)M(A_2)$. Moreover, $M(A_1)M(A_2) = M(A_2)M(A_1)$.*

(5) $M(A) > 0$ *if and only if* $A = G$.

In the next proposition X' is the commutator subgroup of the group X, and $\langle L \rangle$ is the group generated by the set L.

PROPOSITION 3.4. *Let G be a finite group, A a normal subset of G, and C a conjugacy class of G. Fix an ordering of $\mathrm{Con}(G)$ with respect to which $M(A)$ and $M(C)$ are computed. Then:*

(1) *$M(A)$ is irreducible if and only if A generates G. In this case the index of cyclicity of $M(A)$ is equal to $|G : \langle AA^{-1} \rangle| \leqslant |G : G'|$.*

(2) *$M(C)$ is irreducible if and only if C generates G. In this case the index of cyclicity of $M(C)$ is equal to $|G : G'|$.*

(3) *$M(A)$ is primitive if and only if $G = \langle A \rangle = \langle AA^{-1} \rangle$ (in particular this happens if $G = G' = \langle A \rangle$). In this case $\mathrm{cn}(A) = \gamma(M(A)) \leqslant k^2 - 2k + 2$, where $k = |\mathrm{Con}(G)|$.*

(4) *$M(C)$ is primitive if and only if G is a perfect group generated by C. In this case $\mathrm{cn}(C) = \gamma(M(C)) \leqslant k^2 - 2k + 2$, where $k = |\mathrm{Con}(G)|$. Also, $\mathrm{cn}(C)$ is finite if and only if $M(C)$ is primitive.*

REMARK. The bound in part (4) of Proposition 3.4 is known. A different proof and better bounds (not using matrices) can be found on p. 37 of [2] (see also p. 17 of [2]).

late properties of A to those of
of Proposition 2.5. We first state

p, $C_1, C_2, \ldots, C_k$ a fixed ordering
$= \{\chi_1, \chi_2, \ldots, \chi_k\}$, where $C_1 = \{1\}$
$= \left(\omega_{\chi_i}(C_j)\right)^t$. Let A be a normal

$\ldots, \omega_{\chi_k}(A))$. In particular, the
ve integer matrix $M(A)$.
entity matrix.

isets of G, then $M(A_1 \cup A_2) =$
$A_2)$. Moreover, $M(A_1)M(A_2) =$

utator subgroup of the group X,
L.

o, A a normal subset of G, and C
Con(G) with respect to which

A generates G. In this case the
$A^{-1}\rangle| \leqslant |G:G'|$.
C generates G. In this case the
|.
$= \langle A \rangle = \langle AA^{-1} \rangle$ (in particular
$\mathrm{cn}(A) = \gamma(M(A)) \leqslant k^2 - 2k + 2$,

a perfect group generated by C.
where $k = |\mathrm{Con}(G)|$. Also, $\mathrm{cn}(C)$

osition 3.4 is known. A different
can be found on p. 37 of [2] (see

Proof of Proposition 3.3. (1): Let $C_\alpha \in \mathrm{Con}(G)$, and for each $m = 1, 2, \ldots, k$ set $\omega_m = (\omega_{\chi_m}(C_1), \omega_{\chi_m}(C_2), \ldots, \omega_{\chi_m}(C_k))^t$. The shortest way to see the well-known part (1) is to quote the last three lines of p. 218 of [10], from which get that ω_m is an eigenvector of $M(C_\alpha)$ corresponding to the eigenvalue $\omega_{\chi_m}(C_\alpha)$. Since the columns of Y are $\omega_1, \omega_2, \ldots, \omega_m$, each column of Y is a common eigenvector of all the matrices $M(C_\alpha)$ for $\alpha = 1, 2, \ldots, k$. Let $X = (\chi_i(C_j))$ be the character table of G. Then it is well known that X is nonsingular. But

$$Y = \mathrm{diag}(|C_1|, |C_2|, \ldots, |C_k|)\, X^t\, \mathrm{diag}\left(\chi_1(1)^{-1}, \chi_2(1)^{-1}, \ldots, \chi_k(1)^{-1}\right),$$

so that Y is also nonsingular. Now part (1) follows for $A = C$ a conjugacy class.

For a general A we use Lemma 3.2 and part (1) for C_α to get that

$$\begin{aligned} Y^{-1}M(A)Y &= \sum_{C_\alpha \in \mathrm{Con}(A)} Y^{-1}M(C_\alpha)Y \\ &= \mathrm{diag}\left(\sum_{C_\alpha \in \mathrm{Con}(A)} \omega_{\chi_1}(C_\alpha), \sum_{C_\alpha \in \mathrm{Con}(A)} \omega_{\chi_2}(C_\alpha), \ldots, \sum_{C_\alpha \in \mathrm{Con}(A)} \omega_{\chi_k}(C_\alpha) \right) \\ &= \mathrm{diag}\left(\omega_{\chi_1}(A), \omega_{\chi_2}(A), \ldots, \omega_{\chi_k}(A)\right). \end{aligned}$$

(2): Clearly $M(C_1) = I$. Also, $\omega_{\chi_1}(A) = \sum_{C \in \mathrm{Con}(A)} |C| = |A|$ is an eigenvalue of $M(A)$, and any other eigenvalue $\omega_{\chi_m}(A)$ satisfies

$$|\omega_{\chi_m}(A)| = \left| \sum_{C \in \mathrm{Con}(A)} \frac{\chi_m(C)|C|}{\chi_m(1)} \right| \leqslant \sum_{C \in \mathrm{Con}(A)} |C| = A,$$

as claimed.

