PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 51, Number 1, August 1975

SCHUR INDICES AND SUMS OF SQUARES

BURTON FEIN[1]

ABSTRACT. Let G be a finite group of exponent n, F a field of characteristic zero, ϵ a primitive nth root of unity, and suppose that the Sylow 2-subgroup of the Galois group of $F(\epsilon)$ over F is cyclic. Let χ be an absolutely irreducible character of G. Strengthening a recent result of Goldschmidt and Isaacs, it is shown that if -1 is a sum of two squares in F, then the Schur index of χ over F is odd.

In [6], Goldschmidt and Isaacs proved the following striking generalization of the splitting field theorems of Fong, Roquette, Solomon, and Yamada:

Theorem 1 (Goldschmidt-Isaacs). *Let G be a finite group of exponent n and let F be a field of characteristic zero. Suppose for some prime p that a Sylow p-subgroup P of the Galois group $\mathrm{Gal}(F(\sqrt[n]{1})/F)$ is cyclic. If $2 \mid |P|$, assume also that $\sqrt{-1} \in F$. Then the Schur index over F of every absolutely irreducible character of G is relatively prime to p.*

In their paper, Goldschmidt and Isaacs conjecture that the hypothesis that $\sqrt{-1} \in F$ if $2 \mid |P|$ can be replaced by the weaker requirement that -1 is a sum of two squares in F if $2 \mid |P|$. We prove their conjecture in this note.

We denote the set of absolutely irreducible characters of G by $\mathrm{Irr}(G)$. For $\chi \in \mathrm{Irr}(G)$, we denote the Schur index of χ over F by $m_F(\chi)$. ϵ_n will denote a primitive nth root of unity. If A and B are finite dimensional central simple F-algebras, we write $A \sim B$ if A and B are similar in the Brauer group of F. A^r will denote $A \otimes A \otimes \ldots \otimes A$, r times.

Theorem 2. *Let F be a field of characteristic zero such that -1 is a sum of two squares in F and let G be a finite group of exponent n. Assume that the Sylow 2-subgroup of $\mathrm{Gal}(F(\epsilon_n)/F)$ is cyclic and let $\chi \in \mathrm{Irr}(G)$. Then $m_F(\chi)$ is odd.*

Received by the editors December 10, 1973 and, in revised form, May 24, 1974.
AMS (MOS) subject classifications (1970). Primary 20C15.
Key words and phrases. Schur index, division algebra.
[1] This work was supported in part by NSF Grant GP-29068.

Proof. Since $m_F(\chi) = m_{F(\chi)}(\chi)$, we may assume that $F(\chi) = F$. In view of Theorem 1, we may assume that $\sqrt{-1} \notin F$. Since there is nothing to prove if $m_F(\chi)$ is odd, we assume that $2|m_F(\chi)$. Let Q denote the rational field and let $E = Q(\epsilon_n) \cap F$. Let L be the subfield of $Q(\epsilon_n)$ such that $L \supset E$, $[L:E]$ is odd, and $[Q(\epsilon_n):L]$ is a power of 2. Since $Q(\epsilon_n)$ is a splitting field for χ, $m_L(\chi)$ is a power of 2. If $m_L(\chi) = 1$, then $m_{LF}(\chi) = 1$ which would imply that $m_F(\chi)$ is odd. If $4|m_L(\chi)$, then $\sqrt{-1} \in L$ by the Benard-Schacher theorem [2, Theorem 1]. But then $\sqrt{-1} \in LF$ and so, since $[LF:L] = [L:F]$ is odd, we would have $\sqrt{-1} \in F$, contrary to our assumption. We conclude that $m_L(\chi) = 2$.

