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 $\vartheta$ of $G$ we denote the set of irreducible constituents of $\vartheta$ by $\text{Irr}(\vartheta)$. The set of all irreducible characters of $G$ is denoted by $\text{Irr}(G)$.

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 $C_1 C_2 = C_1, C_2$ or $C_1 \cup C_2$ for two nonidentity conjugacy classes $C_1, C_2$ of $G$, and the condition $\text{Irr}(\chi_1 \chi_2) \subseteq \{\chi_1, \chi_2\}$ for two nonprincipal irreducible characters $\chi_1, \chi_2$ 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 $\vartheta$ 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 $\pi$ 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 $\chi \in \text{Irr}(G)$, $Z(\chi) := \{g \in G \mid \chi(g) = \chi(1)\}$ [9, (2.26)], i.e. $Z(\chi)$ is the set of elements of $G$ which act as scalars on a module for $\chi$.

**Theorem A.** (i) Suppose that $\chi$ and $\psi$ 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 $\chi$ 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 $\chi \in \text{Irr}(G)$ such that $\chi$ 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 $\psi \in \text{Irr}(G)$ (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
N < G and g ∈ G − N such that C₁ is the coset gN, and such that the map a ↦ aⁿ is a bijection from C₁ onto C₂.

(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 ↦ aⁿ for a ∈ gN is a monomorphism, then gⁿN is a G-conjugacy class and (gN)ⁿ = gⁿN.

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' ≤ Z(G) have the property that χ vanishes on G − Z(χ) for all χ ∈ 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|,τ(n) divides |Z(G)|. Groups which have an irreducible faithful character χ vanishing on G − Z(χ) 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 (g); (b) G is an extra-special p-group, N = Z(G), and g is any element of G − N; (c) G = NH, where H = GLₙ(q) for some prime power q > 2 and integer n ≥ 2, N is the natural module for H (elementary abelian of order qⁿ), and g ≠ 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 ↦ aⁿ is one-to-one for a ∈ 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 ↦ aⁿ is again one-to-one for a ∈ gN. For example, let g have order 4 such that g² inverts N. Then a ↦ a² for a ∈ gN is a monomorphism. Note that in (a) and (c), gN = {gx | x ∈ 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, \( \chi^{(n)} = \vartheta₁ - \vartheta₂ \) where \( \varthetaᵢ \) is a character of G and Irr(\( \varthetaᵢ \)) ⊆ 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, \( \chi^{(m)} = \eta₁ - \eta₂ \) where, for i = 1, 2, \( \etaᵢ \) is a character of G such that Irr(\( \etaᵢ \)) ⊆ Irr(\( \chi^{m} \)). By [9, p. 60], we have

\[ \chi^{(n)} = (\chi^{(m)})^\langle p \rangle = \eta₁^\langle p \rangle - \eta₂^\langle p \rangle = (\eta₁^p - p\eta₁) - (\eta₂^p - p\eta₂), \]

where, for i = 1, 2, \( \etaᵢ \) is a character of G afforded by a submodule of a module affording \( \etaᵢ^p \). Thus, Irr(\( \etaᵢ \)) ⊆ Irr(\( \etaᵢ^p \)).

Set \( \vartheta₁ = \eta₁^p + p\eta₂ \) and \( \vartheta₂ = \eta₂^p + p\eta₁ \). Then \( \vartheta₁ \) and \( \vartheta₂ \) are characters of G and \( \chi^{(n)} = \vartheta₁ - \vartheta₂ \). Since Irr(\( \vartheta₁ + \vartheta₂ \)) ⊆ Irr(\( \etaᵢ^p \) ∪ Irr(\( \etaᵢ^p \))), it suffices to show that
POWERS OF CHARACTERS AND OF CONJUGACY CLASSES 9

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

\text{PROOF OF THEOREM A(i). Assume that } \chi, \psi \in \text{Irr}(G) \text{ and } \chi^m = k\psi \text{ for some positive integers } n, k \text{ with } n \geq 2. \text{ By the lemma, } \chi^{(n)} = \theta_1 - \psi_2 \text{ where } \text{Irr}(\theta_1) \cup \text{Irr}(\psi_2) \subseteq \text{Irr}(\chi^m) = \{\psi\}. \text{ Therefore, } \theta_1 = k\psi \text{ and } \psi_2 = k\psi \text{ for some integers } k_1, k_2. \text{ Consequently, } \chi^{(n)} = b\psi \text{ for some integer } b. \text{ As } \chi^{(n)}(1) = \chi(1) = b\psi(1), \text{ we conclude that } \chi^{(n)} \text{ is a character of } G. \text{ Since } \chi^m = k\psi \text{ and } \chi^{(n)} = b\psi, \text{ it follows that, for any } g \in G, \chi^m(g) = (k/b)\chi^{(n)}(g). \text{ Evaluation at } g = 1 \text{ yields } k/b = \chi(1)^{n-1}, \text{ so that }

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

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

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

Next, we will show that

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

Let } h \in G - Z(\chi). \text{ By (2) we obtain } h^{n+i} \in G - Z(\chi) \text{ for each integer } i \geq 0, \text{ so that } |\chi(h^{n+i})| < \chi(1). \text{ Suppose that } \chi(h) \neq 0. \text{ Then by (1), } \chi(h^{n+i}) \neq 0 \text{ for all } i \geq 0. \text{ 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 \text{ is used.} \text{ This implies that } \{|\chi(h^{n+i})| | i \geq 0\} \text{ is infinite, a contradiction which establishes (3).}

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

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

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

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

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

\text{PROOF OF THEOREM B(i). Suppose that } C_1 = C_2 \text{ for conjugacy classes } C_1 \neq \{1\}, C_2 \text{ of } G, \text{ and integer } n \geq 2. \text{ Fix some } g \in C_1. \text{ 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 \( 1 \leq i \leq k \), \( g^{n-1}h_i = g^nh_i \in C_1^n = C_2 \), so \( C_2 \supseteq g^nN \). Since \( C_2(g) \leq C_2(g^n) \), \( g \in C_1 \) and \( g^n \in C_2 \), we have that \( |C_2| \leq |C_1| = |N| = |g^nN| \). Hence, \( C_2 = g^nN \) 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 \( 1 < i, j < k \), \( g^n h_i^2 h_j = g^n g^{-2}gh_ig_jh_j \in C_1^n = C_2 \) (note \( n \geq 2 \)), and hence \( g^n h_i^2 h_j = g^n h_t \) for some \( 1 \leq t \leq k \). Therefore,

\[
(4) \quad h_i^2 h_j \in N \quad \text{for all} \ 1 < i, j < k.
\]

In particular, letting \( j = 1 \) yields that \( g \) stabilizes \( N \) under conjugation. Thus any \( h_i \) in \( N \) equals \( h_i^2 \) for some \( i \). So by (4), \( h_s h_j \in N \) 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 \( N \leq G \), \( g \in G - N \), \( gN = C_1 \) 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 \( C_2 \subseteq C_1^n = g^nN \). Since \( |C_2| = |gN| = |g^nN| \) by hypothesis, we have that \( C_2 = C_1^n \).

**References**


**Department of Mathematical Sciences, Northern Illinois University, De Kalb, Illinois 60115**

**DEPARTMENT OF MATHEMATICS, TECHNION–ISRAEL INSTITUTE OF TECHNOLOGY, 32000 Haifa, Israel**