(3): Let $C \in \mathrm{Con}(G)$. By [15, p. 45] we get that

$$m_{ij}(C) = \frac{|C||C_i|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C)\chi(C_i)\overline{\chi(C_j)}}{\chi(1)}.$$

As $m_{ji}(C)$ is real, we get

$$m_{ji}(C) = \overline{m_{ji}(C)} = \frac{|C||C_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\overline{\chi(C)\chi(C_j)\chi(C_i)}}{\chi(1)}$$

$$= \frac{|C_j|}{|C_i|} \times \frac{|C^{-1}||C_i|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C^{-1})\chi(C_i)\overline{\chi(C_j)}}{\chi(1)}$$

$$= \frac{|C_j|}{|C_i|} m_{ij}(C^{-1}).$$

Therefore,

$$m_{ji}(A) = \sum_{C \in \mathrm{Con}(A)} m_{ji}(C) = \sum_{C \in \mathrm{Con}(A)} \frac{|C_j|}{|C_i|} m_{ij}(C^{-1}) = \frac{|C_j|}{|C_i|} m_{ij}(A^{-1}),$$

as claimed.

(4): In general, we denote the (a,b)th entry of a matrix M by $(M)_{ab}$.

Now, $(M(A_1)+M(A_2))_{ij} = m_{ij}(A_1)+m_{ij}(A_2) \neq 0$ if either $m_{ij}(A_1) \neq 0$ or $m_{ij}(A_2) \neq 0$. This is equivalent [by Lemma 3.2(4)] to saying that $C_j \subseteq A_1C_i \cup A_2C_i = (A_1 \cup A_2)C_i$. This is equivalent to saying that $m_{ij}(A_1 \cup A_2) \neq 0$.

Next we consider the product. Let $a, b \in \{1, 2, \ldots, k\}$. Then $(M(A_1)M(A_2))_{ab} = \sum_{i=1}^{k} m_{ai}(A_1)m_{ib}(A_2) \neq 0$ if and only if there exists an i such that $m_{ai}(A_1) \neq 0$ and $m_{ib}(A_2) \neq 0$. By Lemma 3.2(4), this is equivalent to saying that $C_i \subseteq A_1C_a$ and $C_b \subseteq A_2C_i$. Hence $(M(A_1)M(A_2))_{ab} \neq 0$ implies that $C_b \subsetneq A_2A_1C_a = A_1A_2C_a$, which means (again by Lemma 3.2) that $m_{ab}(A_1A_2) \neq 0$. Conversely, assume that $m_{ab}(A_1A_2) \neq 0$; then by Lemma 3.2 we get that $C_b \subsetneq A_2A_1C_a$. As A_1C_a is a normal subset, we can write:

$$C_b \subseteq A_2 \times \bigcup \{C | C \in \mathrm{Con}(A_1C_a)\} \subsetneq \bigcup \{A_2C | C \in \mathrm{Con}(A_1C_a)\}.$$

But each A_2C for $C \in \mathrm{Con}(A_1C_a)$ is a normal subset, so the conjugacy class C_b is contained in one of them. Hence there exists an i such that $C_i \subseteq A_1C_a$ and $C_b \subseteq A_2C_i$. As mentioned above, this implies that $(M(A_1)M(A_2))_{ab} \neq 0$.

Note that $M(A_1)$ and $M(A_2)$ commute, as they have a simultaneous diagonalization (via Y).

$$\frac{\chi(C)\chi(C_j)\chi(C_i)}{\chi(1)}$$

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C^{-1})\chi(C_i)\overline{\chi(C_j)}}{\chi(1)}$$

$$\frac{|C_j|}{|C_i|}m_{ij}(C^{-1}) = \frac{|C_j|}{|C_i|}m_{ij}(A^{-1}),$$

entry of a matrix M by $(M)_{ab}$.
$m_{ij}(A_2) \neq 0$ if either $m_{ij}(A_1) \neq 0$
Lemma 3.2(4)] to saying that $C_j \subseteq$
valent to saying that $m_{ij}(A_1 \cup A_2)$

Let $a, b \in \{1, 2, \ldots, k\}$. Then
$\neq 0$ if and only if there exists an i
By Lemma 3.2(4), this is equivalent
. Hence $(M(A_1)M(A_2))_{ab} \neq 0$ im-
means (again by Lemma 3.2) that
$m_{ab}(A_1A_2) \neq 0$; then by Lemma
a normal subset, we can write:

$$\bigcup \{A_2C | C \in \mathrm{Con}(A_1C_a)\}.$$

rmal subset, so the conjugacy class
ere exists an i such that $C_i \subseteq A_1C_a$
implies that $(M(A_1)M(A_2))_{ab} \neq 0$.
ute, as they have a simultaneous

(5): Assume that $M(A) > 0$. Let $i \in \{1, 2, \ldots, k\}$. Then $m_{1i}(A) \neq 0$. Lemma 3.2 implies that $C_i \subseteq C_1A \subseteq A$, as $C_1 = \{1\}$. Hence, $C_i \subseteq A$ for $i = 1, 2, \ldots, k$, so that $G \subseteq A$. Conversely, assume that $A = G$. Assume that $m_{ij}(A) = 0$ for some i and j. Then $C_j \not\subseteq AC_i = GC_i = G$, a contradiction. So $m_{ij}(A) \neq 0$ for all i, and therefore $M(A) > 0$. ■

Proof of Proposition 3.4. [We postpone the proof of the part of (1) which states that the index of cyclicity of $M(A)$ is equal to $|G : \langle AA^{-1}\rangle|$. The proof of this part will come in Proposition 3.5.]

We will use Proposition 3.3 freely. Let $\mathrm{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$.

Parts (1) and (2): Note first that $\langle A \rangle = G$ if and only if A is not contained in any proper normal subgroup of G.

