ILLINOIS JOURNAL OF MATHEMATICS
Volume 42, Number 4, Winter 1998

# SQUARES OF CHARACTERS THAT ARE THE SUM OF ALL IRREDUCIBLE CHARACTERS

S. M. GAGOLA, JR. AND M. L. LEWIS

## 1. Introduction

We study here the structure of groups $G$ which possess an irreducible character $\chi$ with the property that $\chi^2$ is the sum of all the irreducible characters of $G$. (All groups considered here are finite, and by character we mean complex character, that is, the character afforded by a representation over the field of complex numbers.)

Previous to our present work, E. Abboud in [1] showed that $G$ is a split extension of an elementary abelian 2-group by an elementary abelian 3-group when $G'$ is assumed abelian. We are able to prove here:

(1.1) THEOREM. *If $G$ is a finite solvable group for which there exists an irreducible character $\chi$ such that $\chi^2 = \sum_{\psi \in \mathrm{Irr}(G)} \psi$, then $G$ is an internal direct product of copies of the symmetric group $S_3$.*

Certainly, Theorem (1.1) suggests that the hypotheses are fairly restrictive, at least for solvable groups. Other examples of this situation (already noted in [1]) are the groups $G = \mathrm{SL}_2(2^n)$ for all $n \geq 1$ where $\chi$ is the Steinberg character of degree $2^n$. Notice that the symmetric group $S_3$ occurs as the first term of this family, but the remaining members are all simple groups. It is easy to check that direct products of examples produce further examples. (Conversely, direct factors of examples also serve as examples.) In view of these examples, it seems natural to generalize Theorem (1.1) to $\mathcal{S}$-groups: groups all of whose nonsolvable composition factors are isomorphic to members of the collection $\mathcal{S} = \{\mathrm{SL}_2(2^n) \mid n \geq 2\}$. We obtain:

(1.2) THEOREM. *Let $G$ be a finite group for which there exists an irreducible character $\chi$ such that $\chi^2 = \sum_{\psi \in \mathrm{Irr}(G)} \psi$. If $G$ is an $\mathcal{S}$-group, then $G$ is an internal direct product $G = X_1 \dot{\times} \cdots \dot{\times} X_k$ of groups $X_i$ that are isomorphic to groups in the family $\{S_3\} \cup \mathcal{S}$.*

Notice that Theorem (1.1) is an immediate corollary of Theorem (1.2), as $S_3$ is the only solvable member of the family $\{S_3\} \cup \mathcal{S}$.

Received August 25, 1997.
1991 Mathematics Subject Classification. Primary 20C15.

Theorem (1.2) has been conjectured (in [1]) to hold for all groups.

In all known examples, the character $\chi$ is uniquely determined by its degree (which happens to be the largest power of 2 occurring as a character degree; it need not be the largest character degree). Is $\chi$ always unique? Is its degree always a power of 2? By an elementary argument counting involutions (not given here) it is possible to prove that the character necessarily has even degree.

There is a curious algebraic characterization of the situation considered in this paper. If $W$ is any $\mathbb{C}[G]$-module and $\mathcal{E} = \mathrm{End}_{\mathbb{C}[G]}(W)$ is its endomorphism ring of $\mathbb{C}[G]$-homomorphisms, then $\mathcal{E}$ is commutative if and only if the character afforded by $W$ is multiplicity free, and the natural homomorphism $\mathbb{C}[G] \longrightarrow \mathrm{End}_{\mathcal{E}}(W)$ is an isomorphism if and only if every irreducible character of $G$ appears as a constituent of the character afforded by $W$. In particular, if $\chi$ is an irreducible character afforded by the module $V$, then $\chi^2$ is the sum of all the irreducible characters of $G$ if and only if $\mathcal{E} = \mathrm{End}_{\mathbb{C}[G]}(V \otimes V)$ is commutative, and $\mathbb{C}[G] \longrightarrow \mathrm{End}_{\mathcal{E}}(V \otimes V)$ is an isomorphism. We do not, however, make use of this characterization here.

## 2. Preliminaries

When E. Abboud [1] first considers the situation of a group $G$ which has an irreducible character $\chi$ whose square is the sum of all the irreducible characters of $G$, he starts his analysis more generally by assuming that some potentially higher power $\chi^q$ (where $q$ is a prime) is the sum of all the irreducible characters of $G$. Under the additional hypothesis that the commutator subgroup $G'$ of $G$ is proper, he then proves that the exponent $q$ is 2 and that the factor group $G/G'$ is an elementary abelian 2-group. Our first result shows that only the square of an irreducible character can be the sum of all the characters, without any additional hypothesis on $G'$. In fact, we prove more: only the second power of an irreducible character can be multiplicity free. Recall that a character $\psi$ of a group $G$ is *multiplicity free* if the inner product $(\psi, \theta)$ is either 0 or 1 for all irreducible characters $\theta$ of $G$.

(2.1) LEMMA. *Let $\chi$ be a character of degree at least 2 of a group $G$, and let $m \geq 3$ be an integer. Then $\chi^m$ is not multiplicity free.*

*Proof.* Since $\chi^3$ is a direct factor of $\chi^m$, it suffices to prove only that $\chi^3$ is not multiplicity free. Let $V$ be a module affording $\chi$ so that the tensor product $V^3 = V \otimes V \otimes V$ affords $\chi^3$. Now the symmetric group $S_3$ acts on $V^3$ by "permuting the factors", and since we are assuming $\dim V = \chi(1) \geq 2$, this action by $S_3$ is faithful. Moreover, the action of $S_3$ commutes with the diagonal action by $G$, so that $S_3$ embeds in the group of units of the ring $\mathrm{End}_G(V^3)$, which is therefore not a commutative ring. Since a multiplicity free $\mathbb{C}[G]$-module has a commutative endomorphism ring, it follows that $V^3$ (and hence $\chi^3$) cannot be multiplicity free, as desired. $\square$

(2.2) COROLLARY. If $\chi$ is a character of $G$, a nontrivial group, and if some power $m \geq 2$ of $\chi$ is the sum of all the irreducible characters of $G$, then $m = 2$ and $\chi$ is irreducible.

*Proof.* Since $G$ is nontrivial, $\chi$ cannot be linear and $m = 2$ follows from the previous lemma. Clearly if $\chi$ reduces, say $\chi = \alpha + \beta$, then $\chi^2 = \alpha^2 + 2\alpha\beta + \beta^2$ is not multiplicity free. Hence $\chi$ must be irreducible. □

It is convenient now to codify the main situation of this paper:

HYPOTHESIS (*). *$G$ is a finite group, $\chi$ is an irreducible character of $G$ and* $\chi^2 = \sum_{\psi \in \mathrm{Irr}(G)} \psi$.

An immediate consequence of Hypothesis (*) is that $\chi$ is faithful, and it is easy to see that $\chi$ is real-valued (Theorem (2.4) below). Another consequence of this hypothesis is that the center of the group must be trivial. Lying slightly deeper is the fact that $\chi$ is afforded by a real representation.

Recall that the Frobenius-Schur indicator of an irreducible character $\chi$ of a group $G$, denoted by $\nu_2(\chi)$, is defined by the formula

$$\nu_2(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$$

and satisfies $\nu_2(\chi) \in \{-1, 0, 1\}$. Moreover, the specific values taken on by $\nu_2(\chi)$ indicate whether $\chi$ is real-valued and afforded by a real representation ($\nu_2(\chi) = 1$), is real-valued but not afforded by a real representation ($\nu_2(\chi) = -1$), or is not real-valued ($\nu_2(\chi) = 0$).

(2.3) LEMMA. *Let $G$ be a group and $\chi$ an irreducible character of $G$. Then $\chi\overline{\chi}$ is afforded by a real representation.*

*Proof.* Let $V$ be a $\mathbb{C}[G]$-module affording $\chi$ and set $W = \mathrm{Hom}_{\mathbb{C}}(V, V)$. Then $G$ acts on $W$ by conjugation (that is, $(f^g)(v) = f(vg^{-1})g$ for $f \in \mathrm{Hom}_{\mathbb{C}}(V, V)$, $g \in G$ and $v \in V$) and $W$ affords $\chi\overline{\chi}$. It remains to find an $\mathbb{R}$-subspace $U$ of dimension $\chi(1)^2$ that spans $W$ over $\mathbb{C}$ and which is invariant under conjugation by $G$.

By choosing a basis for $V$ over $\mathbb{C}$, we have $\mathrm{Hom}_{\mathbb{C}}(V, V) \cong \mathbb{C}^{n \times n}$ (space of complex $n \times n$ matrices where $n = \chi(1)$), and a basis can be found for which all matrices representing group elements are unitary (Theorem 4.17 of [7]). The $\mathbb{R}$-subspace of $n \times n$ Hermitian matrices is invariant under conjugation by unitary matrices, has dimension $n^2$, and spans $\mathbb{C}^{n \times n}$ over $\mathbb{C}$. The corresponding $\mathbb{R}$-subspace $U \leq W$ now satisfies the properties we want. □

(2.4) THEOREM. *Assume $(G, \chi)$ satisfies Hypothesis $(*)$. Then $\chi$ is real-valued and every real-valued irreducible character of $G$ has Frobenius-Schur indicator equal to $+1$.*

*Proof.* By assumption, $\chi^2 = \sum_{\psi\in\mathrm{Irr}(G)} \psi$. In particular, $1 = (\chi^2, 1_G) = (\chi, \overline{\chi})$, so $\chi$ is real-valued. Moreover, Lemma (2.3) guarantees that $\chi\overline{\chi} = \chi^2$ is afforded by a real representation. If $\psi$ is any real-valued character then the Schur index of $\psi$ over $\mathbb{R}$ divides $(\chi^2, \psi)$ (Corollary 10.2 (c) of [7]). Since this inner product equals 1 by Hypothesis $(*)$, $\psi$ is afforded by a real representation, and $\nu_2(\psi) = 1$ follows. □

For convenience, define $s(G)$ to be the sum of the degrees of all the irreducible characters of $G$ (counting multiplicity). Thus, $s(G) = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)$. The following result is well known.