By the Brauer-Witt theorem [10, §2], [9] there is a hyperelementary subgroup H of G and $\zeta \in \mathrm{Irr}(H)$ with the following properties:

(1) there is a normal subgroup N of H and a linear character ψ of N such that $\zeta = \psi^H$;

(2) $H/N \cong \mathrm{Gal}(L(\psi)/L)$;

(3) $L(\zeta) = L$;

(4) $m_L(\zeta) = 2$;

(5) the simple component A of the group algebra of H over L corresponding to ζ is isomorphic to the cyclic algebra $(L(\psi)/L, \sigma, \epsilon_r)$ where $\langle\sigma\rangle = \mathrm{Gal}(L(\psi)/L)$ and $\epsilon_r \in L$; and

(6) the simple component B of the group algebra of G over L corresponding to χ is similar to A.

Since $m_L(\zeta) = 2$, A has index 2. Since L is an algebraic number field, A has exponent 2 in the Brauer group of L [1, Chapter 9]. Since $A^r \sim (L(\psi)/L, \sigma, \epsilon_r^r) \sim L$, we see that r is even. Since $\sqrt{-1} \notin E$ and $[L:E]$ is odd, $\sqrt{-1} \notin L$ so $r = 2s$ where s is odd. We have $A \sim (L(\psi)/L, \sigma, -1) \otimes_L (L(\psi)/L, \sigma, \epsilon_s)$. Since $A^2 \sim L \sim (L(\psi)/L, \sigma, \epsilon_s)^2$ and $(L(\psi)/L, \sigma, \epsilon_s)^s \sim L$, $(L(\psi)/L, \sigma, \epsilon_s) \sim L$. Thus $A \sim (L(\psi)/L, \sigma, -1)$.

By (6) the simple component of the group algebra of G over LF corresponding to χ is similar to $B \otimes_L LF$ and so $B \otimes_L LF \not\sim LF$. By (5), $A \otimes_L LF \not\sim LF$. Let D denote the usual quaternion algebra over Q, i.e. $D = (Q(\sqrt{-1})/Q, \tau, -1)$. A field K splits D if and only if -1 is a sum of two squares in K. We will obtain a contradiction to the assumptions $A \otimes_L LF \not\sim LF$ and -1 is a sum of two squares in F by proving that $A \sim D \otimes_Q L$.

Let K be a finite extension of L, $[K:L] \leq 2$, in which -1 is a sum of two squares. We will prove that K is a splitting field for A. If $K = L(\sqrt{-1})$, this follows from Theorem 1. Suppose $K \neq L(\sqrt{-1})$. By [5], $\sqrt{-1} \in Q(\epsilon_n)$.

Since $\mathrm{Gal}(Q(\epsilon_n)/L)$ is a cyclic 2-group, $K(\sqrt{-1})$ is the unique quadratic extension of K in $K(\psi)$. $A \otimes_L K \sim (L(\psi)/L, \sigma, -1) \otimes_L K \sim (K(\psi)/K, \sigma, -1)$. To prove that $(K(\psi)/L, \sigma, -1) \sim K$ we must show that $-1 \in N_{K(\psi)/K}(K(\psi))$ where $N_{K(\psi)/K}$ denotes the norm from $K(\psi)$ to K. By the Hasse norm theorem, $-1 \in N_{K(\psi)/K}(K(\psi))$ if and only if -1 is a local norm at every prime of K [8, Theorem 4.5]. Since -1 is a sum of two squares in K, this also holds in every completion of K and so all archimedean primes of K are complex. Thus we need only consider finite primes of K. We calculate with the local norm residue symbol $(-1, K(\psi)/K)_\pi$ for any prime π of K [7, Chapter 12, §2]. $(-1, K(\psi)/K)_\pi = 1$ if and only if -1 is a local norm at π [7, Theorem 12-2-4]. We first consider extensions of 2.

Let π extend the rational prime 2. By [4, Theorem 1], $[K_\pi : Q_2]$ is even. We have

$$(-1, K(\psi)/K)_\pi = (N_{K_\pi/Q_2}(-1), Q(\psi)/Q)_2$$

$$= (-1^{[K_\pi:Q_2]}, Q(\psi)/Q)_2 = (1, Q(\psi)/Q)_2 = 1$$

by [7, Proposition 12-2-5]. This -1 is a local norm at π for π extending 2.