Assume that $M(A)$ is irreducible. Then $\rho(M(A)) = |A|$ is a simple root of the characteristic polynomial of $M(A)$, so that $\omega_\chi(A) \neq |A|$ for all $\chi \in \mathrm{Irr}(G) - \{1_G\}$. Let $H = \langle A \rangle$. We have to show that $H = G$. If $H < G$, then there exists $\chi \in \mathrm{Irr}(G) - \{1_G\}$ with $H \subseteq \mathrm{Ker}(\chi)$ (as H is normal). Let $C \in \mathrm{Con}(A)$; then $C \subseteq A \subseteq H \subseteq \mathrm{Ker}(\chi)$. Consequently, $\omega_\chi(C) = |C|$ $\forall C \in \mathrm{Con}(A)$. This implies that $\omega_\chi(A) = \sum_{C \in \mathrm{Con}(A)} \omega_\chi(C) = \sum_{C \in \mathrm{Con}(A)} |C| = |A|$, a contradiction. Hence, $H = \langle A \rangle = G$ as required.

Conversely, assume that $\langle A \rangle = G$. In order to show that $M(A)$ is irreducible we will show that $|A|$ is a simple root of the characteristic polynomial of $M(A)$ and that both $M(A)$ and $M(A)^t$ have positive eigenvectors corresponding to the eigenvalue $|A|$. Once this is shown, the irreducibility of $M(A)$ will follow from Theorem 4.1 on p. 18 of [16]. To see that $|A|$ is a simple eigenvalue, suppose that for some $\chi \in \mathrm{Irr}(G)$ we have that $\omega_\chi(A) = |A|$. Part (6) of Lemma 3.2 implies that $A \subseteq \mathrm{Ker}(\chi)$, so that $G = \langle A \rangle \subseteq \mathrm{Ker}(\chi)$. But then, $|G| = \sum_{x \in G} |\chi(x)|^2 = \sum_{x \in G} \chi(1)^2 = |G|\chi(1)^2$, which implies that $\chi(1) = 1$. As $G = \mathrm{Ker}(\chi)$, $\chi = 1_G$. So $|A|$ is a simple eigenvalue.

Let Y be the matrix defined in the statement of Proposition 3.3, and B any normal subset of G. By part (1) of Proposition 3.3 we get that $M(B)Y = Y\,\mathrm{diag}(|B|, \omega_{\chi_2}(B), \ldots, \omega_{\chi_k}(B))$. Let Y_1 be the first column of Y. Then $Y_1 = (|C_1|, |C_2|, \ldots, |C_k|)^t$, where the C_i's are the conjugacy classes of G. In particular $Y_1 > 0$. Note that $M(B)Y_1 = |B|Y_1$, so that Y_1 is a common positive eigenvector of $M(B)$ for all normal subsets B of G. For a specific B, Y_1 corresponds to the eigenvalue $|B|$. So Y_1 is a positive eigenvector of $M(A)$ corresponding to $|A|$ and of $M(A^{-1})$ corresponding to the eigenvalue $|A^{-1}| = \sum_{C \in \mathrm{Con}(A)} |C^{-1}| = |A|$. This means that $M(A^{-1})Y_1 = |A|Y_1$, or $\sum_{j=1}^{k} m_{ij}(A^{-1})|C_j| = |A|\,|C_i|$ for all $i = 1, 2, \ldots, k$. Rewriting this as

$$\sum_{j=1}^{k} m_{ij}(A^{-1}) \frac{|C_j|}{|C_i|} \times 1 = |A| \times 1$$

shows that $(1, 1, \ldots, 1)^t$ is a positive eigenvector of the matrix $\left(m_{ij}(A^{-1})|C_j|/|C_i|\right) = [M(A)]^t$ with respect to the eigenvalue $|A|$. This completes the proof of the irreducibility of $M(A)$ [part (3) of Proposition 3.3 was used in the last stage].

Assume now that $G = \langle A \rangle$, namely that $M(A)$ is irreducible. Let $c(M(A))$ be the index of cyclicity of $M(A)$, and set $c(A) = \{\chi \in \mathrm{Irr}(G) \,|\, |\omega_\chi(A)| = |A|\}$. By Proposition 3.3, $c(M(A)) = |c(A)|$. Let $\chi \in c(A)$. Part (5) of Lemma 3.2 implies that $A \subseteq Z(\chi)$, so that $G = \langle A \rangle \subseteq Z(\chi)$. As the representation for χ is scalar, its degree is 1. Thus $c(M(A))$ is no bigger than the number of linear characters of G, which is $|G:G'|$. If $A = C \in \mathrm{Con}(G)$ and $\chi \in \mathrm{Irr}(G)$ is linear, then clearly $|\omega_\chi(C)| = |C|$, as $\chi(C)$ is a root of unity. Hence $c(C)$ is the set of all linear characters of G, and $c(M(C)) = |G:G'|$.

Parts (3) and (4): By Theorem 1.7(a) on p. 28 of [5], a nonnegative irreducible matrix is primitive if and only if its cyclicity index is equal to one. Now parts (1) and (2) imply parts (3) and (4) except for the statements on the primitivity index.

Let n be any natural number. Part (4) of Proposition 3.3 implies that $M(A^n) \approx (M(A))^n$. Using part (5) of Proposition 3.3, we get that the following are equivalent: (i) $M(A)^n > 0$, (ii) $M(A^n) > 0$, (iii) $A^n = G$. Thus the primitivity index of $M(A)$ is $\mathrm{cn}(A)$. The bound on $\mathrm{cn}(A)$ follows from Theorem 4.14 on p. 48 of [5]. This also shows that $\mathrm{cn}(A) < \infty$ if and only if $M(A)$ is primitive. ■

The next proposition is the analog of Proposition 2.8. Its proof incorporates the completion of the proof of Proposition 3.4(1). The proof is almost identical to that of Proposition 2.8.

