EXISTENCE OF NONZERO TRACE-ZERO IDEMPOTENTS IN THE GROUP ALGEBRAS OF FINITE GROUPS

WENHUA ZHAO AND DAN YAN

Abstract. Let $G$ be a finite group and $K$ a splitting field of $G$ of characteristic $p > 0$. Denote by $KG$ the group algebra of $G$ over $K$ and $Z(KG)$ the center of $KG$. Let $V_G$ be the $K$-subspace of trace-zero elements of $KG$. We give some numerical sufficient and necessary conditions for $V_G$ and $V_G \cap Z(KG)$, respectively, to be Mathieu subspaces of $KG$ in terms of the degrees of irreducible representations of $G$ over $K$. The same numerical conditions also characterize the finite groups $G$ that $KG$ has no nonzero trace-zero idempotents and the finite groups $G$ that $KG$ has no nonzero central trace-zero idempotents, respectively.

1. Motivations and the Main Results

Let $G$ be a finite group, $K$ a splitting field of $G$ (unless stated otherwise) and $KG$ (or $K[G]$) the group algebra of $G$ over $K$. Denote by $1_G$, or simply 1, the identity element of $G$ and $KG$. We denote by $Z(KG)$ and $V_{KG}$, or simply by $V_G$ if the base field $K$ is clear in context, the center of $KG$ and the $K$-subspace of $KG$ spanned over $K$ by all $1 \neq g \in G$, respectively. An element $e \in KG$ is said to be an idempotent if $e^2 = e$, and a non-trivial idempotent if $e$ is an idempotent and $e \neq 1$ or 0.

For each $u \in KG$, denote by $tr_G u$, or $tr u$ if $KG$ is clear in context, the trace of $u$ (i.e., the coefficient of $1_G$ in $u$). An element $v \in KG$ is said to be trace-zero if $tr u = 0$ and trace-one if $tr u = 1$. Hence, the subspace $V_G$ defined above is just the subspace of trace-zero elements of $KG$.

Date: August 09, 2022.

2000 Mathematics Subject Classification. 16S34, 20C05, 16D99, 20C20.

Key words and phrases. Mathieu subspace (Mathieu-Zhao space); group algebras of finite groups; trace-zero idempotents.

The first author has been partially supported by the Simons Foundation grant #278638. The second author is supported by the NSF of China (Grant No. 11871241; 11601146), the China Scholarship Council and the Construct Program of the Key Discipline in Hunan Province.
Since an element $e$ is a trace-zero idempotent of $KG$, if and only if $1 - e$ is a trace-one idempotent of $KG$, all the results derived in this paper on trace-zero idempotents of $KG$ can be transformed in the obvious ways to the results on trace-one idempotents of $KG$.

The purpose of this paper is twofold. The first one is to find some numerical sufficient and necessary conditions in terms of the degrees of irreducible representations of $G$ over $K$ for that $KG$ has no nonzero trace-zero idempotents and that $KG$ has no nonzero central trace-zero idempotents, respectively.

To explain the second purpose of the paper, we need to recall the following concept that was introduced by the first author in [Z2] and [Z3].

**Definition 1.1.** Let $R$ be a commutative ring and $A$ a unital $R$-algebra. An $R$-subspace $V$ of $A$ is said to be a Mathieu subspace (MS) of $A$ if for all $a, b, c \in A$ with $b^m \in V$ for all $m \geq 1$, there exists $N \in \mathbb{N}$ (depending on $a, b$ and $c$) such that $ab^mc \in V$ for all $m \geq N$.

A Mathieu subspace is also called a Mathieu-Zhao space or Mathieu-Zhao subspace in the literature (e.g., see [EKC, DEZ]). The introduction of Mathieu subspaces was directly motivated by the Mathieu Conjecture [Mat] and the Image Conjecture [Z1], which both imply the famous Jacobian conjecture [Ke, BCW, E]. Note that all ideals are Mathieu subspaces, but not conversely. Therefore, the concept of Mathieu subspaces can be viewed as a natural generalization of the concept of ideals.

One of the most fundamental theorems in the theory of Mathieu subspaces is the Duistermaat and van der Kallen theorem [DK] which was proved in 1998. It solves the abelian case of the Mathieu Conjecture. The theorem in terms of group algebras and Mathieu subspaces can be essentially restated as follows.

**Theorem 1.2.** Let $G = \mathbb{Z}^n$ (the free abelian group of rank $n$). Then $V_G$ is a MS of $CG$. In terms of $K$-algebra of Laurent polynomials $\mathbb{C}[x^{-1}, x]$ in $n$ variables, the subspace $V$ of all Laurent polynomials in $x$ with no constant term is a MS of $\mathbb{C}[x^{-1}, x]$.

In order to understand the Duistermaat and van der Kallen theorem in a more general setting, the following problem was proposed in [ZW, Problem 1.4].

**Open Problem 1.3.** Decide commutative rings $R$ and groups $G$ such that $V_{RG}$ is a Mathieu subspace of the group algebra $RG$ of $G$ over $R$.

The following proposition and theorem among some other results were also proved [ZW].
Proposition 1.4. Let $G$ be a finite group and $K$ an arbitrary field. Then $\mathcal{V}_G$ is a MS of $KG$, if and only if $\mathcal{V}_G$ does not contain any nonzero idempotent.

