PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 98, Number 1, September 1986

ON POWERS OF CHARACTERS AND POWERS OF CONJUGACY CLASSES OF A FINITE GROUP

HARVEY I. BLAU AND DAVID CHILLAG

ABSTRACT. Two results are proved. The first gives necessary and sufficient conditions for a power of an irreducible character of a finite group to have exactly one irreducible constituent. The other presents necessary and sufficient conditions for a power of a conjugacy class of a finite group to be a single conjugacy class. Examples are given.

1. Introduction. The product of conjugacy classes $C_1, C_2, \ldots, C_r$ of a finite group G is defined as follows:

$$C_1 \cdot C_2 \cdots C_r = \{x_1 x_2 \cdots x_r \mid x_i \in C_i,\ 1 \leq i \leq r\}.$$

This product is denoted by C^n if $C_1 = C_2 = \cdots = C_r = C$. For an ordinary character ϑ of G we denote the set of irreducible constituents of ϑ by $\mathrm{Irr}(\vartheta)$. The set of all irreducible characters of G is denoted by $\mathrm{Irr}(G)$.

Recently, several results on products of conjugacy classes and similar results on products of characters have been proved. The book [**1**] (in particular, the articles [**2** and **3**]) and the article [**4**] contain analogous results on the so-called covering number and character-covering-number of a finite group. The identity $C_1C_2 = C_1,\ C_2$ or $C_1 \cup C_2$ for two nonidentity conjugacy classes C_1, C_2 of G, and the condition $\mathrm{Irr}(\chi_1\chi_2) \subseteq \{\chi_1, \chi_2\}$ for two nonprincipal irreducible characters χ_1, χ_2 of G, are investigated in the forthcoming articles [**5** and **10**], and an extension of the character-theoretic results to modular representations is studied in [**6**].

Our purpose in this paper is to derive the two analogous results stated below. First we give some notation. The class function $\vartheta^{(n)}$ is defined by $\vartheta^{(n)}(g) = \vartheta(g^n)$ for all $g \in G$, where ϑ is a class function on G and n is a positive integer. If p is a prime, $|G|_p$ denotes the full power of p which divides $|G|$. If π is a set of primes, $|G|_\pi := \prod_{p\in\pi} |G|_p$. If n is a positive integer, $\pi(n)$ is the set of prime divisors of n. If $\chi \in \mathrm{Irr}(G)$, $Z(\chi) := \{g \in G \,|\, |\chi(g)| = \chi(1)\}$ [**9**, (2.26)], i.e. $Z(\chi)$ is the set of elements of G which act as scalars on a module for χ.

THEOREM A. (i) *Suppose that χ and ψ are two irreducible characters of a finite group G such that $\chi^n = k\psi$ for some positive integers n, k with $n \geq 2$. Then χ vanishes on $G - Z(\chi)$, $\psi = \chi^{(n)}$, $k = \chi(1)^{n-1}$ and $|G|_{\pi(n)}$ divides $|Z(\chi)|$.*

(ii) *Conversely, let G be a finite group and $\chi \in \mathrm{Irr}(G)$ such that χ vanishes on $G - Z(\chi)$. If n is any positive integer such that $|G|_{\pi(n)}$ divides $|Z(\chi)|$, then $\chi^n = k\psi$ for some positive integer k and $\psi \in \mathrm{Irr}(G)$ (namely, $k = \chi(1)^{n-1}$ and $\psi = \chi^{(n)}$).*

THEOREM B. (i) *Suppose that $C_1 \neq \{1\}$ and C_2 are conjugacy classes of a finite group G such that $C_1^n = C_2$ for some integer $n \geq 2$. Then there exists some*

Received by the editors September 17, 1985.
1980 *Mathematics Subject Classification*. Primary 20C15, 20D99.

$N \triangleleft G$ and $g \in G - N$ such that C_1 is the coset gN, and such that the map $a \mapsto a^n$ is a bijection from C_1 onto C_2.

(ii) *Conversely, if a finite group G has a normal subgroup N and an element g in $G - N$ such that the coset gN is a single G-conjugacy class, and such that for some integer n the map $a \mapsto a^n$ for $a \in gN$ is a monomorphism, then g^nN is a G-conjugacy class and $(gN)^n = g^nN$.*

EXAMPLES. The conditions of Theorem A hold, of course, for any linear character χ of G (and all positive integers n). All finite groups G such that $G' \leq Z(G)$ have the property that χ vanishes on $G - Z(\chi)$ for all $\chi \in \mathrm{Irr}(G)$ [**9**, (2.31), (2.30)]. For such groups, the hypotheses of Theorem A(ii) are satisfied for any positive integer n which is relatively prime to $|G|$, or, more generally, for which $|G|_{\pi(n)}$ divides $|Z(G)|$. Groups which have an irreducible faithful character χ vanishing on $G - Z(\chi)$ are called groups of central type. Such groups were proved to be solvable in [**8**]. Examples can be found in [**7**].