Proposition 3.5. *Let G be a finite group, A a normal subset of G, and C a conjugacy class of G. Assume that $\langle A \rangle = \langle C \rangle = G$. Then:*

(i) *For every conjugacy class C_i of G we have that* $|G:\langle AA^{-1}\rangle| = \gcd\{m \,|\, C_i \in C_i A^m\}$.

(ii) $|G:\langle AA^{-1}\rangle| = \gcd\{m \,|\, 1 \in A^m\}$.

(iii) *For every conjugacy class C_i of G we have that* $|G:G'| = \gcd\{m \,|\, C_i \in C_i C^m\}$.

(iv) $|G:G'| = \gcd\{m \,|\, 1 \in C^m\}$.

Proof of Proposition 3.5 and completion of the proof of part (1) of Proposition 3.4. Let B be any normal subset of G. Let $G(M(B))$ be the directed graph with the k vertices $C_1 = \{1\}, C_2, \ldots, C_k$ (all the conjugacy classes of G), and an edge leading from C_i to C_j if and only if $C_j \subseteq BC_i$ [that

e eigenvector of the matrix
ect to the eigenvalue $|A|$. This
$M(A)$ [part (3) of Proposition 3.3

$M(A)$ is irreducible. Let $c(M(A))$
$(A) = \{\chi \in \mathrm{Irr}(G) \mid |\omega_\chi(A)| = |A|\}$.
$\chi \in c(A)$. Part (5) of Lemma 3.2
(χ). As the representation for χ
no bigger than the number of
$A = C \in \mathrm{Con}(G)$ and $\chi \in \mathrm{Irr}(G)$
is a root of unity. Hence $c(C)$ is
$M(C)) = |G : G'|$.
on p. 28 of [5], a nonnegative
ts cyclicity index is equal to one.
except for the statements on the

of Proposition 3.3 implies that
on 3.3, we get that the following
, (iii) $A^n = G$. Thus the primitiv-
(A) follows from Theorem 4.14
$A) < \infty$ if and only if $M(A)$ is ■

oposition 2.8. Its proof incorpo-
tion 3.4(1). The proof is almost

, *A a normal subset of G, and C*
$C\rangle = G$. *Then*:

we have that $|G : \langle AA^{-1}\rangle| =$

e have that $|G : G'| = \gcd\{m \mid C_i$

of the proof of part (1) of
et of G. Let $G(M(B))$ be the
$\}, C_2, \ldots, C_k$ (all the conjugacy
C_j if and only if $C_j \subseteq BC_i$ [that

is, $m_{ij}(B) \neq 0$]. Note that $G(M(A^n))$ is the same as $G((M(A)^n)$ for any natural number n, because of part (4) of Proposition 3.3.

Fix an index i. A circuit of length m through C_i exists in $G(M(A))$ if and only if a loop exists in $G((M(A^m))$ through C_i. A loop in $G((M(A^m))$ through C_i exists if and only if $m_{ii}(A^m) \neq 0$, which means that $C_i \subseteq C_i A^m$. Let $c(M(A))$ and $c(M(C))$ be the cyclicity indices of $M(A)$ and $M(C)$ respectively. By Theorem 2.30 on p. 35 of [5] we get

$$c(M(A)) = \gcd\{m \mid \text{there is a loop in } G(M(A^m)) \text{ through } C_i\}$$
$$= \gcd\{m \mid C_i \subseteq C_i A^m\}.$$

By Proposition 3.5, $c(M(C)) = |G : G'|$, so that part (iii) follows. Part (iv) is a special case of part (iii) (for $i = 1$).

Now, $c(M(A)) = \gcd\{m \mid C_i \subseteq C_i A^m\} = \gcd\{m \mid 1 \in A^m\}$. We now use Theorem 3.3(c) and Theorem 3.2(f) of [2, pp. 14–15] to conclude that $c(M(A)) = |\langle A\rangle : \langle AA^{-1}\rangle|$. As $\langle A\rangle = G$, Parts (i) and (ii) are proved, as well as the remaining statement in part (1) of Proposition 3.4. ■

REMARK. Note that [2] was used only to identify $c(M(A))$ in the case that A is not a conjugacy class. So all the results in the case that either $A = C$ is a conjugacy class or that A is general but no $c(M(A))$ is needed are independent of [2]. This is true for all the results in this section.

Before stating more analogs of results on the Brauer character, we have a few corollaries. We list them first and then prove them.

COROLLARY 3.6. *Let A be a normal subset of the finite group G. Then*:

(i) $\sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(A)$ *is a nonnegative integer*.

(ii) *If* $\langle A\rangle = G$ *and* $\sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(A) > 0$, *then* $G = \langle AA^{-1}\rangle$ *and* $\mathrm{cn}(A) \leqslant 2(k-1)$ *where k is the number of conjugacy classes of G*.

(iii) *Let C be a conjugacy class of G. Then* $|C|\sum_{\chi \in \mathrm{Irr}(G)} \chi(C)/\chi(1)$ *is a nonnegative integer. Moreover, if* $\sum_{\chi \in \mathrm{Irr}(G)} \chi(C)/\chi(1) > 0$ *and* $G = \langle C\rangle$, *then* $G = G'$ *and* $\mathrm{cn}(C) \leqslant 2(k-1)$, *where* $k = |\mathrm{Con}(G)|$.

The next corollary shows that in certain cases, better bounds than in Proposition 3.4(4) can be found for $\mathrm{cn}(C)$. We are only interested in the bounds if they are implied by results on nonnegative matrices. Better bounds in many other cases can be found in [2]. Also compare part (2) of the next corollary with [12].