(2.5) PROPOSITION. *Let $G$ be a group with exactly $t$ involutions. Then every irreducible character of $G$ is real-valued with Frobenius-Schur indicator equal to $+1$ if and only if $s(G) = t + 1$.*

*Proof.* By the standard Frobenius-Schur involution counting formula (Corollary 4.6 of [7]), $1 + t = \sum_{\chi\in\mathrm{Irr}(G)} \nu_2(\chi)\chi(1)$. Since $\nu_2(\chi) \leq 1$ holds for all $\chi$, the sum on the right is bounded above by the sum of all the irreducible character degrees, which is $s(G)$, and this bound is achieved if and only if $\nu_2(\chi) = +1$ for all $\chi \in \mathrm{Irr}(G)$. □

The last proposition, which allows for a computation of $s(G)$ by counting involutions, will not actually be needed until the final section. We use it there to observe that no sporadic simple group occurs as a homomorphic image of a group satisfying Hypothesis $(*)$.

## 3. Main results

If $\chi \in \mathrm{Char}(G)$ and $\theta \in \mathrm{Irr}(N)$ where $N \trianglelefteq G$, then "the projection of $\chi$ onto $\mathrm{Char}(G \mid \theta)$" is the sum $\sum_{\beta\in\mathrm{Irr}(G|\theta)} (\chi, \beta)\beta$. When $\theta$ is invariant, this projection operator commutes with induction in the sense that if $N \leq H \leq G$ and $\psi$ is a character of $H$, then $P_\theta(\psi)^G = P_\theta(\psi^G)$ where $P_\theta$ denotes the projection operator (defined on characters of $H$ and $G$).

If $\gamma \in \mathrm{Irr}(N)$ where $N \trianglelefteq G$, define $s(G \mid \gamma)$ as follows:

$$s(G \mid \gamma) = \sum_{\psi\in\mathrm{Irr}(T|\gamma)} \psi(1)/\gamma(1),$$

where $T = \mathcal{I}_G(\gamma)$. This is a refinement of the character degree sum $s(G)$ in the sense that $s(G) = s(G \mid 1_1)$ where $1_1$ denotes the principal character of the identity subgroup. Notice that $s(G \mid \gamma) = s(T \mid \gamma)$, and if $\gamma$ extends to an irreducible character of $T$ then $s(T \mid \gamma) = s(T \mid 1_N)$ is the sum of the character degrees of $T/N$ (counting multiplicities). This last fact follows easily from Gallagher's result [4] that says multiplication by an extension of $\gamma$ to $T$ is a bijection $\mathrm{Irr}(T \mid 1_N) \longrightarrow \mathrm{Irr}(T \mid \gamma)$. This also is Corollary (6.17) of [7]. Whether or not $\gamma$ extends to $T$, we have $|T : N| = \sum_{\psi\in\mathrm{Irr}(T|\gamma)}(\psi(1)/\gamma(1))^2 \geq \sum_{\psi\in\mathrm{Irr}(T|\gamma)} \psi(1)/\gamma(1) = s(T \mid \gamma)$. In particular, if $s(T \mid \gamma) = |T : N|$ then each $\psi \in \mathrm{Irr}(T \mid \gamma)$ is an extension of $\gamma$, and $T/N$ is necessarily abelian.

Our first result of this section, and its immediate corollaries, establish that some rather tight arithmetic restrictions must hold in every homomorphic image of a group satisfying Hypothesis $(*)$.

(3.1) PROPOSITION. *Assume $(G, \chi)$ satisfies Hypothesis $(*)$ and let $N \trianglelefteq G$. Write $\chi|_N = e(\theta_1 + \cdots + \theta_t)$ where the $\theta_i$ are the distinct irreducible Clifford conjugates of $\theta = \theta_1$. Let $T = \mathcal{I}_G(\theta)$ (so that $t = |G : T|$) and let $\psi \in \mathrm{Irr}(T)$ be the Clifford-correspondent of $\chi$. Set $A = \{\alpha \in \mathrm{Irr}(T/N) \mid (\overline{\psi}\psi, \alpha) \neq 0\}$, and $\sigma = \sum_{\alpha\in A} \alpha$. Then $\sigma(1) = e^2$ and $\sigma^G = \sum_{\beta\in\mathrm{Irr}(G/N)} \beta$. In particular, $s(G/N) = e^2 t$.*

*Proof.* By definition of $\psi$, $\psi|_N = e\theta$ and $\psi^G = \chi$. As already noted, $\chi$ is real-valued, so $\chi^2|_N = (\overline{\chi}\chi)|_N = e^2 \sum_i \theta_i\overline{\theta_i} + e^2 \sum_{i\neq j} \theta_i\overline{\theta_j}$, and from this it follows that $(\chi^2|_N, 1_N) = e^2 t$. By assumption, $\chi^2$ is the sum of all the irreducible characters of $G$, so projection onto $\mathrm{Char}(G|1_N)$ sends $\chi^2$ to $\sum_{\beta\in\mathrm{Irr}(G/N)} \beta$. It is now clear that the degree of $\sum_{\beta\in\mathrm{Irr}(G/N)} \beta$ is given by $s(G/N) = e^2 t$.

Since $\psi$ is the Clifford-correspondent of $\chi$ over $\theta$, it follows that $\overline{\psi}$ is the Clifford-correspondent of $\overline{\chi} = \chi$ over $\overline{\theta}$. Hence $\overline{\psi}^G = \chi$ and $\overline{\psi}|_N = e\overline{\theta}$, so that $\chi^2 = (\overline{\chi}\chi) = \overline{\psi}^G \chi = (\overline{\psi}\chi|_T)^G$. Now $\psi$ is the unique constituent of $\chi|_T$ that lies over $\theta$, and hence $\chi|_T$ may be written as $\psi + \zeta$ where $\zeta$ is a (possibly reducible) character of $T$, and $\zeta|_N = e(\theta_2 + \cdots + \theta_t)$. We now have $\chi^2 = (\overline{\psi}\chi|_T)^G = (\overline{\psi}\psi + \overline{\psi}\zeta)^G = (\overline{\psi}\psi)^G + (\overline{\psi}\zeta)^G$. Clearly, $((\overline{\psi}\zeta)|_N, 1_N) = (\zeta|_N, \psi|_N) = 0$, so no irreducible constituent of the character $\overline{\psi}\zeta$ belongs to $\mathrm{Irr}(T \mid 1_N)$. By commutativity of projection with induction, no irreducible constituent of $(\overline{\psi}\zeta)^G$ belongs to $\mathrm{Irr}(G \mid 1_N)$. Moreover, projection onto $\mathrm{Char}(T \mid 1_N)$ sends $\overline{\psi}\psi$ to $\tau = \sum_{\alpha\in A}(\overline{\psi}\psi, \alpha)\alpha$, while projection onto $\mathrm{Char}(G \mid 1_N)$ sends $\chi^2$ to $\sum_{\beta\in\mathrm{Irr}(G/N)} \beta$. By commutativity of operators again, we have $\tau^G = \sum_{\beta\in\mathrm{Irr}(G/N)} \beta$, and $\tau(1) = e^2$ by comparing degrees.

It remains to prove $\tau = \sigma$. The assertion that $\tau = \sigma$ is equivalent to saying that $\tau$ is multiplicity free. But this is the case as $\tau$ induces to a multiplicity free character of $G$. $\square$

(3.2) COROLLARY. *Assume $(G, \chi)$ satisfies Hypothesis $(*)$, and let $N$ be any normal subgroup of $G$. Then $s(G/N)$ divides $|G/N|^2$. In particular, every prime divisor of $s(G/N)$ is also a divisor of $|G/N|$.*

*Proof.* With the same notation as in Proposition (3.1), $s(G/N) = e^2t$ where $t = |G : T|$ and $e$ divides $|T : N|$. Hence $et$ divides $|G/N|$, and so $s(G/N)$ certainly divides $|G/N|^2$. □

(3.3) COROLLARY. *Assume $(G, \chi)$ satisfies Hypothesis $(*)$, and keep the same notation as in Proposition* (3.1). *If $\gamma \in \mathrm{Irr}(N)$ then $e^2 | s(G \mid \gamma)$. Moreover, if $\gamma$ is an irreducible constituent of $\theta_i\theta_j$ for some $i \neq j$ then $2e^2 \leq s(G \mid \gamma)$ and $\mathcal{I}_G(\gamma) > N$.*

*Proof.* Since $(G, \chi)$ satisfies Hypothesis $(*)$, $s(G \mid \gamma) = ((\chi^2)|_N, \gamma)$. Now $(\chi^2)|_N = e^2 \sum_i \theta_i^2 + 2e^2 \sum_{i<j} \theta_i\theta_j$ so that $((\chi^2)|_N, \gamma)$ is divisible by $e^2$, and is at least as large as $2e^2$ when $(\theta_i\theta_j, \gamma) \neq 0$ for some $i \neq j$. When this holds, $|\mathcal{I}_G(\gamma) : N| \geq s(G \mid \gamma) \geq 2e^2 > 1$. □

(3.4) COROLLARY. Assume $(G, \chi)$ satisfies Hypothesis $(*)$, and that $e$ has the same meaning as in Proposition (3.1). Then $e \neq 1$ implies that $\mathcal{I}_G(\gamma) > N$ for all $\gamma \in \mathrm{Irr}(N)$.