To discuss Theorem B, we note that the following are examples of a group G, normal subgroup N and element g of $G-N$ such that gN is exactly one G-conjugacy class: (a) G is a Frobenius group with kernel N and cyclic complement $\langle g \rangle$; (b) G is an extra-special p-group, $N = Z(G)$, and g is any element of $G - N$; (c) $G = NH$, where $H = GL_n(q)$ for some prime power $q > 2$ and integer $n \geq 2$, N is the natural module for H (elementary abelian of order q^n), and $g \neq 1$ is a scalar matrix in H. In all three classes of examples, if n is any integer coprime to the order of g, then the map $a \mapsto a^n$ is one-to-one for $a \in gN$. In (a) and (c), there can easily be found instances where there is an integer n not coprime to the order of g, but for which $a \mapsto a^n$ is again one-to-one for $a \in gN$. For example, let g have order 4 such that g^2 inverts N. Then $a \mapsto a^2$ for $a \in gN$ is a monomorphism. Note that in (a) and (c), $gN = \{g^x \mid x \in N\}$, but this is not true in (b).

ACKNOWLEDGMENT. Much of the work for this paper was done during a visit to the Technion–Israel Institute of Technology in July, 1985, by H. Blau, who thanks that institution for its support and hospitality.

2. Proofs. We first establish the following lemma, which is a slight refinement of [**9**, Exercise (4.7)].

LEMMA. *Let χ be an ordinary character of a finite group G. Then for every positive integer n, $\chi^{(n)} = \vartheta_1 - \vartheta_2$ where ϑ_i is a character of G and $\mathrm{Irr}(\vartheta_i) \subseteq \mathrm{Irr}(\chi^n)$ for $i = 1, 2$.*

PROOF. The proof is by induction on n. The result trivially holds for $n = 1$, since $\chi^{(1)} = 2\chi - \chi$.

Suppose that $n > 1$. Then $n = mp$, where p is a prime divisor of n and m is a positive integer, $m < n$. By induction, $\chi^{(m)} = \eta_1 - \eta_2$ where, for $i = 1, 2$, η_i is a character of G such that $\mathrm{Irr}(\eta_i) \subseteq \mathrm{Irr}(\chi^m)$. By [**9**, p. 60], we have

$$\chi^{(n)} = (\chi^{(m)})^{(p)} = \eta_1^{(p)} - \eta_2^{(p)} = (\eta_1^p - p\tilde{\eta}_1) - (\eta_2^p - p\tilde{\eta}_2),$$

where, for $i = 1, 2$, $\tilde{\eta}_i$ is a character of G afforded by a submodule of a module affording η_i^p. Thus, $\mathrm{Irr}(\tilde{\eta}_i) \subseteq \mathrm{Irr}(\eta_i^p)$.

Set $\vartheta_1 = \eta_1^p + p\tilde{\eta}_2$ and $\vartheta_2 = \eta_2^p + p\tilde{\eta}_1$. Then ϑ_1 and ϑ_2 are characters of G and $\chi^{(n)} = \vartheta_1 - \vartheta_2$. Since $\mathrm{Irr}(\vartheta_1 + \vartheta_2) \subseteq \mathrm{Irr}(\eta_1^p) \cup \mathrm{Irr}(\eta_2^p)$, it suffices to show that

$\mathrm{Irr}(\eta_i^p) \subseteq \mathrm{Irr}(\chi^n)$ for $i = 1, 2$. But $\mathrm{Irr}(\eta_i) \subseteq \mathrm{Irr}(\chi^m)$ implies that $t_i\chi^m = \eta_i + \rho_i$ for some positive integer t_i and character ρ_i of G. Then $t_i^p\chi^n = (\eta_i + \rho_i)^p = \eta_i^p + \tau_i$ for a suitable character τ_i of G. Hence, $\mathrm{Irr}(\eta_i^p) \subseteq \mathrm{Irr}(\chi^n)$ as desired.