Corollary 3.7. *Let G be a finite group, $k = |\mathrm{Con}(G)|$, and C a conjugacy class in G. Assume that $G = \langle C \rangle$ and that either*

(1) *C contains a commutator, or*
(2) *C is a real class and $G = G'$.*

Then $C^{2k-2} = G$.

The next (last) corollaries are known results. (One is due to Arad, Herzog, and Stavi, and the other to Garrison. See [2, Theorem 1.1, p. 9] and [15, p. 59].) Here $\mathrm{cn}(G)$ is the least positive integer n such that $C^n = G$ for all $C \in \mathrm{Con}(G)$, $C \neq 1$. If no such n exists, we say that $\mathrm{cn}(G)$ is infinite.

Corollary 3.8. *Let G be a finite group. Then $\mathrm{cn}(G)$ is finite if and only if G is a nonabelian simple group.*

Corollary 3.9. *Let G be a finite group, and C a conjugacy class of G that generates G. Let m be the number of distinct values of $\omega_\chi(C)$ for $\chi \in \mathrm{Irr}(G)$. Then $G = \{1\} \cup C \cup C^2 \cup \cdots \cup C^{m-1}$.*

Proof of Corollaries 3.6, 3.7, 3.8, 3.9. Note that $\sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(A)$ is the trace of the nonnegative integer matrix $M(A)$, so it is a nonnegative integer. If $\langle A \rangle = G$ and $\sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(A) > 0$, then $M(A)$ is irreducible with nonzero trace. Corollary 2.28 on p. 34 and Theorem 4.9 on p. 47 of [5] imply that $M(A)$ is primitive with primitivity index no bigger than $2(k-1)$. Now Corollary 3.6 follows from Proposition 3.4(3) and (4).

The assumption of Corollary 3.7 implies that $M(C)$ is irreducible. If $g \in C$, g is a commutator; then $|C| \sum_{\chi \in \mathrm{Irr}(G)} \chi(C)/\chi(1) > 0$ by Problem 3.10(b) on p. 45 of [15]. Now, Corollary 3.6 implies that $\mathrm{cn}(C) \leq 2(k-1)$. Suppose now that C is real, i.e., $C = C^{-1}$. Part (3) of Proposition 3.3 now implies that $m_{ji}(C) = m_{ij}(C^{-1})|C_j|/|C_i| = m_{ij}(C)|C_j|/|C_i|$. So $m_{ij}(C) \neq 0$ if and only if $m_{ji}(C) \neq 0$. As $G = G'$, $M(C)$ is primitive (by Proposition 3.4). Now, Corollary 4.10 on p. 47 of [5] and our Proposition 3.4 imply again that $\mathrm{cn}(C) \leq 2(k-1)$, as required. So Corollary 3.7 is proved.

By Proposition 3.4(4) we get that $\mathrm{cn}(C)$ is finite for all $C \in \mathrm{Con}(G)$, $C \neq 1$, if and only if $G = G' = \langle C \rangle$ for all $C \in \mathrm{Con}(G)$, $C \neq 1$. This is clearly equivalent to saying that G is a nonabelian simple group. This proves Corollary 3.8.

Note that the assumption of Corollary 3.9 implies that $M(C)$ is irreducible. Proposition 3.3 implies that m is the number of distinct eigenvalues of the diagonalizable marix $M(C)$. Hence the degree of the minimal polynomial of $M(C)$ is equal to m. We now use Exercise 2.3 on p. 29 of [5] to conclude that $I + M(C) + M(C)^2 + \cdots + M(C)^{m-1} > 0$. Part (4) of Proposition 3.3 now implies that $M(\{1\} \cup C \cup \cdots \cup C^{m-1}) > 0$. Finally, by part (5) of Proposition 3.3 we get that $\{1\} \cup C \cup \cdots \cup C^{m-1} = G$ (we use here the trivial fact that for any nonnegative $k \times k$ matrices K, L, R, S the condition $K \approx L$ and $R \approx S$ implies that $K + R \approx L + S$). ■

Now to the analogs of Propositions 2.9 and 2.10.

PROPOSITION 3.10. *Let A be a normal subset of the finite group G. Assume that $G = \langle A \rangle$. Suppose that one of the following holds:*

(i) $C_i \subseteq AC_i$ *for some* $C_i \in \mathrm{Con}(G)$, *or*
(ii) $C_i \subseteq AC_j \cap A^2C_j$ *for some* $\{C_i, C_j\} \subseteq \mathrm{Con}(G)$, *or*
(iii) $C_i \subseteq A^qC_j \cap A^{q+1}C_j$ *for some* $\{C_i, C_j\} \subseteq \mathrm{Con}(G)$ *and some positive integer* q, *or*
(iv) $1 \in A^m \cap A^{m+1}$ *for some positive integer* m.

Then $G = \langle AA^{-1} \rangle$, and if $A = C$ is a conjugacy class, then G is perfect.