*Proof.* By the previous corollary, $|\mathcal{I}_G(\gamma) : N| \geq s(G \mid \gamma) \geq e^2 > 1$ for all $\gamma \in \mathrm{Irr}(N)$. □

We now use Proposition (3.1) and its corollaries to recover and extend what is known about $G'$ and $G''$ as determined in [1]. Recall that the *vanishing off subgroup* $\mathbf{V}(\chi)$ of a character $\chi$ (as defined on page 200 of [7]) is the (normal) subgroup generated by all group elements $g$ satisfying $\chi(g) \neq 0$.

(3.5) THEOREM. *Assume $(G, \chi)$ satisfies Hypothesis $(*)$. Then $\chi$ is induced from the commutator subgroup $G'$. The commutator factor group $G/G'$ is an elementary abelian 2-group and $G'/G''$ is an elementary abelian 3-group. Furthermore, every irreducible character of $G'$ extends to an irreducible character of its inertia group (and so, in particular, invariant characters of $G'$ extend to $G$). Finally, if $G'' \neq G'$ then $G$ maps homomorphically onto $S_3$.*

*Proof.* Since $\chi^2 = \sum_{\alpha \in \mathrm{Irr}(G)} \alpha$, it follows (as observed in [1]) that $\lambda\chi^2 = \chi^2$ for all characters $\lambda$ of degree 1. Hence $\mathbf{V}(\chi) = \mathbf{V}(\chi^2) \subseteq \ker(\lambda)$ for all $\lambda \in \mathrm{Irr}(G/G')$, which implies that $\mathbf{V}(\chi) \subseteq \bigcap_\lambda \ker(\lambda) = G'$. Let $N = G'$ in the situation of Proposition (3.1). With the notation of that proposition, $e^2t = s(G/G') = |G : G'|$, and this implies that $e^2 = |T : G'|$. However, $|T : G'| = \sum_{\beta \in \mathrm{Irr}(T|\theta)} (\beta(1)/\theta(1))^2 \geq (\psi(1)/\theta(1))^2 = e^2$. This implies that $\mathrm{Irr}(T \mid \theta)$ contains only $\psi$, and hence $\mathrm{Irr}(G \mid \theta)$ contains only $\chi$, by Clifford's Theorem. Corollary (3.3) now implies that $s(G \mid \theta) = e$ is divisible by $e^2$. Thus $e = 1$, $T = G'$ and $\psi = \theta$, so that $\chi = \theta^G$ is induced from $G'$. This proves the first assertion of the theorem.

If an odd prime $p$ divides $|G : G'|$, then let $K$ be a normal subgroup of $G$ having index $p$. Since $\chi$ is induced from $G'$, it is induced from $K$. Write $\chi|_K = \varphi_1 + \cdots + \varphi_p$ where the $\varphi_i$ are the distinct Clifford conjugates of $\chi|_K$. Let $\gamma$ be any irreducible constituent of $\varphi_1\varphi_2$. By Corollary (3.3) (with $N = K$ and the $\varphi_i$ replacing the $\theta_i$), $\gamma$ is necessarily invariant, so $s(G \mid \gamma) = p$. Since $p$ is odd, $G/K$ acts without fixed points on the collection of doubletons $\{\varphi_i, \varphi_j\}$. In particular, the $G/K$-orbit of $\{\varphi_1, \varphi_2\}$ has size $p$, so $p = s(G \mid \gamma) = (\chi^2|_N, \gamma) \geq 2(\sum_{i<j} \varphi_i\varphi_j, \gamma) \geq 2p$, a contradiction. This proves that $G/G'$ must be a 2-group.

If $G/G'$ is not elementary abelian, then choose $L \trianglelefteq G$ so that $G/L$ is cyclic of order four. As in the last paragraph, $\chi$ must be induced from $L$ and so $\chi|_L$ has 4 Clifford conjugates. Write $\chi|_L = \zeta_1 + \zeta_2 + \zeta_3 + \zeta_4$, where notation is chosen so that the $\zeta_i$ are cyclically permuted in order by a generator of $G/L$, say $gL$. Choose an irreducible constituent, say $\gamma$, of $\zeta_1\zeta_2$. By Corollary (3.3) (with the $\zeta_i$ replacing the $\theta_i$), $\mathcal{I}_G(\gamma) > L$ so that $g^2 \in \mathcal{I}_G(\gamma)$. Hence $\gamma$ is an irreducible constituent of $\zeta_3\zeta_4$ as well. Now $\gamma$ extends to $\mathcal{I}_G(\gamma)$ (as $\mathcal{I}_G(\gamma)/L$ is cyclic), so $|\mathcal{I}_G(\gamma) : N| = s(G \mid \gamma) = (\chi^2|_N, \gamma) \geq 2(\zeta_1\zeta_2, \gamma) + 2(\zeta_3\zeta_4, \gamma) \geq 4$. Therefore $\mathcal{I}_G(\gamma) = G$ and $\gamma$ is invariant. But this implies that $\gamma$ is a constituent of $\zeta_i\zeta_{i+1}$ for $i = 1, 2, 3, 4$ and recomputing the inner product yields $s(G \mid \gamma) \geq 8$, a contradiction. Hence $G/G'$ must be an elementary abelian 2-group.

We next prove extendibility of irreducible characters of $G'$ to their inertia groups. Let $\gamma$ be any irreducible character of $G'$, and let $\theta_1, \theta_2, \ldots, \theta_t$ denote the distinct Clifford conjugates of $\chi|_{G'}$. From the first paragraph, $\theta_1^G = \chi$, $\mathcal{I}_G(\theta_1) = G'$ (so that $t = |G/G'|$) and $G/G'$ acts regularly on $\{\theta_1, \theta_2, \ldots, \theta_t\}$. Since $\gamma$ is a constituent of $\chi^2|_{G'}$, $\gamma$ must appear either as a constituent of $\theta_l^2$ for some $l$, or as a constituent of $\theta_l\theta_m$ for some $l \neq m$. In the first case, as $\mathcal{I}_G(\gamma)/G'$ acts semi-regularly on the $\theta_i$, there are $|\mathcal{I}_G(\gamma) : G'|$ subscripts $l$ for which the corresponding $\theta_l^2$ contain $\gamma$ as a constituent, and so $s(G \mid \gamma) = (\chi^2|_{G'}, \gamma) \geq (\sum_i \theta_i^2, \gamma) \geq |\mathcal{I}_G(\gamma) : G'|$. This forces the equality $s(G \mid \gamma) = |\mathcal{I}_G(\gamma) : G'|$, and from the discussion following the definition of $s(G \mid \gamma)$, $\gamma$ extends to the inertia group $\mathcal{I}_G(\gamma)$.

Now suppose $\gamma$ is a constituent of $\theta_l\theta_m$ for some $l \neq m$. Let $H$ be the set-wise stabilizer of $\{\theta_l, \theta_m\}$ in $G$ and notice that $|H : G'| = 2$ as $G/G'$ is an elementary abelian 2-group that is regular on the $\theta_i$. Furthermore, $\gamma$ appears as a constituent of $(\theta_l\theta_m)^g$ for all $g \in H\mathcal{I}_G(\gamma)$. Hence, $s(G \mid \gamma) = (\chi^2|_{G'}, \gamma) \geq 2(\sum_{i<j} \theta_i\theta_j, \gamma) \geq 2|H\mathcal{I}_G(\gamma) : H| = 2|\mathcal{I}_G(\gamma) : \mathcal{I}_G(\gamma) \cap H|$. Now $\mathcal{I}_G(\gamma) \cap H$ can only be $G'$ or $H$, and the first possibility is impossible as $s(G \mid \gamma)$ cannot exceed $|\mathcal{I}_G(\gamma) : G'|$. Thus $H \subseteq \mathcal{I}_G(\gamma)$ and $s(G \mid \gamma)$ must equal $|\mathcal{I}_G(\gamma) : G'|$. As in the last paragraph, this forces the extendibility of $\gamma$ to $\mathcal{I}_G(\gamma)$.

At this point, all irreducible characters of $G'$ extend to their inertia groups, and in particular invariant characters extend to $G$.