Theorem 1.5. Let $G$ be a finite group and $K$ an arbitrary field. Then the following statements hold:

i) If $\text{char. } K = 0$ or $\text{char. } K = p > |G|$, then $\mathcal{V}_G$ is a MS of $KG$, where $|G|$ denotes the order of $G$.

ii) Assume that $G$ is abelian and $|G| = p^r d$ with $r, d \in \mathbb{N}$ and $p \nmid d$. If $\text{char. } K = p > 0$ and $K$ has a $d$-th primitive root of unity, then $\mathcal{V}_G$ is a MS of $KG$, if and only if $p > d$.

The second purpose of the paper is to find some numerical sufficient and necessary conditions in terms of the degrees of irreducible representations of $G$ over $K$ for that $\mathcal{V}_G$ and $\mathcal{V}_G \cap Z(KG)$ are Mathieu subspaces of $KG$, respectively.

The two purposes of the paper actually coincide. More precisely, by Proposition 1.4 $\mathcal{V}_G$ is a MS of $KG$, if and only if $KG$ has no nonzero trace-zero idempotent, and by Lemma 4.1 in Section 4, $\mathcal{V}_G \cap Z(KG)$ is a MS of $KG$, if and only if $KG$ has no nonzero central trace-zero idempotent.

To state the two main results of the paper, we denote by $\phi_i$ ($1 \leq i \leq s$) the (non-isomorphic) irreducible representations of $G$ over $K$, and $n_i$ the degree of the representation $\phi_i$. Then the first main theorem of this paper is as follows.

Theorem 1.6. Let $G$ be a finite group and $K$ a splitting field of $G$ of char. $K = p > 0$. Then $\mathcal{V}_G$ is a MS of $KG$, if and only if the following property holds:

$$(*) \quad c_1 n_1 + c_2 n_2 + \cdots + c_s n_s \not\equiv 0 \pmod{p}$$

for all integers $0 \leq c_i \leq n_i$ ($1 \leq i \leq s$) that are not all zero.

Remark 1.7. Let $\overline{B}$ be a sequence of elements in $\mathbb{Z}_p$ formed by $n_i$-copies of $n_i \pmod{p}$ with $1 \leq i \leq s$. Then it is easy to see that the property $(*)$ in Theorem 1.6 for integers $n_i$ ($1 \leq i \leq s$) is equivalent to that the sequence $\overline{B}$ is a so-called zero-sum free sequence (e.g., see [G]) of elements of $\mathbb{Z}_p$.

Remark 1.8. Given a finite group $G$ and $K$ an arbitrary field. If char. $K = 0$ or char. $K = p > |G|$, then by Proposition 1.4 and Theorems 1.5 $KG$ contains no nonzero trace-zero idempotent. If char. $K = p \leq |G|$, let $L$ be a splitting field of $G$, which contains $K$ (e.g., let $L = K[\xi]$, where $\xi$ is a primitive $d$-th root of unity and $d$ is the exponent of $G$. By [PD] Theorem 2.7B, p.58] $L$ is a splitting field of $G$).
Then we may apply Theorem 1.6 to decide if $V_{LG}$ is a MS of $LG$. If it is, then by Proposition 1.4 $V_{KG}$ is a MS of $KG$ and $KG$ contains no nonzero trace-zero idempotent.

In order to state our second main result, we need some basic notations and facts in modular representation theory. Here we freely adapt those fixed and developed in [PD].

Assume that $\text{char. } K = p > 0$ and $|G| = p^r d$ with $r, d \in \mathbb{N}$ and $p \nmid d$. Let $\hat{K}$ be a field extension of finite degree of the $p$-adic number field $\mathbb{Q}_p$ such that $X^d - 1$ splits completely in $\hat{K}[X]$. Then by Lemma 2.10 proved in Section 2, $\hat{K}$ is a splitting field for all subgroups of $G$. Let $A$ be the integral closure of the $p$-adic integers in $\hat{K}$, and $\pi A$ the unique maximal ideal of $A$ (which contains $pA$). Let $K = A/\pi A$. $K$ is a finite field of characteristic $p > 0$. Then by discussion in [PD, Section 2.7] $\hat{K}$ and $K$ are splitting fields for all subgroups and quotient groups of $G$. In particular, by [PD, Theorem 1.7B, p. 25] all irreducible $\hat{K}G$-modules and irreducible $KG$-modules are absolutely irreducible.

Let $f_i (1 \leq i \leq t)$ be the block idempotents of $KG$ and $n_{i,j} (1 \leq j \leq s_i)$ the degrees of all distinct irreducible representations of $G$ over $\hat{K}$ which lies in the $i$-th $p$-block of $KG$.

Our second main theorem of the paper is as follows.

**Theorem 1.9.** Let $G$ be a finite group and $K$ a splitting field of $G$. Then the following statements hold:

i) For every field $L$ with $\text{char. } L = 0$, or $\text{char. } L = p > |G|$, $V_{LG} \cap Z(LG)$ is a MS of $LG$.

ii) If $\text{char. } K = p > 0$ and $p \nmid |G|$, then $V_{KG} \cap Z(KG)$ is a MS of $KG$, if and only if for each $\emptyset \neq J \subseteq \{1, 2, \ldots, s\}$ we have

\[ \sum_{i \in J} n_i^2 \not\equiv 0 \pmod{p}. \]  

(1.1)

iii) If $\text{char. } K = p > 0$ and $p \mid |G|$, then $V_{KG} \cap Z(KG)$ is a MS of $KG$, if and only if for all $\emptyset \neq J \subseteq \{1, 2, \ldots, t\}$, both the numerator and the denominator of the rational number $\frac{1}{|G|} \sum_{i \in J} \sum_{j=1}^{s_i} n_{i,j}^2$ in the reduced form are co-prime to $p$.