Proof. As $G = \langle A \rangle$, $M(A)$ is irreducible. Part (i) is equivalent to $m_{ii}(A) \neq 0$, and (iii) is equivalent to $m_{ji}^{(q)}(A)m_{ji}^{(q+1)}(A) > 0$ (using Lemma 3.2). Each of these implies that $M(A)$ is primitive (see Corollary 2.28 and Problem 6.20 on p. 55 of [5]), which in turn implies that the cyclicity index of $M(A)$ is equal to 1. Now parts (i) and (iii) follow from Proposition 3.4(3) and (4). Part (ii) is a special case of part (iii), and part (iv) is a consequence of parts (ii) and (iv) of Proposition 3.5. ■

NOTATION 3.11. Let G be a finite group, and B a normal subset of G with $G = \langle B \rangle$. Set $\mathrm{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$. Let $p_1(B), p_2(B), \ldots, p_k(B)$ be the elementary symmetric functions in the $\omega_{\chi_i}(B)$'s. Namely,

$$p_1(B) = \sum_{i=1}^{k} \omega_{\chi_i}(B), \qquad p_2(B) = \sum_{i<j} \omega_{\chi_i}(B)\omega_{\chi_j}(B), \ldots, p_k(B) = \prod_{i=1}^{k} \omega_{\chi_i}(B).$$

Let $h(B) = |G : \langle BB^{-1} \rangle|$ if $B \notin \mathrm{Con}(G)$ and $h(B) = |G : G'|$ if $B \in \mathrm{Con}(G)$ (the definitions are the same; see for example Theorem 3.2 on p. 14 of [2]). Note that the $p_i(B)$'s are always integers (even if $G \neq \langle B \rangle$), because they are the coefficients (up to sign) of a characteristic polynomial of the integer matrix $M(B)$.

Proposition 3.12. *Let G be a finite group, $k = |\mathrm{Con}(G)|$, A a normal subset of G, and $h = h(A)$. Assume that $G = \langle A \rangle$. Then*:

(i) *For all $i \leqslant k+1-h$, at least $h-1$ of the following integers are zero*: $p_i(A), p_{i+1}(A), \dots, p_{i+h-1}(A)$.

(ii) *If $h \neq 1$ then $p_i(A)p_{i+1}(A) = 0$ for all $i < k$.*

(iii) *For each $r \leqslant k$ there exists a j, $0 < j \leqslant k$, such that $\omega_{\chi_r}(A) = e^{2\pi i/h}\omega_{\chi_j}(A)$ (where $i = \sqrt{-1}$).*

Proof. For $h = 1$ the proposition is trivial, so we may assume that $h > 1$. Since $G = \langle A \rangle$, we have that $M(A)$ is irreducible but not primitive. The index of cyclicity of $M(A)$ is h [by Proposition 3.4(1) and (2)]. Now, $P_i(A)$ is, up to sign, the coefficient of x^{k-i} in the characteristic polynomial $p_A(x)$ of $M(A)$. Let x^{m_1} and x^{m_2} be two consecutive powers of x in $p_A(x)$ with nonzero coefficients. Theorem 2.27 on p. 34 of [5] implies that h divides $m_1 - m_2$. So $m_1 - m_2 \geqslant h$, and Part (i) follows. Part (ii) follows from part (i). Part (iii) follows from Theorem 1.2 on p. 48 of [16] and our Proposition 3.3. ■

Proposition 3.13. *Let G be a finite group, $C_1, C_2, \dots, C_k$ an ordering of $\mathrm{Con}(G)$, A a normal subset of G, and $h = h(A)$. Assume that $G = \langle A \rangle$ and that $h > 1$. Then there is a partition $\mathrm{Con}(G) = \mathscr{A}_1 \cup \mathscr{A}_2 \cup \cdots \cup \mathscr{A}_h$ into pairwise disjoint subsets $\mathscr{A}_1, \mathscr{A}_2, \dots, \mathscr{A}_h$ with the following properties*:

(i) *If $C \in \mathscr{A}_i$, then*

$$\mathrm{Con}(AC) \subseteq \begin{cases} \mathscr{A}_{i+1} & \text{if } i < h, \\ \mathscr{A}_1 & \text{if } i = h \end{cases} \quad \text{and} \quad \mathrm{Con}(A^h C) \subseteq \mathscr{A}_i.$$

(ii) *For every $i = 1, 2, \dots, h$, there exists a positive integer $m(i)$ such that for every $C \in \mathscr{A}_i$ we have that $\mathrm{Con}(A^{hm(i)}C) = \mathscr{A}_i$.*

(iii) *Set $\mu = \min_i\{|\mathscr{A}_i|\}$. Then the number of irreducible characters χ of G such that $\chi(A) = 0$ is at least $k - h\mu$.*

(iv) *Let $\chi \in \mathrm{Irr}(G) - \{1_G\}$ be such that $A \subseteq Z(\chi)$ (there exists such a χ). For every $j = 1, 2, \dots, k$ set $\omega_\chi(C_j) = |\omega_\chi(C_j)|e^{i\delta_j}$ (where $i = \sqrt{-1}$). Then $\{\delta_j \mid 1 \leqslant j \leqslant k\} = \{(2\pi/h)j \mid j = 0, 1, \dots, h-1\}$, and for $j = 0, 1, \dots, h-1$ we have that $\mathscr{A}_{j+1} = \{C \in \mathrm{Con}(G) \mid \omega_\chi(C) = |\omega_\chi(C)|e^{i(2\pi j/h)}\}$.*

(v) *If $\chi(A) \neq 0$ for all $\chi \in \mathrm{Irr}(G)$ then $|\mathscr{A}_j| = k/h$. In particular, h (which is $|G:\langle AA^{-1}\rangle|$ or $|G:G'|$ if A is a conjugacy class) divides $k = |\mathrm{Con}(G)|$. Furthermore, let $\chi \in \mathrm{Irr}(G) - \{1_G\}$ be such that $A \subseteq Z(\chi)$. Then the set $\{\chi(C) \mid C \in \mathrm{Con}(G)\}$ contains exactly k/h elements of argument $2\pi j/h$*

; group, $k = |\mathrm{Con}(G)|$, A a normal
$G = \langle A \rangle$. Then:

1 of the following integers are zero:

or all $i < k$.
j, $0 < j \leqslant k$, such that $\omega_{\chi_r}(A) =$

ivial, so we may assume that $h > 1$.
irreducible but not primitive. The
ition 3.4(1) and (2)]. Now, $P_i(A)$ is,
characteristic polynomial $p_A(x)$ of
utive powers of x in $p_A(x)$ with
. 34 of [5] implies that h divides
lows. Part (ii) follows from part (i).
48 of [16] and our Proposition 3.3.