Suppose 2 divides the index $|G' : G''|$. Then $M \trianglelefteq G$ can be chosen with $M \leq G'$ and $|G' : M| = 2$. If $1_{G'} \neq \mu \in \mathrm{Irr}(G'/M)$, then $\mu$ is necessarily invariant in $G$, and hence is extendible to $G$ by the previous paragraph. As $\mu$ is linear, any extension must lie over $1_{G'}$, and this contradicts $\mu \neq 1_{G'}$. Hence, $G'/G''$ has odd order.

View $G/G'$ as a group of operators for the abelian group $G'/G''$, and let $\overline{C} \neq 1$ be an indecomposable $G/G'$-summand of $G'/G''$. Every element $x$ of $G/G'$ either inverts or centralizes $\overline{C}$ (as $\overline{C} = C_{\overline{C}}(x) \dot{\times} [\overline{C}, x]$ by Fitting's Lemma, and the two factors are $G/G'$-invariant since $\langle x \rangle \trianglelefteq G/G'$). Hence, every subgroup of $\overline{C}$ is invariant under $G/G'$ proving that $\overline{C}$ must be cyclic. Write $G'/G'' = \overline{C} \times \overline{D}$ for $G/G'$-invariant $\overline{D} \leq G'/G''$. Of course $\overline{C} = C/G''$ and $\overline{D} = D/G''$ for corresponding subgroups $C$ and $D$ of $G'$ containing $G''$ (and normal in $G$). The centralizer $C_G(G'/D) = C_G(\overline{C})$ must be proper in $G$ as $C$ is contained in $G'$. As already noted, the action by each $x$ in $G/G'$ on $\overline{C}$ is either trivial or inversion, so $|G : C_G(\overline{C})| = 2$. As a result, $G$ maps homomorphically onto the dihedral group $D_{2m}$ of order $2m$ where $m = |\overline{C}|$ is odd. The group $D_{2m}$ has two linear characters and $\frac{m-1}{2}$ irreducible characters of degree 2, so that $s(D_{2m}) = 1 + 1 + \frac{m-1}{2} \cdot 2 = m + 1$. By Corollary (3,2), $s(D_{2m})$ must be a divisor of $|D_{2m}|^2 = 4m^2$, and this implies that $m = 3$ and $G$ maps onto $D_6 = S_3$.

By the last paragraph, every nontrivial indecomposable summand of $G'/G''$ is cyclic of order 3 (so that $G'/G''$ is an elementary abelian 3-group), and $G$ maps onto $S_3$ when $G'' \neq G'$. Theorem (3.5) is now completely proved. □

One of the conclusions of Theorem (3.5) is that irreducible characters of $G'$ extend to their inertia groups. It is convenient at this point to extend this property of $G'$ to all the subgroups of $G$ containing $G'$.

(3.6) LEMMA. *Let $N$ be a normal subgroup of the group $G$ and assume $G/N$ is abelian. If every irreducible character of $N$ extends to a character of its inertia group, then the same is true for every irreducible character of every subgroup of $G$ containing $N$.*

*Proof.* Let $M$ be a subgroup of $G$ containing $N$, fix $\gamma \in \operatorname{Irr}(M)$, and note that the hypotheses imply that $M$ is normal in $G$. Choose $\beta$, an irreducible constituent of $\gamma|_N$, and let $T = \mathcal{I}_G(\gamma)$ and $U = \mathcal{I}_T(\beta)$. Now $T$ permutes the irreducible constituents of $\gamma|_N$ and $M \leq T$ is a transitive subgroup so $T = MU$. By Clifford's Theorem, let $\varphi \in \operatorname{Irr}(U \cap M)$ be the Clifford correspondent of $\gamma$ over $\beta$. Choose also $\widehat{\varphi} \in \operatorname{Irr}(U \mid \varphi)$. Since $\beta$ extends to its inertia group, $\beta$ certainly extends to a character of $U$. Moreover, as $U/N$ is abelian, each element of $\operatorname{Irr}(U \mid \beta)$ is an extension of $\beta$. In particular $\widehat{\varphi}|_N = \beta$ and so $\widehat{\varphi}|_{U\cap M} = \varphi$.

Now $\widehat{\varphi}^T|_M = (\widehat{\varphi}|_{U\cap M})^M = \varphi^M = \gamma$, so $\gamma$ extends to $\widehat{\varphi}^T \in \operatorname{Irr}(T)$, as desired. □

Notice that Theorem (3.5) produced (when $G'' \neq G'$) a homomorphic image which also satisfies Hypothesis (∗). The next result establishes that Hypothesis (∗) holds for the normal subgroup as well, not only when the factor group is $S_3 \cong \mathrm{SL}_2(2)$, but also when the factor group is $\mathrm{SL}_2(2^n)$. Clearly, this will be useful in any inductive argument.

(3.7) THEOREM. *Let $(G, \chi)$ satisfy Hypothesis $(*)$, and let $N$ be a normal subgroup of $G$ satisfying $G/N \cong \mathrm{SL}_2(2^n)$ for some $n \geq 1$. Then $\chi|_N = 2^n \cdot \theta$ where $\theta \in \mathrm{Irr}(N)$ and $(N, \theta)$ satisfies Hypothesis $(*)$. Moreover, every $N$-conjugacy class is invariant under $G$, and every irreducible character of $N$ is invariant in $G$ and in fact extends to $G$.*

*Proof.* Write $\chi|_N = e(\theta_1 + \cdots + \theta_t)$ as in Proposition (3.1). By that result, $s(G/N) = e^2 t$. Now the complete character table of $\mathrm{SL}_2(2^n)$ is known (see, for example, Theorem 38.2 of Dornhoff's text [3]) and $s(\mathrm{SL}_2(2^n))$ is easily computed to be $2^{2n}$. In particular, $e$ and $t$ are powers of 2. Let $T = \mathcal{I}_G(\theta_1)$ so that $t = |G : T|$.

Write $t = 2^a$ and notice that $a \leq n$ as $t$ is a power of 2 dividing $|\mathrm{SL}_2(2^n)| = (2^n + 1) \cdot 2^n \cdot (2^n - 1)$. Then $e^2 = 2^{2n} t^{-1} = 2^{2n-a}$. However, $e$ must divide the index $|T : N|$, the 2-part of which is $2^{n-a}$, so that $2^{2n-a} = e^2 \leq 2^{2n-2a}$. This leads easily to $a = 0$, $t = 1$ and $e = 2^n$. In particular, $\theta = \theta_1$ is invariant in $G$.

We now argue that all $G$-invariant characters of $N$ extend to $G$. This certainly is true for $n \neq 2$ as the Schur multiplier of $\mathrm{SL}_2(2^n)$ is trivial. (A table of Schur multipliers may be found in the Atlas [2].) If $n = 2$, the multiplier has order 2, and a "representation group" for $G/N$ is $\mathrm{SL}_2(5)$. The degrees of the faithful irreducible characters of $\mathrm{SL}_2(5)$ are 2, 2, 4 and 6 so that if $\gamma \in \mathrm{Irr}(N)$ is invariant but $\gamma$ does not extend then $s(G \mid \gamma) = 2 + 2 + 4 + 6 = 14$. This contradicts Corollary (3.3) as $e^2 = 16$ does not divide 14.

At this point we know all invariant characters of $N$ extend to $G$, and in particular $\theta$ does. Let $\widehat{\theta}$ be an extension of $\theta$ to $G$ (when $n > 1$, $G/N$ is perfect and so $\widehat{\theta}$ is unique in this case). Now $\chi \in \mathrm{Irr}(G \mid \theta)$ so $\chi = \varphi\widehat{\theta}$ for some $\varphi \in \mathrm{Irr}(G/N)$. Notice that $\varphi$ has degree $2^n$ so that $\varphi$ must be the Steinberg character of $\mathrm{SL}_2(2^n)$. Since $\chi^2$ is multiplicity free, so is $\varphi^2$ and $\widehat{\theta}^2$. (In fact, $\varphi^2 = \sum_{\alpha \in \mathrm{Irr}(G/N)} \alpha$.) Define $B \subseteq \mathrm{Irr}(G)$ by $\widehat{\theta}^2 = \sum_{\beta \in B} \beta$. As $\chi^2$ is multiplicity free, the characters $\alpha\beta$ for $\alpha \in \mathrm{Irr}(G/N)$ and $\beta \in B$ are multiplicity free, disjoint, and sum to the sum of all the characters of $G$.

We now argue that $\beta|_N \in \mathrm{Irr}(N)$ for all $\beta \in B$, and that the restriction map $B \longrightarrow \mathrm{Irr}(N)$ is a bijection. Let $\gamma \in \mathrm{Irr}(N)$. As $\gamma$ is a constituent of $\chi^2|_N$, $\gamma$ must appear as an irreducible constituent of $(\alpha\beta)|_N$ for some $\alpha \in \mathrm{Irr}(G/N)$ and $\beta \in B$. But $(\alpha\beta)|_N = \alpha(1)\beta|_N$, so $\gamma$ is an irreducible constituent of $\beta|_N$. This proves $B \cap \mathrm{Irr}(G \mid \gamma) \neq \vee$ for all $\gamma \in \mathrm{Irr}(N)$.