Note also that if char. $K = 0$ or char. $K = p > 0$ with $p \nmid |G|$, then by Maschke’s Theorem (e.g., see [PD, Theorem 1.3B]) $KG$ is semi-simple. For all $1 \leq i \leq t = s$, the dimension over $K$ of $i$-th (indecomposable) $p$-block of $KG$ is equal to $n_i^2$.

If char. $K = p > 0$ with $p \mid |G|$, then for each $1 \leq i \leq t$, by [PD, Theorem 4.2D, p. 99] and also the fact mentioned above on the blocks
of $\hat{KG}$ (noting char. $\hat{K} = 0$), we see that the dimension of the $i$-th $p$-block of $KG$ over $K$ is equal to $\sum_{j=1}^{s_i} n_{i,j}^2$ (in the same notation as in Theorem 1.9). Then it is easy to see that the case of Theorem 1.9 over all splitting base fields can be re-stated in the following more uniform way.

**Corollary 1.10.** Let $K$ be a splitting field (of arbitrary characteristic) of $G$. Let $t$ be the number of (indecomposable) blocks of $KG$ and $d_i$ ($1 \leq i \leq t$) the dimension over $K$ of the $i$-th block of $KG$. Then for $\forall \emptyset \neq J \subseteq \{1, 2, \ldots, t\}$, both the numerator and the denominator of the rational number $\frac{1}{|G|} \sum_{i \in J} d_i$ in the reduced form are co-prime to $p$.

Note that by Lemma 4.1 in Section 4 the sufficient and necessary conditions in Theorem 1.9 and Corollary 1.10 are also sufficient and necessary conditions for the nonexistence of nonzero central trace-zero idempotents in $KG$.

**Arrangements.** We mainly give a proof for Theorem 1.6 in Section 2 and discuss some applications of Theorem 1.6 in Section 3. In Section 4 we mainly give a proof for Theorem 1.9.

**2. Proof of Theorem 1.6**

Throughout this section, $G$ stands for a finite group and $K$ a splitting field of $G$ of characteristic $p > 0$. We denote by $\phi_i$ ($1 \leq i \leq s$) all the (non-isomorphic) irreducible representations of $G$ over $K$ and $n_i$ the degree of the representation $\phi_i$ for all $1 \leq i \leq s$. Here we fix the irreducible representation $\phi_i$ ($1 \leq i \leq s$) as a $K$-algebra homomorphism from $KG$ to the $n_i \times n_i$ matrix algebra $M_{n_i}(K)$. Note that by Burnside’s Theorem (e.g., see [PD, Corollary, p. 11]) each $\phi_i$ ($1 \leq i \leq s$) is surjective.

Let $\mathcal{A} = \bigoplus_{i=1}^{s} M_{n_i}(K)$ and $\mathcal{A}_i = M_{n_i}(K)$ ($1 \leq i \leq s$). For each $1 \leq i \leq s$ we define $\text{tr}_i : \mathcal{A} \rightarrow K$ to the $K$-linear functional whose restriction on the $i$-th component $M_{n_i}(K)$ of $\mathcal{A}$ is the usual trace function of the $n_i \times n_i$ matrices, and on $j$-th component of $\mathcal{A}$ is equal to 0 for all $j \neq i$.

With the notations and settings above we recall the classical Wedderburn Structure Theorem (see [PD, Theorem 1.3A]) for $KG$.

**Theorem 2.1.** Define $\Phi : KG \rightarrow \mathcal{A}$ be setting $\Phi(\sigma) = \sum_{i=1}^{s} \phi_i(\sigma)$ for all $\sigma \in KG$. Then $\Phi$ is a surjective homomorphism of $K$-algebras and $\text{Ker} \Phi = J(KG)$, where $J(KG)$ stands for the Jacobson radical of $KG$.

Next, we recall the following theorem which clarifies all co-dimensional one MS’ of $\mathcal{A}$.
Theorem 2.2. ([Ko] Corollary 4.5) A codimensional one $K$-subspace $V$ of $A$ is a MS of $A$, if and only if $V = \text{Ker} \ L$ for some $K$-linear functional $L$ of $A$ such that $L = \sum_{i=1}^{s} c_i \text{tr}_i$, where the coefficients $c_i \in K$ ($1 \leq i \leq s$) satisfy the property: for all $\emptyset \neq J \subseteq \{1, 2, ..., s\}$ with not all $c_i$ ($i \in J$) being zero, we have $\sum_{i \in J} c_i \neq 0$.

The following proposition classifies all the co-dimensional one MS’ $V$ of $KG$ with $V \supseteq J(KG)$ (the Jacobson radical of $KG$).

**Proposition 2.3.** Let $V$ be a co-dimensional one $K$-subspace of $KG$ with $V \supseteq J(KG)$, and $\chi_i$ the character of $G$ obtained from the irreducible representation $\phi_i$ ($1 \leq i \leq s$). Then $V$ is a MS of $KG$, if and only if $V = \text{Ker} \ \ell$, where $\ell = \sum_{i=1}^{s} c_i \chi_i$ for some $c_i \in K$ ($1 \leq i \leq s$) which satisfy the property: for all $\emptyset \neq J \subseteq \{1, 2, ..., s\}$ with not all $c_i$ ($i \in J$) being zero, we have $\sum_{i \in J} c_i \neq 0$.