■

group, $C_1, C_2, \ldots, C_k$ an ordering of
$= h(A)$. Assume that $G = \langle A \rangle$ and
$(G) = \mathscr{A}_1 \cup \mathscr{A}_2 \cup \cdots \cup \mathscr{A}_h$ into
with the following properties:

and $\mathrm{Con}(A^h C) \subseteq \mathscr{A}_i$.

ts a positive integer $m(i)$ such that
$C) = \mathscr{A}_i$.
ber of irreducible characters χ of

$A \subseteq Z(\chi)$ (there exists such a χ).
$(C_j)|e^{i\delta_j}$ (where $i = \sqrt{-1}$). Then
$-1\}$, and for $j = 0, 1, \ldots, h-1$ we
$\omega_\chi(C)|e^{i(2\pi j/h)}\}$.
hen $|\mathscr{A}_j| = k/h$. In particular, h
a conjugacy class) divides $k =$
$\}$ be such that $A \subseteq Z(\chi)$. Then the
$/h$ elements of argument $2\pi j/h$

for $j = 0, 1, \ldots, h-1$. In particular, there are exactly k/h positive real (and, if h is even exactly, k/h negative real) elements in this set.

Proof. The proof is the same as the proof of Proposition 2.11, adjusted to this case. Let α be the given ordering of $\mathrm{Con}(G)$, and write $\mathrm{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$. Set $M(B) = M^\alpha(B)$ for every normal subset B of G. As $G = \langle A \rangle$, we know that $M(A)$ is irreducible with cyclicity index $h > 1$. Let $Y = \big(\omega_{\chi_i}(C_j)\big)'$. By Proposition 3.3,

$$M(A)Y = Y\operatorname{diag}\big((\omega_{\chi_1}(A), \omega_{\chi_2}(A), \ldots, \omega_{\chi_k}(A)\big).$$

Let $\chi \in \mathrm{Irr}(G) - \{1_G\}$ be such that $A \subseteq Z(\chi)$. Such a χ exists, for since the cyclicity index of $M(A)$ is bigger than 1, we must have some eigenvalue $\omega_\chi(A)$ of $M(A)$, other than $|A|$, satisfying $|\omega_\chi(A)| = |A|$. Hence, $\chi \neq 1_G$ and $A \subseteq Z(\chi)$ by Lemma 3.2(5). Now, $\chi = \chi_r$ for some $r \neq 1$.

Let v be the rth column of Y, namely, $v = (\omega_\chi(C_1), \omega_\chi(C_2), \ldots, \omega_\chi(C_k))'$. Then $M(A)v = \omega_\chi(A)v$, so that v is an eigenvector of $M(A)$ corresponding to the eigenvalue $\omega_\chi(A)$. By Theorem 1.2, $\omega_\chi(A)$ is a simple eigenvalue of $M(A)$, and so every eigenvector corresponding to $\omega_\chi(A)$ is of the form λv for some $\lambda \in \mathbb{C}$. Write $\omega_\chi(C_j) = |\omega_\chi(C_j)|e^{i\delta_j}$. Note that $\omega_\chi(C_1) = 1$, so that we can take the matrix $D = \operatorname{diag}(e^{i\delta_1}, e^{i\delta_2}, \ldots, e^{i\delta_k})$ as the matrix D of the proof of Theorem 2.20 on p.32 of [5] (the matrix D goes back to the proof of Theorem 2.14 on p. 31 of [5]).

By the proof of Theorem 2.20(c) on p. 33 of [5] we get that $\{\delta_j \mid 1 \leqslant j \leqslant k\} = \{(2\pi/h)j \mid j = 0, 1, \ldots, h-1\}$. For $j = 0, 1, \ldots, h-1$ we set $\mathscr{A}_{j+1} = \{C \in \mathrm{Con}(G) \mid \omega_\chi(C) = |\omega_\chi(C)|e^{i(2\pi j/h)}\}$. We now rename the elements of $\mathscr{A}_t$ as follows: $\mathscr{A}_t = \{C_{t,1}, C_{t,2}, \ldots, C_{t,m_t}\}$ for $t = 1, 2, \ldots, h$. Clearly, $\mathrm{Con}(G) = \bigcup_{i=1}^h \mathscr{A}_i$. Let P be the permutation matrix corresponding to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & k \\ 1,1 & 1,2 & 1,3 & \cdots & 1,m_1 & 2,1 & 2,2 & \cdots & 2,m_2 & 3,1 & \cdots & & h,m_h \end{pmatrix}.$$

Again, the proof of Theorem 2.20(c) of [5] shows that

$$PM(A)P' = \begin{pmatrix} 0_1 & M_{12} & 0 & \cdots & 0 \\ 0 & 0_2 & M_{23} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0_{h-1} & M_{h-1,h} \\ M_{h1} & 0 & \cdots & 0 & 0_h \end{pmatrix} = M^\beta(B)$$

for some ordering β of Con(G), where each 0_j is a square zero matrix whose order is $|\mathscr{A}_j|$, and $M_{12}, M_{23}, \dots, M_{h-1,h}, M_{1h}$ are nonnegative matrices. The definition of $M^{\beta}(A)$ now implies that the first statements of part (i) and part (iv) hold. Part (iii) is a consequence of Theorem 4.4 on p. 60 of [16]. By Problem 6.10 on p. 54 of [5] we get that $M^{\beta}(A^h) = [M^{\beta}(A)]^h = \mathrm{diag}(N_1, N_2, \dots, N_h)$, where each N_i is a primitive square matrix. Let $m(j)$ be the primitivity index of N_j; then $N_j^{m(j)} > 0$. Now the second statement of (i) and all of (ii) follow from the definitions of $M^{\beta}(A^h)$ and $M^{\beta}(A^{hm(j)})$ respectively. Part (v) follows from the previous parts and Corollary 4.2 on p. 61 of [16]. ■