Even though it is not yet known that $\alpha\beta \in \mathrm{Irr}(G)$ for all $\alpha \in \mathrm{Irr}(G/N)$ and $\beta \in B \cap \mathrm{Irr}(G \mid \gamma)$, we still have

$$\begin{aligned} s(G \mid \gamma) &= \sum_{\substack{\alpha \in \mathrm{Irr}(G/N) \\ \beta \in B \cap \mathrm{Irr}(G|\gamma)}} ((\alpha\beta)|_N, \gamma) = \sum_{\substack{\alpha \in \mathrm{Irr}(G/N) \\ \beta \in B \cap \mathrm{Irr}(G|\gamma)}} \alpha(1)(\beta|_N, \gamma) \\ &= 2^{2n} \sum_{\beta \in B \cap \mathrm{Irr}(G|\gamma)} (\beta|_N, \gamma) \geq 2^{2n} \, |B \cap \mathrm{Irr}(G \mid \gamma)| \geq 2^{2n}. \end{aligned}$$

Now $|\mathcal{I}_G(\gamma) : N| \geq s(G \mid \gamma) \geq 2^{2n}$ so $|G : \mathcal{I}_G(\gamma)| \leq (2^{2n} - 1)/2^n = 2^n - 1/2^n < 2^n$. However, the smallest degree of any nonprincipal character of

$\mathrm{SL}_2(2^n)$ is $2^n - 1$, so that any proper subgroup has index at least $2^n$. This forces $\mathcal{I}_G(\gamma) = G$ and $\gamma$ is invariant. We have already shown $G$-invariant characters of $N$ extend to $G$, and so $\gamma$ extends. Hence $s(G \mid \gamma) = s(G \mid 1_N) = s(G/N) = 2^{2n}$. In view of the displayed inequalities above, $B \cap \mathrm{Irr}(G \mid \gamma) = \{\beta\}$ consists of a unique character, and $(\beta|_N, \gamma) = 1$, so that $\beta$ is an extension of $\gamma$. At this point, every $\gamma \in \mathrm{Irr}(N)$ has a unique extension to $G$ which lies in $B$.

If $\beta \in B$, then select $\gamma \in \mathrm{Irr}(N)$ to be an irreducible constituent of $\beta|_N$, and let $\beta' \in B$ be the unique extension of $\gamma$ that lies in $B$. As $|B \cap \mathrm{Irr}(G \mid \gamma)| = 1$ is known, we conclude that $\beta = \beta'$ so $\beta|_N$ is irreducible. Hence, restriction $B \longrightarrow \mathrm{Irr}(N)$ does define a bijection.

Since every irreducible character of $N$ is invariant in $G$ (in fact is extendible to $G$) it follows by second orthogonality applied in $N$ that the $N$-conjugacy classes are stabilized by $G$.

Finally, $2^{2n}\theta^2 = \chi^2|_N = (\varphi^2\widehat{\theta^2})|_N = 2^{2n} \cdot \sum_{\beta\in B}(\beta|_N) = 2^{2n} \cdot \sum_{\gamma\in\mathrm{Irr}(N)} \gamma$, so $\theta^2 = \sum_{\gamma\in\mathrm{Irr}(N)} \gamma$ showing that $(N, \theta)$ satisfies Hypothesis $(*)$. □

Certain composition factors (namely, those of type $\mathrm{SL}_2(2^n)$ for $n \geq 2$) of a group satisfying Hypothesis $(*)$ must occur as a top composition factor in order to make good use of the last result. Our next goal is to show that these composition factors do in fact float to the top if they are not too far down. We begin with a result that will allow us to handle chief factors just below $G'$.

To state this result, we extend the definition of $s(G)$ to allow for operator groups. If $A$ is a group of operators for a group $G$ acting by automorphisms, then $A$ certainly permutes $\mathrm{Irr}(G)$. Let $\mathrm{Irr}_A(G)$ denote the set of $A$-fixed irreducible characters, and set $s_A(G) = \sum_{\chi\in\mathrm{Irr}_A(G)} \chi(1)$.

(3.8) PROPOSITION. *Let $X$ be a finite group, and suppose $N \trianglelefteq G$ where $N$ is a direct product of $k$ copies of $X$ and $G/N$ is an elementary abelian 2-group such that $G/N$ acts transitively on the given set of direct factors of $N$. Assume that the kernel $M$ of the action of $G$ on this set of direct factors satisfies $|M : N| \leq 2$ and that every irreducible character of $N$ extends to its inertia group in $G$. If $|M : N| = 1$ then $s(G) = s(X)^k + (k-1)|X|^{k/2}$, while if $|M : N| = 2$ then $s(G) = s(X)^k + s_M(X)^k + (2k-2)|X|^{k/2}$.*

*Proof.* Let $\alpha \in \mathrm{Irr}(N)$. Then $\alpha^G$ is multiplicity free, and we see that the sum of all the irreducible characters of $G$ is exactly $\sum \alpha^G$ as $\alpha$ runs over a set of representatives for the $G$-orbits on $\mathrm{Irr}(N)$. It follows that $s(G) = \sum \alpha(1)|G : N|/t_\alpha$, where the sum runs over $\alpha \in \mathrm{Irr}(N)$ and $t_\alpha$ is the size of the orbit of $\alpha$. Since $t_\alpha = |G : \mathcal{I}(\alpha)|$, where $\mathcal{I}(\alpha)$ is the inertia group of $\alpha$ (stabilizer of $\alpha$), this yields

$$s(G) = \sum_{\alpha\in\mathrm{Irr}(N)} \alpha(1)|\mathcal{I}(\alpha) : N| = \sum_{\alpha\in\mathrm{Irr}(N)} \left( \sum_{\substack{g\in G/N \\ \text{stabilizing } \alpha}} \alpha(1) \right) = \sum_{g\in G/N} \left( \sum_{\substack{\alpha\in\mathrm{Irr}(N) \\ \text{stabilized by } g}} \alpha(1) \right).$$

Now if $g = 1$, the inner sum above is $s(N) = s(X)^k$. If $g \notin M/N$, then $g$ has $k/2$ orbits of size two on the $k$ direct factors, since $G/M$ permutes the direct factors regularly. From each orbit choose one direct factor and let $N_1$ be the product of these $k/2$ direct factors. Then $N_2 = N_1^g$ is the product of the remaining factors, $N_2^g = N_1$, and $N = N_1 N_2 \cong N_1 \times N_2$. The irreducible characters of $N$ stabilized by $g$ have the form $\mu \times \mu^g$ for $\mu \in \mathrm{Irr}(N_1)$, and the corresponding inside sum is $\sum_{\mu \in \mathrm{Irr}(N_1)} \mu(1)^2 = |N_1| = |X|^{k/2}$.

When $M = N$, all elements of $G/N$ are accounted for. Each of the $k - 1$ nonidentity elements of $G/N$ contributes $|X|^{k/2}$ to the inner sum displayed, while we have already observed that the identity element contributes $s(X)^k$. The first formula for $s(G)$ now follows.

Now assume $|M : N| = 2$. Since $M \trianglelefteq G$ and $M$ normalizes each of the $k$ given direct factors, it follows (by transitivity) that each of these factors is isomorphic as an $M$-group. We may regard $X$ itself as one of these factors, and this is the sense in which $X$ admits an action by $M$ (so that $s_M(X)$ is defined). The nonidentity element of $M/N$ clearly contributes $s_M(N) = s_M(X)^k$ to the inner sum displayed. We have already seen that the $2k-2$ elements of $G/N$ not contained in $M/N$ contribute $|X|^{k/2}$ to the inner sum, while, of course, the identity element contributes $s(N) = s(X)^k$. The second formula for $s(G)$ now follows. □

It is clear that in the situation of Proposition (3.8) further expressions for $s(G)$ may be derived under more general assumptions concerning the factor group $M/N$. However, the case $|M : N| \leq 2$ is all that is needed for the next result, and the main result of the paper.

(3.9) THEOREM. *Let $(G, \chi)$ satisfy Hypothesis $(*)$. If the simple group $\mathrm{SL}_2(2^n)$ for $n \geq 2$ occurs as a homomorphic image of the commutator subgroup $G'$ of $G$, then it already occurs as a homomorphic image of $G$.*

*Proof.* Assume $G'$ maps onto $\mathrm{SL}_2(q)$ where $q = 2^n$ and $n \geq 2$. Then a $G$-chief factor $G'/L$ exists which is isomorphic to a direct product of a certain number of copies, say $k$, of $\mathrm{SL}_2(q)$. Let $K/L = C_{G/L}(G'/L)$ and $N = G'K$ so that $K$ and $N$ are normal subgroups of $G$ satisfying $K \cap G' = L$. By construction, $N/K$ is a $G$-chief factor isomorphic to $G'/L$, and $G/K$ is isomorphic to a subgroup of $\mathrm{Aut}(N/K)$. Notice that since $G' \leq N$, the quotient $G/N$ is an elementary abelian 2-group by an application of Theorem (3.5).

If $N = G$ then necessarily $k = 1$ and the theorem follows. Then assume for the remainder of the proof that $N < G$. A contradiction will be reached by showing that $s(G/K)$ does not divide $|G/K|^2$, contrary to Corollary (3.2).

Proposition (3.8) will be used to compute $s(G/K)$, so we next check that the hypotheses of this proposition are satisfied in the group $G/K$ (with $X = \mathrm{SL}_2(2^n)$). Notice that Theorem (3.5) implies that every irreducible character of $G'$ extends to a character of its inertia group. Lemma (3.6) now guarantees extendibility of irreducible characters of $N$ (and hence $N/K$) to their inertia groups.