**Proof:** Since $\Phi$ by Theorem 2.1 is surjective and $V \supseteq J(KG)$, there exists a co-dimensional one $K$-subspace $W$ of $A$ such that $V = \Phi^{-1}(W)$ (Actually, $W = \Phi(V)$). By Theorem 2.2 (or [EKC] Theorem 5.8.1]), $W$ is a MS of $A$ iff $W = \text{Ker} \ L$ for some $K$-linear functional $L$ of $A$ such that $L = \sum_{i=1}^{s} c_i \text{tr}_i$, for some $c_i \in K$ ($1 \leq i \leq s$) which satisfy the property in the proposition.

Let $\Phi^*$ be the dual map of $\Phi$, i.e., $\Phi^*(\psi) = \psi \circ \Phi$ for all $K$-linear functional $\psi$ of $A$. Then by definition of characters we have $\Phi^*(\text{tr}_i) = \chi_i$ for all $1 \leq i \leq s$. Since $V = \Phi^{-1}(W)$, $W = \Phi(V)$ and $W = \text{Ker} \ L$, we have $V = \text{Ker} \ \ell$ with $\ell = \phi^*(L) = \sum_{i=1}^{s} c_i \chi_i$. Since by Theorem 2.1 and [Z3] Proposition 2.7], $V$ is a MS of $KG$, if and only if $W$ is a MS of $A$, the proposition follows. \qed

Now, we can prove Theorem 1.6 for the semisimple case.

**Lemma 2.4.** Assume that $p \nmid |G|$. Then

i) $\Phi(V_G) = \text{Ker} \ F$, where $F = \sum_{i=1}^{s} n_i \text{tr}_i$.

ii) $V_G = \text{Ker} \ \ell$, where $\ell = \Phi^*(F) = \sum_{i=1}^{s} n_i \chi_i$.

iii) $V_G$ is a MS of $KG$, if and only if $\sum_{i=1}^{s} c_i n_i \neq 0$ for all $\emptyset \neq (c_1, ..., c_s) \in \{0, 1, ..., n_1\} \times \cdots \times \{0, 1, ..., n_s\}$. In other words, Theorem 7.6 holds in this case.

**Proof:** Note first that, since $p \nmid |G|$, by Maschke’s Theorem (e.g., see [PD] Theorem 1.3B]) the group algebra $KG$ is semisimple, i.e., $J(KG) = 0$. Then $\Phi$ in Theorem 2.1 is a $K$-algebra isomorphism.

i) Let $1_G \neq g \in G$ and $u = \Phi(g)$. Write $u = \sum_{i=1}^{s} B_i$ with $B_i \in A_i := M_{n_i}(K)$ for all $1 \leq i \leq s$. To show $u \in \text{Ker} \ F$, we consider the trace of the regular action of $g$ on $KG$ and the trace of the regular action of $u$
EXISTENCE OF NONZERO TRACE-ZERO IDEMPOTENTS

on \( A \). Since \( \Phi \) in this case is an isomorphism of \( K \)-algebras, we know that these two traces are equal to one another.

First, by choosing elements of \( G \) as a basis of \( KG \), it is easy to see that the trace of the regular action of \( g \) on \( KG \) is equal to 0.

Second, for each \( 1 \leq i \leq s \), since the matrix \( B_i \) annihilates all elements of \( A_j \) for all \( j \neq i \), the trace of the regular action of \( B_i \) on \( A \) is equal to the trace of the regular action of \( B_i \) on \( A_i = M_{n_i}(K) \), which can be readily checked to be \( n_i \text{tr}_i(B_i) \) by choosing the matrices \( E_{k,\ell}'s \) (with 1 as the \((k,\ell)\)-entry and zero elsewhere) as a basis of \( A_i = M_{n_i}(K) \). Hence the trace of the regular action of \( u \) on \( A \) is equal to \( \sum_{i=1}^{s} n_i \text{tr}_i(B_i) \). Therefore \( \Phi(V_G) \subseteq \text{Ker} F \) for \( V_G \) is spanned over \( K \) by all non-identity elements of \( G \). Since \( \Phi(V_G) \) and \( \text{Ker} F \) are both co-dimensional one subspaces of \( A \), we have \( \Phi(V_G) = \text{Ker} F \), and statement \( i \) follows.

\( ii \) follows immediately from \( i \), and the fact that \( \Phi^*(\text{tr}_i) = \chi_i \) for all \( 1 \leq i \leq s \).

\( iii \) follows immediately from \( ii \), Proposition 2.3 above and the fact that \( n_i \neq 0 \) for all \( 1 \leq i \leq s \). ✷

Next we shall give a proof of Theorem 1.6 for the case \( p \mid |G| \). In order to do so we need first to prove some lemmas, for which we do not assume \( p \mid |G| \).

**Lemma 2.5.** Assume that \( KG \) has \( k \) nonzero (pairwise) orthogonal idempotents \( e_i \) \( (1 \leq i \leq k) \) with \( k \geq p \). Then \( V_G \) is not a MS of \( KG \).