PROPOSITION 3.14. *Let G be a finite group,* $\mathrm{Con}(G) = \{C_1, C_2, \dots, C_k\}$ *with* $C_1 = \{1\}$. *Let A be a normal subset of G such that* $|A| > 1$ *and* $\langle A \rangle = G$. *Then for every* $C \in \mathrm{Con}(G)$ *we have that* $|C|$ *does not divide at least* $\log_{|A|}|C|$ *of the* $|C_i|$*'s.*

Proof. The proof is the same as the proof of Proposition 2.13(iii), adjusted to this case. The assumption implies that $M(A)$ is irreducible. Its leading eigenvalue is $|A|$, and $(|C_1| = 1, |C_2|, \dots, |C_k|)^t$ is an eigenvector corresponding to it. Now the result follows from a result of Ashley [4]. ■

REMARK. The correspondences $\theta \to M(\theta)$ and $A \to M(A)$ that were introduced in Sections II and III of this article can be used to study special families of matrices. Properties of these families (which generalize many of the known generalizations of the circulant matrices) are consequences of properties of group characters and conjugacy classes. See for example [8, 9]. See also [13] for a review article about related methods of studying this type of families of matrices using groups.

We would like to thank Professor Morton E. Harris for the proof of part (ii) of Theorem 2.7 and for helpful conversations. A major part of this paper was written while the author was visiting the University of Minnesota in Minneapolis. I would like to thank the Department of Mathematics of the University of Minnesota for their hospitality.

REFERENCES

1 J. L. Alperin, *Local Representation Theory*, Cambridge U.P., 1986.
2 Z. Arad, M. Herzog, and J. Stavi, Powers and products of conjugacy classes in finite groups, in *Products of Conjugacy Classes in Finite Groups*, Lecture Notes in Math. 1112, Springer-Verlag, Berlin, 1985, pp. 6–51.

ıch 0_j is a square zero matrix whose M_{1h} are nonnegative matrices. The first statements of part (i) and part Theorem 4.4 on p. 60 of [16]. By get that $M^{\beta}(A^h) = [M^{\beta}(A)]^h =$ rimitive square matrix. Let $m(j)$ be 0. Now the second statement of (i) tions of $M^{\beta}(A^h)$ and $M^{\beta}(A^{hm(j)})$ revious parts and Corollary 4.2 on ■

te group, $\mathrm{Con}(G) = \{C_1, C_2, \ldots, C_k\}$ *f G such that* $|A| > 1$ *and* $\langle A \rangle = G$. $|C|$ *does not divide at least* $\log_{|A|}|C|$

the proof of Proposition 2.13(ii). ıplies that $M(A)$ is irreducible. Its $1, |C_2|, \ldots, |C_k|)^t$ is an eigenvector s from a result of Ashley [4]. ■

$\to M(\theta)$ and $A \to M(A)$ that were article can be used to study special families (which generalize many of ant matrices) are consequences of gacy classes. See for example [8, 9]. lated methods of studying this type

rton E. Harris for the proof of part rsations. A major part of this paper ng the University of Minnesota in Department of Mathematics of the ity.

y, Cambridge U.P., 1986.
s and products of conjugacy classes in *Classes in Finite Groups*, Lecture Notes 985, pp. 6–51.

3 Z. Arad, D. Chillag, and M. Herzog, Powers of characters of finite groups, *J. Algebra* 103:241–255 (1986).
4 J. Ashley, On the Perron-Frobenius eigenvector for nonnegative integral matrices whose largest eigenvalue is integral, *Linear Algebra Appl.* 94:103–108 (1987).
5 A. Berman and R. J. Plemmons, *Nonnegative Matrices in the Mathematical Sciences*, Academic, New York, 1979.
6 D. Chillag, Characters, nonnegative matrices and generalized circulants, *Proc. Symp. Pure Math.* 47(2):33–40 (1987).
7 D. Chillag, Character values of finite groups as eigenvalues of nonnegative integer matrices, *Proc. Amer. Math. Soc.* 97:565–567 (1986).
8 D. Chillag, Generalized circulants and class functions of finite groups, *Linear Algebra Appl.* 93:191–208 (1987).
9 D. Chillag, Generalized circulants and class functions of finite groups. II, *Linear Algebra Appl.* 108:199–212 (1988).
10 C. Curtis and I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders*, Vol. 1, Wiley-Interscience, New York, 1981.
11 P. J. Davis, *Circulant Matrices*, Wiley, New York, 1979.
12 J. Denes, Research problems, *Period. Math. Hungar.* 16(2):139–140 (1985).
13 P. Diaconis, Patterned matrices, in *Matrix Theory and Applications* (C. Johnson, ed.), Vol. 40 of the AMS Proceed. of Sympos., *Applied Math.*, 37–58 (1990).
14 W. Feit, *The Representation Theory of Finite Groups*, North Holland, Amsterdam, 1982.
15 I. M. Isaacs, *Character Theory of Finite Groups*, Academic, New York, 1976.
16 H. Minc, *Nonnegative Matrices*, Wiley-Interscience, New York, 1988.

Received 15 December 1989; final manuscript accepted 9 December 1990