Let $\overline{S} = S/K$ be one of the simple direct factors of $N/K$, and set $\mathcal{A} = \{\overline{S}^g \mid g \in G\}$. Then $\mathcal{A}$ is the complete set of simple direct factors of $N/K$. Also set $M = N_G(S)$ so that $|\mathcal{A}| = k = |G : M|$, as $G$ transitively permutes the direct factors of $\overline{N}$. Since $G' \leq N \leq M$ we have $M \trianglelefteq G$ and so $M = N_G(S^g)$ for all $g \in G$. Thus, $M$ is the kernel of the permutation action of $G$ on $\mathcal{A}$, and $G/M$ permutes the set $\mathcal{A}$ regularly. Similarly, if $C = S \cdot C_G(\overline{S})$ then $C$ is normal in $G$ as $N \leq C$, so $C = S^g \cdot C_G(\overline{S}^g)$ for all $g \in G$. Thus, $\overline{C}$ acts as a group of inner automorphisms of $\overline{N}$, and since $C_{\overline{G}}(\overline{N}) = \overline{1}$ we conclude that $\overline{C} = \overline{N}$ and so $C = N$. Notice that $M/N = M/C$ is isomorphic to a subgroup of $\mathrm{Out}(\overline{S})$, which is cyclic of order $n$ (represented by "field automorphisms" of $\mathrm{SL}_2(q)$). But $M/N$ is an elementary abelian 2-group so $|M/N| \leq 2$.

At this point we know the hypotheses of Proposition (3.8) are satisfied in the group $G/K$, and we consider, in turn, the two cases for the conclusion.

First, suppose that $M = N$. Then $k = |G : N| \geq 2$ and by Proposition (3.8),

$$s(G/K) = s(X)^k + (k-1)|X|^{k/2} = q^{2k} + (k-1) \cdot (q+1)^{k/2} q^{k/2} (q-1)^{k/2}.$$

Now Corollary (3.2) implies that this integer divides $|G/K|^2 = k^2 \cdot (q+1)^{2k} q^{2k} (q-1)^{2k}$. The largest power of 2 dividing $s(G/K)$ is $q^{k/2}$, so odd primes definitely divide $s(G/K)$. If $p$ is such a prime, then $p$ must also divide $|G/K|^2$ and so $p$ must divide $(q^2-1)$ (recall that $k$ is a power of 2). Considering the form of $s(G/K)$ displayed above, we easily get the contradiction $p \mid q^{2k}$ (recall that $q = 2^n$ is a power of 2).

Now suppose $|M : N| = 2$. We need to compute $s_M(N/K) = s_M(X)^k$.

If $g \in M - N$ then the action of $g$ is a proper outer automorphism on each of the direct factors of $\overline{N} = N/K$. Adjusting $\overline{g} = gK$ by an element of $\overline{N}$, the action of $\overline{g}$ on $\overline{N}$ is induced by a field automorphism of order 2, say $\alpha \longmapsto \alpha^{q_o}$ ($\alpha \in \mathrm{GF}(q)$) where $q_o = 2^{n/2}$. Notice that for an involutory field automorphism to exist, $n$ is necessarily even. We need to identify the irreducible characters of $\mathrm{SL}_2(q)$ fixed by this automorphism.

Certainly the principal character and the Steinberg character (the unique character of degree $q$) are fixed. The remaining characters have degree $q \pm 1$, and we need to identify the $g$-fixed characters among these. If $\chi$ has degree $q \pm 1$ then the value of $\chi$ at a fixed generator of a cyclic subgroup $C$ of order $q \mp 1$ has the form $\pm(\varepsilon + \varepsilon^{-1})$, where $\varepsilon$ is a $|C|$-root of 1, not necessarily primitive but $\varepsilon \neq 1$. The assignment $\chi \mapsto \{\varepsilon, \varepsilon^{-1}\}$ is a bijection from characters of degree $q \pm 1$ to the resulting $(|C|-1)/2$ pairs of $|C|$-roots of 1. Moreover, if $\chi \mapsto \{\varepsilon, \varepsilon^{-1}\}$ then $\chi^g \mapsto \{\varepsilon^{q_o}, \varepsilon^{-q_o}\}$ so fixed characters may be counted by counting fixed pairs of roots of 1.

First, suppose $\chi(1) = q-1$ (so that $|C| = q+1$). If $\varepsilon^{q_o} \in \{\varepsilon, \varepsilon^{-1}\}$ then $\varepsilon^{q_o \pm 1} = 1$, and so $\varepsilon^{q-1} = 1$, since $q_o \pm 1$ divides $q-1$. But $\varepsilon^{|C|} = \varepsilon^{q+1} = 1$ so $\varepsilon^2 = 1$ and then $\varepsilon = 1$ as $q+1$ is odd. This contradiction means that there are no $g$-fixed characters of degree $q-1$.

Finally, suppose $\chi(1) = q+1$ so that $|C| = q-1$. Then $\varepsilon^{q_o} \in \{\varepsilon, \varepsilon^{-1}\}$ if and only if $\varepsilon^{q_o \pm 1} = 1$ which is true if and only if $\varepsilon$ is in the subgroup of order $q_o + 1$ or $q_o - 1$ in the group of $(q-1)$-roots of 1. This determines $\frac{q_o}{2} + \frac{q_o - 2}{2} = q_o - 1$ pairs fixed under $g$, and hence there are exactly $q_o - 1$ characters of degree $q+1$ fixed under $g$. Adding degrees of $g$-fixed characters produces $s_M(X) = 1 + q + (q_o - 1)(q+1) = q_o(q+1)$, and $s_M(N/K) = q_o^k(q+1)^k$ follows from this.

At this point we have determined that

$$s(G/K) = q^{2k} + q_o^k(q+1)^k + (2k-2)\cdot(q+1)^{k/2}q^{k/2}(q-1)^{k/2}.$$

First, suppose $M = G$. Then $k = 1$ and the formula for $s(G/K)$ above reduces to

$$s(G/K) = q^2 + q_o(q+1) = q_o(q_o^3 + q_o^2 + 1).$$

By Corollary (3.2), this expression must divide $|G/K|^2 = 4\cdot(q+1)^2q^2(q-1)^2$. Since $\gcd(s(G/K), (q+1)(q_o+1)) = 1$ we conclude that $(q_o^3 + q_o^2 + 1)$ divides the smaller integer $(q_o - 1)^2$, clearly a contradiction.

It remains to consider $N < M < G$ where $|G : M| = k > 1$ is a power of 2. By Corollary (3.2) again, $s(G/K)$ must divide $|G/K|^2 = 4k^2\cdot(q+1)^{2k}q^{2k}(q-1)^{2k}$. Recall that $q = q_o^2$ and $k$ are powers of 2. Removing the factor $q_o^k$ from $s(G/K)$ (which is the full power of 2 dividing $s(G/K)$) yields an odd integer that is easily seen to be congruent to 3 modulo 4. Let $p$ be an odd prime dividing $s(G/K)$ which satisfies $p \equiv 3 \pmod 4$. As $\gcd(s(G/K), q+1) = 1$ and $p$ must divide $|G/K|^2$, we conclude $p \mid (q-1)$. Hence $q \equiv 1 \pmod p$, and since $k$ is even and $q = q_o^2$ we also have $q_o^k \equiv 1 \pmod p$. Therefore $0 \equiv s(G/K) \equiv q^{2k} + q_o^k\cdot(q+1)^k + 0 \equiv 1 + 1\cdot 2^k + 0 \equiv 1 + 2^k \pmod p$. Now $k$ is a power of 2, so the congruence $2^k \equiv -1 \pmod p$ implies that the order of 2 in the multiplicative group of nonzero residues modulo $p$ is exactly $2k$. In particular $2k$ must divide $p-1$, which contradicts $p \equiv 3 \pmod 4$. □

All the machinery is now in place for the proof of the main result of this paper (Theorem (1.2)).

*Proof of Theorem* (1.2). Assume that $(G, \chi)$ satisfies Hypothesis $(*)$ where $G$ is an $\mathcal{S}$-group.

We first argue that $G$ maps homomorphically onto at least one group in the collection $\{S_3\} \cup \mathcal{S}$. This is certainly the case if $G'' < G'$ by applying Theorem (3.5). If $G'' = G'$ then $G'$ maps onto some nonabelian simple group $X$, and by hypothesis, $X$ is isomorphic to a group in $\mathcal{S}$. An application of Theorem (3.9) now yields that $X$ is a homomorphic image of $G$. In any case, there exists $N \trianglelefteq G$ such that $G/N$ is isomorphic to $\mathrm{SL}_2(2^n)$ for some $n \geq 1$. If $N = 1$ we are finished, so assume $N \neq 1$.