**Proof:** For each \( 1 \leq j \leq k \) set \( s_j = \sum_{i=1}^{j} e_i \). Then it is easy to see that \( s_j \ (1 \leq j \leq k) \) are all nonzero idempotents. By [Pa, Theorem 3.5 in p. 48], which was first proved by Zalesskii [Za] in 1972, \( \text{tr} s_j \in \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \) for all \( 1 \leq j \leq k \). Since \( k \geq p \), there exists either \( 1 \leq j_0 \leq k \) such that \( \text{tr} s_{j_0} = 0 \), or \( a < b \) such that \( \text{tr} s_a = \text{tr} s_b \), whence \( \text{tr} (s_b - s_a) = 0 \). Since \( s_b - s_a = e_{a+1} + \cdots + e_b \) is also a nonzero idempotent, \( V_G \) in either case contains a nonzero trace-zero idempotent, namely, \( s_{j_0} \) or \( s_b - s_a \). Then by Proposition 1.4 \( V_G \) is not a MS of \( KG \). ✷

**Lemma 2.6.** Assume that \( V_G \) is a MS of \( KG \). Then

\( i \) \( p > \sum_{i=1}^{s} n_i \).

\( ii \) \( G \) has a normal Sylow \( p \)-subgroup.

**Proof:** \( i \) Let \( m = \sum_{i=1}^{s} n_i \) and assume \( p \leq m \). We view \( A \) as a \( K \)-subalgebra of the matrix algebra \( M_m(K) \) by putting \( M_{n_i}(K) \) \( (1 \leq i \leq s) \) as the \((i,i)\)-th block on the diagonal. Let \( f_i \ (1 \leq i \leq m) \) be
the \( m \times m \) diagonal matrix with all entries being zero except the \((i,i)\)-th entry being 1. Hence \( f_i \) (\( 1 \leq i \leq m \)) are orthogonal idempotents of \( A \) such that \( \sum_{i=1}^{m} f_i = 1_A \). Note that by Theorem 2.1, \( \text{Ker } \phi = J(KG) \) and hence is nilpotent. Then by [Pa, Lemma 3.7 (i), p. 49] there exist nonzero orthogonal idempotents \( e_i \in KG \) (\( 1 \leq i \leq m \)) such that \( \Phi(e_i) = f_i \). Hence, by Lemma 2.5, \( V_G \) is not a MS of \( KG \). Contradiction.

ii) By i) we have \( p > n_i \) for each \( 1 \leq i \leq s \), whence \( p \nmid n_i \). It is well known that \( n_i \) (\( 1 \leq i \leq s \)) are also the degrees of irreducible Brauer characters of \( G \) (by the very definition of the irreducible Brauer characters, e.g., see [N1, p. 17]). Then by [Mi2, Theorem 2.4] (which is a modular version of the Itô-Michler Theorem [I, Mi2], see also [N2]) \( G \) has a normal Sylow \( p \)-subgroup.  

Recall that an element \( g \in G \) is said to be a \( p \)-singular element, or simply a \( p \)-element of \( G \) if the order of \( g \) is a power of \( p \). \( g \) is said to be a \( p \)-regular element, or simply a \( p' \)-element of \( G \) of the order of \( g \) is co-prime to \( p \). The identity element \( 1_G \) is the only both \( p \)-singular and \( p \)-regular element of \( G \).

It is easy to check that every element \( g \in G \) can be written as the product of a \( p \)-element and \( p' \)-element, which commute with one another. We denote by \( G^o \) the set of all \( p' \)-elements of \( G \).

**Lemma 2.7.** Let \( e \) be an idempotent of \( KG \) and \( h \in G \setminus G^o \), i.e., \( h \) is not a \( p' \)-element. Then the sum of the coefficients in \( e \) of the elements in the conjugacy class \( C \) of \( h \) is equal to 0.

**Proof:** Write \( |G| = p^r d \) for some \( r, d \in \mathbb{N} \) with \( p \nmid d \). Then it is easy to see that \( g^{p^r} \in G^o \) for all \( g \in G \). Write the idempotent \( e \) as

\[
e = \sum_{a \in G \setminus G^o} c_a a + \sum_{b \in G^o} c_b b
\]

with \( c_a, c_b \in K \) (\( a \in G \setminus G^o, b \in G^o \)).

By [Pa] Lemma 3.1, p. 45] there exists \( \beta \) in the commutator subspace \([KG, KG]\) of \( KG \) such that

\[
e = e^{p^r} = \sum_{a \in G \setminus G^o} c_a^{p^r} a^{p^r} + \sum_{b \in G^o} c_b^{p^r} b^{p^r} + \beta.
\]

---

\(^1\) The proof of [Mi2, Theorem 2.4] used the classification of finite simple groups. For a proof of this theorem without using the classification, see [Man, Theorem on p. 121]. For a short proof for a special case of the “only if” part of the theorem, see [R].
Since $a^r \in G^o$ for all $a \in G \setminus G^o$, we further have

\[(2.3) \quad e = e^r = \sum_{b \in G^o} d_b b + \beta\]

for some $d_b \in K$ ($b \in G^o$).

Then by eqs. (2.2) and (2.3) we get

\[(2.4) \quad \sum_{a \in G \setminus G^o} c_a a + \sum_{b \in G^o} (c_b - d_b) b = \beta \in [KG, KG].\]

Since $h \in G \setminus G^o$, its conjugacy class $C \subset G \setminus G^o$. Then by [Pa] Lemma 3.2, p. 46] and the equation above we have $(\sum_{a \in C} c_a)^r = \sum_{a \in C} e^a = 0$, whence the lemma follows. \qed

The next lemma will play a crucial role in the proof of Theorem 1.6.

