ELEMENTARY PROOF OF BRAUER'S AND NESBITT'S THEOREM ON ZEROS OF CHARACTERS OF FINITE GROUPS

MANFRED LEITZ

(Communicated by Ronald M. Solomon)

ABSTRACT. The following has been proven by Brauer and Nesbitt. Let G be a finite group, and let p be a prime. Assume χ is an irreducible complex character of G such that the order of a p-Sylow subgroup of G divides the degree of χ. Then χ vanishes on all those elements of G whose order is divisible by p. The two only known proofs of this theorem use profound methods of representation theory, namely the theory of modular representations or Brauer's characterization of generalized characters. The purpose of this paper is to present a more elementary proof.

The aim of this paper is to give a new elementary proof of the following theorem which is due to Brauer and Nesbitt (see [2, Theorem 1]).

Theorem (Brauer and Nesbitt). *Let G be a finite group, and let p be a prime. Suppose χ is an irreducible complex character of G such that p does not divide the co-degree $|G|/\chi(1)$ (χ is said to have p-defect zero). Then χ vanishes on all those elements of G whose order is divisible by p.*

As far as we know there exist two different proofs of this theorem. The original proof (see [2] or [5, Chapter 15, especially Theorem 15.29]) needs the theory of modular representations, and the other proof (see [4] or [5, Theorem 8.17]) which is due to Gallagher requires Brauer's characterization of generalized characters (see [5, Theorem 8.4 (a)]). We will give a new proof making use only of basic methods from character theory which do not exceed the first three chapters of Isaacs' book [5].

The starting-point of our proof is the formula in the following Lemma 1 which can be obtained by an iterated application of the formula contained in [5, Theorem 2.13] (see also [3, p. 721]).

Lemma 1. *Let ψ be an irreducible complex character of G, let K be a conjugacy class of G, and let $g \in K$. Then for each positive integer m the equation*

$$\sum_{(x_1, x_2, \ldots, x_m) \in S_m(K)} \psi(x_1) \cdot \psi(x_2) \cdots \psi(x_m) = \left(\frac{|G|}{\psi(1)}\right)^{m-1} \cdot |K| \cdot \psi(g) \qquad (m \in \mathbb{N})$$

holds, where the set $S_m(K) \subseteq G^m$ is given by

$$S_m(K) := \{(x_1, x_2, \ldots, x_m) \in G^m : x_1 \cdot x_2 \cdots x_m \in K\} \qquad (m \in \mathbb{N}).$$

Proof. If ψ is an irreducible character of G, then $\overline{\psi}$ is also an irreducible character of G, where $\overline{\psi}(x) := \psi(x^{-1})$ $(x \in G)$. If $e_{\overline{\psi}} \in \mathbb{C}[G]$ denotes the primitive central idempotent in the group algebra $\mathbb{C}[G]$ corresponding to $\overline{\psi}$, then

$$e_{\overline{\psi}} = (\psi(1)/|G|) \cdot \sum_{x \in G} \psi(x) \cdot x$$

(see [5, Theorem 2.12]). Evaluating $e_{\overline{\psi}}^m$ in accordance with this formula, then comparing for each $x \in G$ the coefficients in the equation $e_{\overline{\psi}}^m = e_{\overline{\psi}}$, and finally taking the sum of these coefficients over all $x \in K$ ($\sum_{x \in K} \psi(x) = |K| \cdot \psi(g)$) yields the assertion. $\qquad\blacksquare$

We describe in short how we will proceed in what follows. Let p and χ satisfy the assumptions of the theorem. Assume K is a p-singular conjugacy class of G (i.e. p divides the order of the elements of K), and let $g \in K$. Furthermore, let p^a be the highest power of p which divides the order of G. Using the formula from Lemma 1, we will show that *all* the numbers $c_n := p^{-n} \cdot (|G|/\chi(1))^{p^{a+n}-1} \cdot |K| \cdot \chi(g)$ $(n \in \mathbb{N})$ are algebraic integers. Then the conclusion $\chi(g) = 0$ is straightforward by a standard argument from algebraic number theory. In order to realize that the numbers c_n $(n \in \mathbb{N})$ indeed are algebraic integers, we divide the sum from Lemma 1 into subsums. For it, we introduce for each $m \in \mathbb{N}$ a distinguished automorphism σ_m of the group G^m which will turn out to be very useful in proving the theorem.

We wish to express here that we were stimulated by a reasoning of Zassenhaus used by him in a proof of a theorem about S-rings (see the footnote in [6, p. 454]) to look at the theme in the way as follows.

Definition. Let m be a positive integer. The *shift-automorphism* $\sigma_m \colon G^m \to G^m$ is defined by $(x_1, x_2, \ldots, x_m)^{\sigma_m} := (x_2, \ldots, x_m, x_1)$.

If Δ denotes an orbit of the action of the cyclic group $\langle \sigma_m \rangle$ of order m on G^m, and $(x_1, x_2, \ldots, x_m)$, $(y_1, y_2, \ldots, y_m)$ both are in Δ, then the product-elements $x_1 \cdot x_2 \cdots x_m$ and $y_1 \cdot y_2 \cdots y_m$ are conjugate in G because of the identity $x_{k+1} \cdots x_m \cdot x_1 \cdots x_k = (x_1 \cdots x_k)^{-1} \cdot (x_1 \cdots x_m) \cdot (x_1 \cdots x_k)$ for $k \in \{1, \ldots, m-1\}$. Now the following observations are quite clear.

