SCHUR INDICES AND SUMS OF SQUARES

BURTON FEIN¹

ABSTRACT. Let G be a finite group of exponent n, \( F \) a field of characteristic zero, \( \epsilon \) a primitive \( n \)-th root of unity, and suppose that the Sylow 2-subgroup of the Galois group of \( F(\epsilon) \) over \( F \) is cyclic. Let \( \chi \) 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 \( \chi \) 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 \( \text{Gal}(F(\sqrt[n]{\epsilon})/F) \) is cyclic. If \( 2 \mid |P| \), assume also that \( \sqrt{-1} \notin F \). 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 \( \sqrt{-1} \notin F \) 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 \( \text{Irr}(G) \). For \( \chi \in \text{Irr}(G) \), we denote the Schur index of \( \chi \) over \( F \) by \( m_F(\chi) \). \( \epsilon_n \) will denote a primitive \( n \)-th 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 \( \text{Gal}(F(\epsilon_n)/F) \) is cyclic and let \( \chi \in \text{Irr}(G) \). Then \( m_F(\chi) \) is odd.

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 \( \chi, m_L(\chi) \) 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 \( \sqrt{-1} \in E \) 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 \( \zeta \in \operatorname{Irr}(H) \) with the following properties:

(1) there is a normal subgroup \( N \) of \( H \) and a linear character \( \psi \) of \( N \) such that \( \zeta = \psi^H \);
(2) \( H/N \cong \operatorname{Gal}(L(\psi)/L) \);
(3) \( L(\zeta) = L \);
(4) \( m_L(\zeta) = 2 \);
(5) the simple component \( A \) of the group algebra of \( H \) over \( L \) corresponding to \( \zeta \) is isomorphic to the cyclic algebra \((L(\psi)/L, \sigma, \epsilon_s)\) where \( \langle \sigma \rangle = \operatorname{Gal}(L(\psi)/L) \) and \( \epsilon_s \in L \); and
(6) the simple component \( B \) of the group algebra of \( G \) over \( L \) corresponding to \( \chi \) 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 \( A' \sim (L(\psi)/L, \sigma, \epsilon_s') \sim L \), 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 \( A^2 \sim L(\psi)/L, (\sigma, \epsilon_s)^2 \) 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 \( \chi \) is similar to \( B \otimes_L LF \) and so \( B \otimes_L LF \not\subseteq LF \). By (5), \( A \otimes_L LF \not\subseteq LF \). Let \( D \) denote the usual quaternion algebra over \( Q \), i.e. \( D = (Q(\sqrt{-1})/Q, r, -1) \). 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 \( A \otimes_L LF \not\subseteq LF \) 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 \( \text{Gal}(\mathbb{Q}(\epsilon_n)/L) \) 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 \( K \) \([8, \text{Theorem } 4.5]\). 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 \((-1, K(\psi)/K)_n\) for any prime \( n \) of \( K \) \([7, \text{Chapter } 12, \text{§2}]\). \((-1, K(\psi)/K)_n = 1\) if and only if \(-1 \) is a local norm at \( n \) \([8, \text{Proposition } 3.11]\). We first consider extensions of \( 2 \).

Let \( n \) extend the rational prime \( 2 \). By \([4, \text{Theorem } 1]\), \([K_\pi : \mathbb{Q}_2]\) is even. We have

\[
(-1, K(\psi)/K)_n = (N_{K_\pi/\mathbb{Q}_2}(-1), Q(\psi)/Q)_2
\]

\[
= (-1, K(\psi)/K)_n = (1, Q(\psi)/Q)_2 = 1
\]

by \([7, \text{Proposition } 12-2-5]\). This \(-1 \) is a local norm at \( n \) for \( n \) extending \( 2 \).

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

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

Since \( p \equiv 1 \) (mod 4), \( \epsilon_4 \in \mathbb{Q}_p \) \([8, \text{Corollary } 3.7]\). 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 \([3, \text{Corollary } 2]\), \( D_0 \cong D \otimes_Q L \) 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 $(K(\sqrt{\psi})/K, \sigma, -1) \sim K$ and so $-1$ is a norm from $K(\sqrt{\psi})$ to $K$. Since $K(\sqrt{\psi}) \supset K(\sqrt{-1}) \supset K$, $-1$ is a norm from $K(\sqrt{-1})$ to $K$, proving that $-1$ is a sum of two squares in $K$. This proves that $D_0 \cong D \otimes \mathbb{Q} L$ and completes the proof of Theorem 2.

REFERENCES


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