**Lemma 2.8.** Let $H$ be a normal $p$-subgroup of $G$. Then $V_G$ is a MS of $KG$, if and only if $V_{G/H}$ is a MS of the group algebra $K[G/H]$ of $G/H$ over $K$.

**Proof:** Let $\rho : K[G] \to K[G/H]$ be the $K$-algebra homomorphism induced by the quotient map from $G$ to $G/H$. Then by [Pa] Lemma 1.8, p. 10] $\text{Ker } \rho = \omega(KH)KG$, where $\omega(KH)$ is the augmentation ideal of $KH$ which is spanned by $(h - 1)$ ($h \in H$) over $K$. Therefore $K[G/H] \simeq KG/\omega(KH)KG$.

Let $g_i$ ($1 \leq i \leq k := |G/H|$) with $g_1 = 1_G$ be the representatives of the distinct (right) cosets of $H$ in $G$. Then for every idempotent $e \in KG$, there exist some $a_i \in KH$ ($1 \leq i \leq k$) such that

\[(2.5) \quad e = a_1 1_G + a_2 g_2 + \cdots + a_k g_k.\]

Hence, the coefficient of $1_G$ in $e$ is equal to the coefficient of $1_H$ in $a_1$, i.e., $\text{tr}_G e = \text{tr}_H a_1$. Furthermore, since $H \trianglelefteq G$, the $G$-conjugacy class of each $h \in H$ is contained in $H$. Since $H$ is a $p$-group, by Lemma 2.7 the sum of the coefficients in $a_1$ over the $G$-conjugacy class of each $1_H \neq h \in H$ is equal to zero, whence $\rho(a_1) = \text{tr}_H a_1$.

On the other hand, by eq. (2.5) and the definition of $\rho$ we also have $\text{tr}_{G/H} \rho(e) = \rho(a_1)$. In summary, the following equations hold:

\[(2.6) \quad \text{tr}_G e = \text{tr}_H a_1 = \rho(a_1) = \text{tr}_{G/H} \rho(e).\]

(\Rightarrow) Assume that $V_G$ is a MS of $KG$ and $V_{G/H}$ is not a MS of $K[G/H]$. Then by Proposition 1.4 there exists a nonzero idempotent $u \in V_{G/H}$ (with $\text{tr}_{G/H} u = 0$). Since $H \trianglelefteq G$, it follows easily from [Pa] Lemma 1.6, p. 70] that $\text{Ker } \rho (= \omega(KH)KG)$ is a nilpotent ideal of $KG$. Then by [Pa] Lemma 3.7 (i), p. 49] there exists an idempotent $e \in KG$ such that $\rho(e) = u$. By eq. (2.6) $\text{tr}_G e = \text{tr}_{G/H} u = 0$, i.e., $e \in V_G$. Since
$V_G$ is MS of $KG$, by Proposition 1.4 we have $e = 0$, whence $u = 0$. Contradiction.

$(\Leftarrow)$ Assume that $V_{G/H}$ is a MS of $K[G/H]$ and $V_G$ is not a MS of $KG$. Then by Proposition 1.4 there exists a nonzero idempotent $e \in V_G$ (with $\text{tr}_G e = 0$). Note that $\rho(e) \neq 0$, for Ker $\rho = \omega(KH)KG$ is nilpotent (as pointed out above). Therefore $\rho(e)$ is a nonzero idempotent of $K[G/H]$, and by eq. (2.6) $\text{tr}_{G/H} \rho(e) = 0$, whence $\rho(e) \in V_{G/H}$. Since $V_{G/H}$ is a MS of $K[G/H]$, by Proposition 1.4 $\rho(e) = 0$. Contradiction. □

**Remark 2.9.** We will show later in Proposition 3.3 that the $p$-subgroup condition on $H$ for the “only if” part of Lemma 2.8 can actually be dropped.

Now we can prove Theorem 1.6 as follows.

**Proof of Theorem 1.6** (⇒) Assume that $V_G$ is a MS of $KG$. Then by Lemma 2.6 (ii) $G$ has a normal Sylow $p$-subgroup $H$. By Lemma 2.8 $V_{G/H}$ is a MS of $K[G/H]$. Since $p \nmid |G/H|$, it follows from Lemma 2.4 (iii) that the property $(\ast)$ in Theorem 1.6 holds for $K[G/H]$.

On the other hand, by [Pal, Proposition 4.7, p. 67] the Jacobson radical $J(KG)$ of $KG$ is equal to the ideal $I_H$ of $KG$ generated by $(h - 1)$ $(h \in H)$. Since by Theorem 2.1 $K[G/H] \simeq KG/I_H \simeq KG/J(KG)$, the degrees of irreducible representations of $KG$ over $K$ (or equivalently, irreducible representations of $G$ over $K$) are the same as the degrees of irreducible representations of $K[G/H]$ over $K$ (or equivalently, irreducible representations of $G/H$ over $K$). Therefore, the property $(\ast)$ in Theorem 1.6 holds also for $KG$.