Observations. Let m be a positive integer, let σ_m be the shift-automorphism of G^m, and let Δ be an orbit of the action of $\langle \sigma_m \rangle$ on G^m.
  (i) If K is a conjugacy class of G and $S_m(K) = \{(x_1, x_2, \ldots, x_m) \in G^m \colon x_1 \cdot x_2 \cdots x_m \in K\}$ (see Lemma 1), then either $\Delta \subseteq S_m(K)$ or $\Delta \cap S_m(K) = \varnothing$, and the cyclic group $\langle \sigma_m \rangle$ permutes the set $S_m(K)$.
 (ii) Let $\psi \colon G \to \mathbb{C}$ be an arbitrary map. Then the map $(x_1, x_2, \ldots, x_m) \in G^m \to \psi(x_1) \cdot \psi(x_2) \cdots \psi(x_m) \in \mathbb{C}$ is constant on Δ. If $(y_1, y_2, \ldots, y_m) \in \Delta$, then

$$\sum_{(x_1, x_2, \ldots, x_m) \in \Delta} \psi(x_1) \cdot \psi(x_2) \cdots \psi(x_m) = |\Delta| \cdot \psi(y_1) \cdot \psi(y_2) \cdots \psi(y_m).$$

The following Lemma 2 plays the leading role in the proof of the theorem.

Lemma 2. *Let m be an integer of the form $m = p^{a+n}$ (p a prime, p^a the order of a p-Sylow subgroup of G, n a positive integer), and let K be a conjugacy class of G such that the order of its elements is divisible by p. Furthermore, let Δ be an orbit of the action of the group $\langle \sigma_m \rangle$ on the set $S_m(K) = \{(x_1, x_2, \ldots, x_m) \in G^m \colon x_1 \cdot x_2 \cdots x_m \in K\}$. Then the length $|\Delta|$ of Δ is divisible by p^n.*

Proof. Let $(y_1, y_2, \ldots, y_m) \in \Delta$, and set $g := y_1 \cdot y_2 \cdots y_m$. By the assumptions, p divides the order of g. Define $r \in \mathbb{N} \cup \{0\}$ by $|\Delta| = p^r$. Then $(y_1, \ldots, y_m)$ must be a concatenation of $p^{a+(n-r)}$ identical p^r-tuples $(y_1, \ldots, y_{p^r})$, and hence $g = h^{p^{a+(n-r)}}$, where $h := y_1 \cdot y_2 \cdots y_{p^r}$. It follows that $r > n$ must hold, otherwise p would not divide the order of g. $\qquad\square$

Proof of the Theorem. Let assumptions be as formulated in the theorem. Assume K is a p-singular conjugacy class of G, and let $g \in K$. Furthermore, let p^a be the p-part of $|G|$, let $n \in \mathbb{N}$ be an arbitrary integer, and set $m_n := p^{a+n}$. By Lemma 1 and Observations (i)

$$
\begin{aligned}
c_n &:= p^{-n} \cdot \left(\frac{|G|}{\chi(1)} \right)^{m_n - 1} \cdot |K| \cdot \chi(g) \\
&= \sum_{\Delta \subseteq S_{m_n}(K)} p^{-n} \cdot \sum_{(x_1, x_2, \ldots, x_{m_n}) \in \Delta} \chi(x_1) \cdot \chi(x_2) \cdots \chi(x_{m_n}),
\end{aligned}
$$

where the outer sum is taken over all the $\langle \sigma_{m_n} \rangle$-orbits Δ (see Definition) which are contained in $S_{m_n}(K)$ (see Lemma 1). From Observations (ii), Lemma 2, and [5, Corollaries 3.5 and 3.6] follows that c_n is an algebraic integer. Since n is an arbitrary integer, and p does not divide $|G|/\chi(1)$, $\chi(g)$ must be divisible by arbitrarily large powers of p in the ring of all algebraic integers (as, for instance, is apparent from [1, Chapter 3, Lemma 2]). Therefore, if the polynomial $f(X) \in \mathbb{Z}[X]$ annihilates $\chi(g)$, the rational integer $f(0)$ must be divisible by arbitrarily large powers of p as well (by [5, Corollary 3.5]). We conclude that $\chi(g)$ is equal to zero. $\qquad\square$

Remark. A completely analogous theorem on zeros of characters holds for twisted group algebras of finite groups over the complex field. In this case, our arguments work as well (with slight alterations of technical but not of substantial nature).

ACKNOWLEDGEMENT

ADDED AFTER POSTING

After this paper was submitted and accepted for publication, B. Külshammer informed me that a similar proof of (a more general version of) Brauer's and Nesbitt's theorem is contained in his paper *Central idempotents in p-adic group rings*, J. Austral. Math. Soc. Ser. A **56** (1994), 278–289 (see the proof of Proposition 3).

REFERENCES

[1] Y. G. Berkovich and E. M. Zhmud′, *Characters of finite groups* (Part 1), American Mathematical Society (Translations of Mathematical Monographs, Vol. 172), Providence, 1998. MR **98m:**20011

[2] R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. **42** (1941), 556–590. MR **2:**309c

[3] P. X. Gallagher, *Group characters and Sylow subgroups*, J. London Math. Soc. **39** (1964), 720–722. MR **30:**173

[4] P. X. Gallagher, *Zeros of characters of finite groups*, J. Algebra **4** (1966), 42–45. MR **34:**252

[5] I. M. Isaacs, *Character theory of finite groups*, Dover Publications, New York, 1994 (corrected reprint). MR **57:**417 (original ed.)

[6] O. Tamaschke, *Zur Theorie der Permutationsgruppen mit regulärer Untergruppe* II, Math. Z. **80** (1963), 443–465. MR **27:**3697

FACHBEREICH INFORMATIK UND MATHEMATIK, FACHHOCHSCHULE REGENSBURG, POSTFACH 120327, 93025 REGENSBURG, GERMANY

E-mail address: `manfred.leitz@mathematik.fh-regensburg.de`