PROOF OF THEOREM A(i). Assume that $\chi, \psi \in \mathrm{Irr}(G)$ and $\chi^n = k\psi$ for some positive integers n, k with $n \geq 2$. By the lemma, $\chi^{(n)} = \vartheta_1 - \vartheta_2$ where $\mathrm{Irr}(\vartheta_1) \cup \mathrm{Irr}(\vartheta_2) \subseteq \mathrm{Irr}(\chi^n) = \{\psi\}$. Therefore, $\vartheta_1 = k_1\psi$ and $\vartheta_2 = k_2\psi$ for some integers k_1, k_2. Consequently, $\chi^{(n)} = b\psi$ for some integer b. As $\chi^{(n)}(1) = \chi(1) = b\psi(1)$, we conclude that $b > 0$ and that $\chi^{(n)}$ is a character of G. Since $\chi^n = k\psi$ and $\chi^{(n)} = b\psi$, it follows that, for any $g \in G$, $\chi^n(g) = (k/b)\chi^{(n)}(g)$. Evaluation at $g = 1$ yields $k/b = \chi(1)^{n-1}$, so that

$$\chi^n = \chi(1)^{n-1}\chi^{(n)}. \tag{1}$$

It follows from (1) that for any $g \in G$, $|\chi(g)| = \chi(1)$ if and only if $|\chi(g^n)| = \chi(1)$. Hence,

$$g \in Z(\chi) \quad \text{if and only if} \quad g^n \in Z(\chi). \tag{2}$$

Next, we will show that

$$\chi \text{ vanishes on } G - Z(\chi). \tag{3}$$

Let $h \in G - Z(\chi)$. By (2) we obtain $h^{n^i} \in G - Z(\chi)$ for each integer $i \geq 0$, so that $|\chi(h^{n^i})| < \chi(1)$. Suppose that $\chi(h) \neq 0$. Then by (1), $\chi(h^{n^i}) \neq 0$ for all $i \geq 0$. It also follows from (1) that

$$|\chi(h^{n^i})| = |\chi(1)/\chi(h^{n^i})|^{n-1}\,|\chi(h^{n^{i+1}})| > |\chi(h^{n^{i+1}})|.$$

(Here is where the assumption $n \geq 2$ is used.) This implies that $\{|\chi(h^{n^i})|\,|i \geq 0\}$ is infinite, a contradiction which establishes (3).

From (2) and (3) we obtain $|\chi(g)| = |\chi(g^n)| = |\chi^{(n)}(g)|$ for all $g \in G$. Then by the First Orthogonality Relation, $[\chi^{(n)}, \chi^{(n)}] = [\chi, \chi] = 1$. Hence $\chi^{(n)}$ is irreducible and equals ψ.

Finally, let $\pi = \pi(n)$ and suppose that $|G/Z(\chi)|_\pi \neq 1$. Let $gZ(\chi)$ be a non-identity π-element of $G/Z(\chi)$. Then $g^{n^j} \in Z(\chi)$ for some positive integer j. So $g \in Z(\chi)$, be repeated application of (2), which is a contradiction. Therefore, $|G|_\pi$ divides $|Z(\chi)|$ and (i) is proved.

PROOF OF THEOREM A(ii). Assume that $\chi \in \mathrm{Irr}(G)$, χ vanishes on $G - Z(\chi)$, and n is a positive integer such that $|G|_{\pi(n)}$ divides $|Z(\chi)|$. Let $g \in G$ be such that $g^n \in Z(\chi)$. Then $g \in Z(\chi)$, for otherwise $G/Z(\chi)$ would contain a $\pi(n)$-element. Hence, for every $g \in G$ we have that $g \in Z(\chi)$ if and only if $g^n \in Z(\chi)$. So our assumption that χ vanishes on $G - Z(\chi)$ trivially implies that $\chi^n(g) = \chi(1)^{n-1}\chi^{(n)}(g) = 0$ for all $g \notin Z(\chi)$. Since $\chi_{Z(\chi)} = \chi(1)\lambda$ for some linear character λ of $Z(\chi)$, we get that for each $g \in Z(\chi)$,

$$\chi^n(g) = \chi(1)^n\lambda(g)^n = \chi(1)^{n-1}\chi^{(n)}(g).$$

Therefore, $\chi^n = \chi(1)^{n-1}\chi^{(n)}$. Now $|\chi(g)| = |\chi^{(n)}(g)|$ ($= 0$ or $\chi(1)$) for all $g \in G$, and thus $[\chi^{(n)}, \chi^{(n)}] = 1$. Hence (as $\chi^{(n)}$ is always an integral combination of irreducible characters), $\chi^{(n)} \in \mathrm{Irr}(G)$.