Since -1 is a unit, $(-1, K(\psi)/K)_\pi = 1$ if π is unramified from K to $K(\psi)$ [8, Proposition 3.11]. Thus we may restrict our attention to those primes π of K where π extends the rational odd prime p, $p|n$, and where π is ramified from K to $K(\psi)$. In particular, $K(\epsilon_p) \neq K$.

As noted previously, $K(\sqrt{-1})$ is the unique quadratic extension of K in $K(\psi)$. Suppose $p \equiv 3 \pmod 4$. Then $K(\epsilon_p) = K(\sqrt{-1})$ so π is unramified from K to $K(\epsilon_p)$. Since $K(\psi)$ is an extension of K by roots of unity, π is unramified from K to $K(\psi)$. Thus we need only consider the case when $p \equiv 1 \pmod 4$.

Since $p \equiv 1 \pmod 4$, $\epsilon_4 \in Q_p$ [8, Corollary 3.7]. By Theorem 1, $m_{K_\pi}(\zeta) = 1$ and so $(-1, K(\psi)/K)_\pi = 1$. This completes the proof that if -1 is a sum of two squares in K, $[K:L] \leq 2$, then K splits A. In particular, -1 is not a sum of two squares in L and so $D \otimes_Q L$ is a division algebra.

Let D_0 be the division algebra component of A. By [3, Corollary 2], $D_0 \cong D \otimes_Q L$ if and only if D_0 and $D \otimes_Q L$ have precisely the same set of maximal subfields. A field K is a maximal subfield of $D \otimes_Q L$ if and only if $[K:L] = 2$ and -1 is a sum of two squares in K. As seen above, such fields split A and so are maximal subfields of D_0. Conversely, let $[K:L] = 2$, K a splitting field for A. We must show that -1 is a sum of two squares in K. If $K = L(\sqrt{-1})$ we are done, so assume $K \neq L(\sqrt{-1})$. Then $(K(\psi)/K, \sigma, -1) \sim K$ and so -1 is a norm from $K(\psi)$ to K. Since $K(\psi) \supset K(\sqrt{-1}) \supset K$, -1 is a norm from $K(\sqrt{-1})$ to K, proving that -1 is a sum of two squares in K. This proves that $D_0 \cong D \otimes_Q L$ and completes the proof of Theorem 2.

REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R. I., 1939. MR 1, 99.
2. M. Benard and M. Schacher, *The Schur subgroup*. II, J. Algebra 22 (1972), 378–385. MR 46 #1890.
3. B. Fein, *Embedding rational division algebras*, Proc. Amer. Math. Soc. 32 (1972), 427–429. MR 44 #6756.
4. B. Fein, B. Gordon and J. Smith, *On the representation of* -1 *as a sum of two squares in an algebraic number field*, J. Number Theory 3 (1971), 310–315.
5. B. Fein and T. Yamada, *The Schur index and the order and exponent of a finite group*, J. Algebra 28 (1974), 496–498.
6. D. Goldschmidt and I. Isaacs, *Schur indices in finite groups*, J. Algebra 33 (1975), 191–199.
7. L. Goldstein, *Analytic number theory*, Prentice-Hall, Englewood Cliffs, N. J., 1971.
8. G. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.
9. E. Witt, *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper*, J. Reine Angew. Math. 190 (1952), 231–245. MR 14, 845.
10. T. Yamada, *Characterization of the simple components of the group algebras over the p-adic number field*, J. Math. Soc. Japan 23 (1971), 295–310. MR 43 #4933.

DEPARTMENT OF MATHEMATICS, OREGON STATE UNIVERSITY, CORVALLIS, OREGON 97330