By Theorem (3.7), $\chi|_N = 2^n\cdot\theta$ where $\theta \in \mathrm{Irr}(N)$ and $(N, \theta)$ satisfies Hypothesis $(*)$. By induction, $N = X_1 \dot{\times} \cdots \dot{\times} X_m$ where each $X_i$ is isomorphic to a member of $\{S_3\} \cup \mathcal{S}$. Theorem (3.7) also guarantees that each $N$-class is invariant under conjugation in $G$, so each $X_i$ is in fact a normal subgroup of $G$. It remains to prove that $N$ has a normal complement. This is the case if the action of $G$ on each $X_i$ is as a group of inner automorphisms, because then $G = C_G(N) \cdot N$ and $C_G(N) \cap N = Z(N) = 1$.

Since $S_3$ is a complete group, $G$ acts as a group of inner automorphisms on each $X_i$ for which $X_i \cong S_3$. Moreover, if $X_i \in \mathcal{S}$ then (because $\mathrm{Out}(X_i)$ is cyclic and $G/N$ is not) the natural map $G \longrightarrow \mathrm{Out}(X_i)$ has kernel $X_iC_G(X_i)$ satisfying $X_iC_G(X_i) > N$. If $G/N \in \mathcal{S}$ then $G/N$ is nonabelian simple so that $G = X_iC_G(X_i)$ and we are finished. It remains to show that when $G/N \cong S_3$ then $|G : X_iC_G(X_i)|$ cannot be 2. If $|G : X_iC_G(X_i)| = 2$ then there exists an element $x \in G - X_iC_G(X_i)$ which acts on $X_i$ as the nontrivial field automorphism of order 2. In particular, $X_i$ is isomorphic to $\mathrm{SL}_2(2^n)$ for some even integer $n$. However, the stated automorphism definitely acts nontrivially on the conjugacy classes of $X_i$: if $g \in X_i$ has order $2^n + 1$ then $g^x$ is not conjugate to $g$ in $X_i$ (compare eigenvalues). In all cases then $G = X_iC_G(X_i)$. □

As already noted, Theorem (1.1) is an immediate corollary of Theorem (1.2).

## 4. Some extensions

Do there exist examples of groups satisfying Hypothesis $(*)$ which are not $\mathcal{S}$-groups? If this is the case, then Theorems (3.5), (3.7) and (3.9) imply that an example $G$ exists which has a nonabelian simple group different from $\mathrm{SL}_2(2^n)$ $(n \geq 2)$ occurring as a homomorphic image of either $G$ or $G'$.

Some simple groups can be eliminated as a homomorphic image of $G$ by applying Theorem (2.4). For example, any simple group which has a real-valued irreducible character with Frobenius-Schur indicator equal to $-1$ is eliminated by that theorem. A glance at the Atlas [2] shows that the McLaughlin group $M^cL$ is one example of this.

If $X$ is a simple group for which $s(X)$ can readily be computed, and $s(X)$ is divisible by a prime not dividing the order of $X$, then $X$ is eliminated as a top composition factor by Corollary (3.2). This happens for all the remaining sporadic simple groups with the exception of $s(M_{23}) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$. However, the Mathieu group $M_{23}$ does not have a subgroup of index $2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$ or $3 \cdot 5 \cdot 7 \cdot 23$. (The order of such a subgroup $H$ is $11 \cdot 2^7 \cdot 3$ or $11 \cdot 2^5 \cdot 3$. A Sylow 11-normalizer in $M_{23}$ has order $11 \cdot 5$ and so $H$ would have to be a Frobenius group with Frobenius complement having order 11, clearly a contradiction.)

A useful observation that simplifies the computation of $s(X)$ for a (simple) group $X$ in which all real-valued characters have Frobenius-Schur indicator equal to $+1$ is that

$$s(X) = 1 + t + \sum_{\chi \text{ nonreal}} \chi(1)$$

where $t$ is the number of involutions, and the sum extends over all irreducible characters $\chi$ that are not real-valued. In the case of the sporadic simple groups, there are at most 4 classes of involutions, and the largest number of complex conjugate pairs of irreducible characters occurring in the sum is 22. (This occurs for the Monster group, but typically the number of complex conjugate pairs is much smaller; the next worse case is 9 such pairs occurring in Thompson's group $Th$.)

Although not considered sporadic, the group ${}^2F_4(2)'$ is also eliminated from occurring as a top composition factor of a group satisfying Hypothesis $(*)$ because $s({}^2F_4(2)')$ is divisible by the prime 1783 which does not divide the order of ${}^2F_4(2)'$.

The discussion above shows that no sporadic simple group occurs as a homomorphic image of a group satisfying Hypothesis $(*)$. To eliminate other families, it appears useful to compute $s(X_n(q))$ explicitly as a function of $q$ where $X_n(q)$ denotes a simple group corresponding to a fixed Lie algebra type $X$ of rank $n$, the parameter $q$ corresponding to the choice of finite field. In the rank one case, $X_n(q)$ is $\mathrm{PSL}_2(q)$, and the entire character table is known. (For example, Theorems 38.1 and 38.2 of [3] construct character tables for $\mathrm{PSL}_2(q)$ for $q$ odd and $q$ a power of 2, respectively.) Using the tables, it is straightforward to sum degrees to get $s(\mathrm{PSL}_2(q)) = q^2$, $(q^2+q+2)/2$ and $q(q+1)/2$ when $q$ is even, $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, respectively. This certainly suggests that $s(X_n(q))$ is a polynomial in $q$ on residue classes. This has in fact been checked by D. White using the program CHEVIE for the groups

$$\mathrm{PSL}_2(q),\quad \mathrm{PSL}_3(q),\quad \mathrm{Sp}_4(2^n),\quad \mathrm{Sp}_6(2^n),\quad \mathrm{G}_2(q)$$

and the twisted types

$$\mathrm{PSU}_3(q),\quad \mathrm{Sz}(2^{2m+1}),\quad {}^3\mathrm{D}_4(q),\quad {}^2\mathrm{G}_2(3^{2m+1}).$$

We end this paper by considering only the first family listed above, namely the simple linear fractional groups $\mathrm{PSL}_2(q)$. For even $q$, the groups satisfy Hypothesis $(*)$, and it seems natural to decide the status of the remaining members of that family (when $q$ is odd). Of course, because $\mathrm{PSL}_2(3) \cong A_4$ is not simple, and $\mathrm{PSL}_2(5) \cong A_5 \cong \mathrm{SL}_2(4)$, we need only consider $q > 5$. Our final result shows that these groups do not occur as top composition factors of groups satisfying Hypothesis $(*)$.

(4.1) PROPOSITION. Assume $(G, \chi)$ satisfies Hypothesis $(*)$, and let $q > 5$ be a power of an odd prime. Then $\mathrm{PSL}_2(q)$ is not a homomorphic image of $G$.

*Proof.* Suppose $N \trianglelefteq G$ and $G/N$ is isomorphic to $\mathrm{PSL}_2(q)$. As already noted above, $s(G/N) = (q^2+q+2)/2$ when $q \equiv 1 \pmod 4$ and $s(G/N) = q(q+1)/2$ when $q \equiv 3 \pmod 4$. The first case is easily ruled out by Corollary (3.2) as $q > 5$. Then assume $q \equiv 3 \pmod 4$. Using the notation of Proposition (3.1), we have $e^2t = q(q+1)/2$. Notice, $q$ must be an odd power of a prime $p \equiv 3 \pmod 4$, so $p$ must divide the square-free part of $e^2t$. Hence $p \mid t = |G : T|$.

Suppose $q \nmid t$. Then $p \mid e$ and the $p$-part of $|\overline{T}| = |T/N|$ is the square of the $p$-part of $e$. Let $\overline{P} = P/N \in \mathrm{Syl}_p(\overline{T})$ so that $|\overline{P}|$ is a square. Since the Sylow $p$-subgroups of $G/N$ are elementary abelian, the same is true of $\overline{T}$. In particular, $\overline{P}$ is noncyclic.

If $\overline{T}$ is $p$-solvable, its $p$-length must be 1 since $\overline{P}$ is abelian. Let $\overline{1} \leq \overline{U} = \mathrm{O}_{p'}(\overline{T}) \leq \overline{U}\,\overline{P} = \mathrm{O}_{p',p}(\overline{T}) \leq \overline{T} = \mathrm{O}_{p',p,p'}(\overline{T})$ be the $p$-series of $\overline{T}$. Since $\overline{P}$ is noncyclic, $\overline{U}$ is generated by the subgroups $C_{\overline{U}}(\overline{x})$ for $\overline{x} \in \overline{P} - \overline{1}$. (This generation property of centralizers follows, for example, by an application of Theorem 5.3.16 of [5] applied to each of the Sylow subgroups of $\overline{U}$.) But the centralizer of any $p$-element in $\mathrm{PSL}_2(q)$ is a $p$-subgroup (in fact, a Sylow $p$-subgroup of $\mathrm{PSL}_2(q)$), so $\overline{U} = \overline{1}$. Hence $\overline{P} \trianglelefteq \overline{T}$.

Select $\overline{Q} \in \mathrm{Syl}_p(\overline{G})$ with $\overline{P} \leq \overline{Q}$ so that $\overline{P} = \overline{T} \cap \overline{Q}$. Since $\overline{Q}$ is known to be a TI-set in $\overline{G}$ (that is $\overline{Q} \cap \overline{Q}^g = \overline{1}$ if $\overline{Q} \neq \overline{Q}^g$) we conclude $\overline{T} \leq N_{\overline{G}}(\overline{P}) \leq N_{\overline{G}}(\overline{Q})$. However, $t = |\overline{G} : \overline{T}|$ divides $e^2 t = (q+1)q/2$ so $(q-1)$ divides $|\overline{T}|$. This contradicts $|N_{\overline{G}}(\overline{Q})| = \frac{q-1}{2} \cdot q$, and thereby proves that $\overline{T}$ is not $p$-solvable.