PROOF OF THEOREM B(i). Suppose that $C_1^n = C_2$ for conjugacy classes $C_1 \neq \{1\}$, C_2 of G, and integer $n \geq 2$. Fix some $g \in C_1$. Write $C_1 = \{g, gh_2, \ldots, gh_k\}$

where $N := \{h_1 = 1, h_2, \ldots, h_k\}$ is a suitable set of k distinct elements of G, *i.e.* $C_1 = gN$. For each $1 \leq i \leq k$, $g^{n-1}gh_i = g^n h_i \in C_1^n = C_2$, so $C_2 \supseteq g^n N$. Since $C_G(g) \leq C_G(g^n)$, $g \in C_1$ and $g^n \in C_2$, we have that $|C_2| \leq |C_1| = |N| = |g^n N|$. Hence, $C_2 = g^n N$ and $|C_1| = |C_2|$. Since $\{a^n | a \in C_1\}$ is a conjugacy class (namely, C_2), it follows that the map $a \mapsto a^n$ is a bijection from C_1 onto C_2. We complete the proof by showing that N is a normal subgroup and $g \notin N$:

For any $1 \leq i, j \leq k$, $g^n h_i^g h_j = g^{n-2} g h_i g h_j \in C_1^n = C_2$ (note $n \geq 2$), and hence $g^n h_i^g h_j = g^n h_t$ for some $1 \leq t \leq k$. Therefore,

$$h_i^g h_j \in N \quad \text{for all } 1 \leq i, j \leq k. \tag{4}$$

In particular, letting $j = 1$ yields that g stabilizes N under conjugation. Thus any h_r in N equals h_i^g for some i. So by (4), $h_r h_j \in N$ for all r, j, *i.e.* N is a subgroup.

For any $y \in G$, $g^y = gh$ for some $h \in N$ and

$$gN = C_1 = C_1^y = g^y N^y = ghN^y.$$

So $N^y = h^{-1}N = N$, hence N is normal in G. If $g \in N$, then $g^{-1} \in N$ would imply that C_1 contains $gg^{-1} = 1$, which is a contradiction.

PROOF OF THEOREM B(ii). Suppose that $N \triangleleft G$, $g \in G - N$, $gN = C_1$ is a conjugacy class of G, and $a \mapsto a^n$ is one-to-one for all $a \in gN$. Now $C_2 := \{a^n | a \in C_1\}$ is a conjugacy class of G and $C_2 \subseteq C_1^n = g^n N$. Since $|C_2| = |gN| = |g^n N|$ by hypothesis, we have that $C_2 = C_1^n$.

REFERENCES

1. Z. Arad and M. Herzog (Editors), *Products of conjugacy classes in groups*, Lecture Notes in Math., vol. 1112, Springer-Verlag, Berlin, 1985.
2. Z. Arad, M. Herzog and J. Stavi, *Powers and products of conjugacy classes in groups*, Products of Conjugacy Classes in Groups, Lecture Notes in Math., vol. 1112, Springer-Verlag, Berlin, 1985, pp. 6–51.
3. Z. Arad, D. Chillag and G. Moran, *Groups with a small covering number*, Products of Conjugacy Classes in Groups, Lecture Notes in Math., vol. 1112, Springer-Verlag, Berlin, 1985, pp. 222–244.
4. Z. Arad, D. Chillag and M. Herzog, *Powers of characters of finite groups*, J. Algebra (to appear).
5. Z. Arad and E. Fisman, *An analogy between products of two conjugacy classes and products of two irreducible characters in finite groups* (submitted to Proc. Edinburgh Math. Soc.).
6. H. I. Blau, *On tensor products of simple modules for finite group algebras* (in preparation).
7. F. R. DeMeyer and G. J. Janusz, *Finite groups with an irreducible representation of large degree*, Math. Z. **108** (1969), 145–153.
8. R. B. Howlett and I. M. Isaacs, *On groups of central type*, Math. Z. **179** (1982), 555–569.
9. I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976.
10. A. Mann, *Products of classes and characters in finite groups* (in preparation).

DEPARTMENT OF MATHEMATICAL SCIENCES, NORTHERN ILLINOIS UNIVERSITY, DE KALB, ILLINOIS 60115

DEPARTMENT OF MATHEMATICS, TECHNION–ISRAEL INSTITUTE OF TECHNOLOGY, 32000 HAIFA, ISRAEL