$(\Leftarrow)$ Assume that the property $(\ast)$ in Theorem 1.6 holds for $KG$. If $p \leq n_{i_0}$ for some $1 \leq i_0 \leq s$, then the property $(\ast)$ fails for the coefficients $c_{i_0} = p$ and $c_i = 0$ $(i \neq i_0)$. Therefore, $p > n_i$, and hence $p \nmid n_i$, for all $1 \leq i \leq s$. Then by [Mi2, Theorem 2.4] or [Man, Theorem on p. 121] or the theorem in the short note [R], $G$ has a normal Sylow $p$-subgroup $H$. Since as pointed above, the degrees $n_i$ $(1 \leq i \leq s)$ of irreducible representations of $G$ over $K$ are the same as the degrees of irreducible representations of $G/H$ over $K$, the property $(\ast)$ in Theorem 1.6 holds for $K[G/H]$. Since $p \nmid |G/H|$, by Lemma 2.4 (iii) $V_{G/H}$ is a MS of $K[G/H]$, and by Lemma 2.8 $V_G$ is a MS of $KG$. □

To end this section we point out that Theorem 1.5 (ii) also follows from Theorem 1.6. First, by the lemma given below, the condition $p > d$ implies that $K$ is a splitting field of $G$. Second, it is well known (e.g., see [PD, Corollary on p. 19]) that all irreducible representations of an abelian group are of dimension one, i.e., $n_i = 1$ for all $1 \leq i \leq s$. 

**Proof of Theorem 1.5** (ii) Assume that $V_{G/H}$ is a MS of $K[G/H]$ and $V_G$ is not a MS of $KG$. Then by Proposition 1.4 there exists a nonzero idempotent $e \in V_G$ (with $\text{tr}_G e = 0$). Note that $\rho(e) \neq 0$, for Ker $\rho = \omega(KH)KG$ is nilpotent (as pointed out above). Therefore $\rho(e)$ is a nonzero idempotent of $K[G/H]$, and by eq. (2.6) $\text{tr}_{G/H} \rho(e) = 0$, whence $\rho(e) \in V_{G/H}$. Since $V_{G/H}$ is a MS of $K[G/H]$, by Proposition 1.4 $\rho(e) = 0$. Contradiction. □
Then it is easy to see that the property \((\ast)\) in Theorem 1.6 holds, if and only if \(p > s\).

On the other hand, by [PD, Theorem 1.5] the number of irreducible representations of \(G\) over \(K\) is equal to the number of conjugacy classes of \(p'\)-elements of \(G\), i.e., \(s = d\) (since \(G\) is abelian). Then by the facts above and also the lemma below, Theorem 1.5 \(\text{ii}\) follows from Theorem 1.6.

**Lemma 2.10.** Assume that \(|G| = p^r d\) for some \(r, d \in \mathbb{N}\) such that \(p \nmid d\). Let \(L\) be a field of characteristic \(p > 0\), which contains a primitive \(d\)-th root of unity. Then \(L\) is a splitting field of \(G\).

**Proof:** Since \(L\) contains a primitive \(d\)-th root of unity, the polynomial \(X^d - 1\) splits into the product of some degree one polynomials in \(L[X]\). Let \(n = |G|\). Since \(X^n - 1 = X^{p^r d} - 1 = (X^d - 1)^{p^r}\), the polynomial \(X^n - 1\) also splits into the product of degree one polynomials in \(L[X]\), hence so does \(X^m - 1\), where \(m\) is the exponent of \(G\). Then by [PD, Theorem 2.7B, p. 58] \(L\) is a splitting field of \(G\). \(\Box\)

### 3. Some Applications of Theorem 1.6

Throughout this section \(G\) stands for a finite group with \(|G| = p^r d\) and \(p \nmid d\), and \(K\) a splitting field of \(G\) of characteristic \(p > 0\). We will also freely use the notation fixed in Sections 1 and 2, e.g., \(n_i\) (1 \(\leq i \leq s\)) stand for the degrees of all irreducible representations of \(G\) over \(K\).

**Proposition 3.1.** Assume that \(|G| = p^r d\) with \(p \nmid d\). If \(p > \sum_{i=1}^{s} n_i^2\), then \(V_G\) is a MS of \(KG\). In particular, if \(G\) has a normal Sylow \(p\)-subgroup and \(p > d\), then \(V_G\) is a MS of \(KG\).

**Proof:** First, it is easy to see that the condition \(p > \sum_{i=1}^{s} n_i^2\) implies the property \((\ast)\) in Theorem 1.6, and hence by the same theorem \(V_G\) is a MS of \(KG\).

Now assume that \(G\) has a normal Sylow \(p\)-subgroup \(H\). Then, as pointed out in the proof of Lemma 2.8 in Section 2, \(n_i\) (1 \(\leq i \leq s\)) are also the degrees of all irreducible representations of \(G/H\) over \(K\). Since \(p \nmid d = |G/H|\), by Maschke’s Theorem (e.g., see [PD, Theorem 1.3B, ii]) \(K[G/H]\) is semi-simple. In particular, we have \(\sum_{i=1}^{s} n_i^2 = d\) by Theorem 2.1 and hence \(p > \sum_{i=1}^{s} n_i^2\). Then by the first part of the proposition proved above, \(V_G\) is a MS of \(KG\). \(\Box\)

**Remark 3.2.** Let \(G\) be a \(p\)-group, then \(V_G\) by the proposition above is a MS of \(KG\). Actually, by [Pa, Proposition 4.7, p. 67] \(KG\) is a local \(K\)-algebra and hence, does not have any non-trivial idempotents. Then
by [Z3, Theorem 4.2] every $K$-subspace $V$ of $KG$ such that $1 \notin V$ is a MS of $KG$.