The subgroups of $\mathrm{PSL}_2(q)$ were classified by Dickson, and this result can be found in Huppert's text [6] (see Hauptsatz II.8.27). The non $p$-solvable subgroups occurring in that classification are: $A_5$ (when $p \in \{3, 5\}$), $\mathrm{PSL}_2(q_o)$, and $\mathrm{PGL}_2(q_o)$, where $q$ is a power of $q_o$. For the last case to occur, $q$ must be an even power of $q_o$, and this is eliminated as $q \equiv 3 \pmod 4$. If $\overline{T} \cong \mathrm{PSL}_2(q_o)$, then the $p$-part of the order of $\overline{T}$ is $|\overline{P}| = q_o$, which is a perfect square. Since $q$ is a power of $q_o$, this forces $q$ itself to be a perfect square, contradicting again the above congruence on $q$. Finally, $\overline{T}$ cannot be $A_5$ because the odd primes 3 and 5 divide the order of $A_5$ only to the first power. This contradiction proves then that $q$ must, in fact, divide $t$.

At this point, we have $q \mid t$, so $\overline{T}$ is a $p'$-subgroup of $\mathrm{PSL}_2(q)$. Since Brauer characters of $p'$-groups can be lifted, $\overline{T}$ occurs as a subgroup of $\mathrm{PSL}_2(\mathbb{C})$. These subgroups have been classified by Dickson as well (see Theorem 14.23 of [7]). From the classification of finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$, $\overline{T}$ contains an abelian subgroup of index 2, or else $\overline{T}$ is one of $A_4$, $S_4$ or $A_5$.

First, suppose $\overline{T}$ contains an abelian subgroup of index 2. Now the odd integer $\frac{q-1}{2}$ divides $|\overline{T}|$, so $\overline{T}$ contains an abelian subgroup $\overline{K}$ of order $\frac{q-1}{2}$. In $\overline{G} \cong \mathrm{PSL}_2(q)$, the subgroup $\overline{K}$ is the centralizer of each of its nonidentity elements, so $\overline{K}$ must have index exactly 2 in $\overline{T}$, and $|\overline{T}| = q-1$. Hence $t = (q+1)q/2$ and $e = 1$. Let $A$ and $\sigma$ be as in Proposition (3.1). Clearly from the description of $A$ we have $1_T \in A$. Then necessarily $\sigma = 1_T$ as $\sigma(1) = e = 1$ and $1_T$ is a constituent of $\sigma$. Hence $(1_T)^G = \sum_{\beta \in \mathrm{Irr}(G/N)} \beta$. However, if $\beta \in \mathrm{Irr}(G/N)$ is any character of degree $q-1$, then $\beta(u) = \pm 2$ for any involution $u$ of $G/N$ (both possibilities for the sign occur if $q > 7$) and $((1_T)^G, \beta) = (1_T, \beta|_T) = 1 + \frac{1}{2}\beta(u) \in \{0, 2\}$. This contradiction means that $\overline{T}$ must in fact be one of $A_4$, $S_4$ or $A_5$. Notice that $\frac{q-1}{2}$ is a nontrivial odd divisor of $|\overline{T}|$, so $\frac{q-1}{2} = 3, 5$ or $15$ and this leads to $q = 7, 11$ or $31$.

When $q$ is 11 or 31 then 5 necessarily divides $|\overline{T}|$ so $\overline{T} \cong A_5$. Also, $t = |\overline{G} :$

$\overline{T}| = \frac{(q+1)q(q-1)}{120}$, and $e^2t = \frac{q(q+1)}{2}$. Then solving for $e^2$ yields $e^2 = \frac{60}{q-1} \in \{6, 2\}$, and this contradiction leads to the final case $q = 7$.

When $q = 7$ then $e^2t = \frac{q(q+1)}{2} = 28$, so $e$ is either 1 or 2. If $e = 1$ then $t = 28$ and so $|\overline{T}| = \frac{|\overline{G}|}{28} = 6$, contradicting $|\overline{T}| \in \{12, 24, 60\}$. Hence $e = 2$, $t = 7$ and $|\overline{T}| = \frac{|\overline{G}|}{7} = 24$. Thus, $\chi|_N$ has the form $2(\theta_1 + \cdots + \theta_7)$. The final contradiction will be obtained by analyzing $s(G \mid \gamma)$ for certain $\gamma \in \mathrm{Irr}(N)$.

Suppose $\gamma$ is an irreducible constituent of the product $\theta_1\theta_2$, and let $H = \mathcal{I}_G(\gamma)$. Then Corollary (3.3) implies that $|H : N| \geq s(G \mid \gamma) \geq 2e^2 = 8$. The only possibilities for $|H/N|$ are 8, 12, 21, 24 and 168. The possibilities for $s(G \mid \gamma)$ can be worked out in each case. When $\gamma$ extends to $H$ we have $s(G \mid \gamma) = s(H \mid \gamma) = s(H/N)$. Except for the case $|H/N| = 21$, the Schur multiplier of $H/N$ has order 2, and when $\gamma$ fails to extend to $H$, $s(G \mid \gamma) = s(H \mid \gamma)$ is the sum of the degrees of the faithful irreducible characters of a representation group for $H/N$. (This sum happens to coincide with $s(H/N)$ when $|H/N| = 12$ or 168.) The result is that $s(G \mid \gamma)$ is an element of $\{6, 4\}$, $\{6\}$, $\{9\}$, $\{10, 8\}$ or $\{28\}$ corresponding to each of the five possibilities for $|H/N|$, respectively. Now, in addition to $s(G \mid \gamma) \geq 8$, Corollary (3.3) also requires $e^2 = 4$ to divide $s(G \mid \gamma)$, and this rules out the first three cases. Moreover, when $|H/N| = 24$, then $s(G \mid \gamma) = 8$.

Suppose $|H/N| = 24$ so that $H/N \cong S_4$. There are two conjugacy classes of subgroups of $\mathrm{PSL}_2(7)$ that are isomorphic to $S_4$. If $H$ is conjugate to $T$, then the orbits of $H$ on $\{\theta_1, \ldots, \theta_7\}$ have sizes 1 and 6. If $H$ is not conjugate to $T$ then the orbit sizes are 3 and 4. In any case then, $H$ does not stabilize $\{\theta_1, \theta_2\}$ so that $\gamma$ is a constituent of some other product $\theta_l\theta_m$. Hence, $8 = s(G \mid \gamma) \geq 2e^2(\sum \theta_i\theta_j, \gamma) \geq 8 + 8$, a contradiction.

The previous paragraph has just determined that each irreducible constituent $\gamma$ of $\theta_1\theta_2$ is $G$-invariant. We have seen that for invariant $\gamma$, $s(G \mid \gamma) = 28$. However, $G$ acts doubly transitively on $\{\theta_1, \ldots, \theta_7\}$ so that $\gamma$ is an irreducible constituent of *each* $\theta_i\theta_j$. But then $28 = s(G \mid \gamma) \geq 2e^2(\sum \theta_i\theta_j, \gamma) \geq 8 \cdot 21 = 168$, the final contradiction. □

It is amusing to note that if $T$ is a subgroup of $\mathrm{PSL}_2(7)$ that is isomorphic to $S_4$, then a reducible character $\sigma$ of $T$ can be found which satisfies $\sigma^{\mathrm{PSL}_2(7)} = \sum_{\beta \in \mathrm{Irr}(\mathrm{PSL}_2(7))} \beta$. In fact, if $\pi = 1_T + \psi$ is the permutation character of $T \cong S_4$ corresponding to the natural action on 4 points, then $\det(\psi) = \lambda$ is the sign character, and $\sigma = 1_T + \lambda \cdot \psi$ is the unique character of $T$ which works.

*Acknowledgement.* We are grateful for the timely, detailed and perceptive review made by the referee of this paper. He suggested proofs of Lemmas 2.1 and 2.3 more elegant than we had in the original paper. Moreover, Proposition 3.8 is both conceptually simpler, and more general than our original approach. This lemma to Theorem 3.9 made it possible to remove a fairly involved and somewhat messy involution count that appeared in the original proof of that theorem, an argument which we are happy to dispense with.

## REFERENCES

1. E. Abboud, *Exploring the structure of a finite group given an equation in its irreducible characters*, preprint.
2. J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *The atlas of finite groups*, Oxford University Press, New York, 1985.
3. L Dornhoff, *Group representation theory, Part A*, Marcel Dekker, New York, 1971
4. P. X. Gallagher, *Group characters and normal Hall subgroups*, Nagoya Math. J. **21** (1962), 223–230.
5. D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968.
6. B. Huppert, *Endliche Gruppen, I*, Springer-Verlag, Berlin, 1967.
7. I. M. Isaacs, *Character theory of finite groups*, Academic Press, San Diego, 1976.

Mathematics Department, Kent State University, Kent, OH 44242
gagola@mcs.kent.edu
lewis@mcs.kent.edu