The next two propositions claim that the set of all finite groups $G$ over some fixed splitting fields $K$ is closed under taking subgroups, and taking quotient groups as well as taking semi-product with $p$-groups.

**Proposition 3.3.** Let $Q$ be a subgroup of $G$ or a quotient group of $G$. Assume that $K$ is also a splitting field of $Q$ and $V_G$ is a MS of $ KG $. Then $V_Q$ is a MS of $ KQ $.

**Proof:** The case that $Q$ is a subgroup can be seen easily from the assumption and Proposition 1.4. So we assume that $Q = G/H$ for some $H \leq G$.

Let $\rho : KG \to K[G/H]$ be the $K$-algebra homomorphism induced by the quotient map from $G$ to $G/H$ and $\psi_i : K[G/H] \to M_{n_i}(K)$ ($1 \leq i \leq t$) all (non-isomorphic) irreducible representations of $G/H$ over $K$. Then by Burnside’s Theorem (e.g., see [PD, Corollary, p. 11]) each $\psi_i$ is surjective. Since $\pi$ is surjective, so is the composition $\phi_i := \psi_i \circ \rho$. Hence $\phi_i$ ($1 \leq i \leq t$) are non-isomorphic irreducible representations of $G$ over $K$ of degree $n_i$. Therefore, the condition ($\ast$) in Theorem 1.6 for the degrees of irreducible modules of $G$ over $K$ implies the same condition ($\ast$) for the degrees of irreducible modules of $G/H$ over $K$ (by letting $c_i = 0$ for all $t + 1 \leq i \leq s$). Then by applying Theorem 1.6 to $G/H$ the proposition follows. ☐

A special case of the proposition above for quotient groups of $G$ follows also directly from Proposition 1.4 and the lemma below which has some interests on its own.

**Lemma 3.4.** Let $H \leq G$ such that $p \nmid |H|$ and $\rho : KG \to K[G/H]$ be the $K$-algebra homomorphism induced by the quotient map from $G$ to $G/H$. Then for every idempotent $e \in K[G/H]$ there exists an idempotent $u \in KG$ such that $\rho(u) = e$ and $tr_G u = \frac{1}{|H|} tr_{G/H} e$.

**Proof:** Let $k = |G/H|$ and $g_i$ ($1 \leq i \leq k$) be the representatives of all the cosets of $H$ in $G$ with $g_1 = 1_G$. For each $g \in G$ we set also $\bar{g} = \rho(g)$. Write $e = \sum_{i=1}^{k} c_i \bar{g}_i$ for some $c_i \in K$ ($1 \leq i \leq k$). Let $E_H = \frac{1}{|H|} \sum_{h \in H} h$ (i.e., the principal idempotent of the group algebra $KH$ of $H$). Then it is well known (and also easy to check) that we have

$$ E_H^2 = E_H \quad \text{and} \quad E_H h = E_H $$

(3.7)
for all $h \in H$. Furthermore, by using the assumption $H \trianglelefteq G$ we have also that $E_H g = g E_H$ for all $g \in G$, whence $E_H \in Z(KG)$. Set

\begin{equation}
(3.8) \quad v := \sum_{i=1}^{k} c_i g_i \quad \text{and} \quad u := E_H v.
\end{equation}

Then $\rho(v) = e$, $\rho(E_H) = 1$, and hence $\rho(u) = e$. Consequently, $v^2 - v \in \text{Ker } \rho$, for $\rho(v^2) = \rho(v)^2 = e^2 = e = \rho(v)$, and $v^2 = v + w$ for some $w \in \text{Ker } \rho$. Furthermore, by [Pa, Lemma 1.8, p. 10] there exist some $\alpha_h \in KG$ ($h \in H$) such that $w = \sum_{h \in H} (h - 1) \alpha_h$. Now, by eq. (3.7) and the fact $E_H \in Z(KG)$ we have

\[ u^2 = E_H v E_H^2 v = E_H^2 v^2 = E_H v^2 = E_H (v + w) = E_H (v + \sum_{h \in H} (h - 1) \alpha_h) = E_H v + \sum_{h \in H} (E_h h - h) \alpha_h = E_H v = u. \]

Therefore $u$ is an idempotent of $KG$ with $\rho(u) = e$, and by eq. (3.8) $\text{tr}_G u = \frac{1}{|H|} \text{tr}_{G/H} e$, as desired. \quad \Box

**Proposition 3.5.** Let $P$ be a $p$-group and $\tilde{G} = P \rtimes G$. Then $V_G$ is a MS of $KG$, if and only if $V_{\tilde{G}}$ is a MS of $K\tilde{G}$.

**Proof:** Since $\tilde{G}/P \cong G$ and $P$ is a normal $p$-subgroup of $\tilde{G}$, the proposition follows immediately from Lemma 2.8. \quad \Box

**Proposition 3.6.** Assume that $K$ is splitting field for all subgroups and quotient groups of $G$ and $V_G$ is a MS of $KG$. Then for every subgroup or quotient $Q$, the following statements hold:

i) the degree of every irreducible module of $Q$ over $K$ is less than $p$.

ii) the number of $p$-blocks of $KQ$ is less than $p$.

**Proof:** By Proposition 3.3 we may assume $Q = G$. Then i) follows from Lemma 2.6 i). Since the number of $p$-blocks of $KG$ is equal to the number of (orthogonal and primitive) block idempotents of $KG$, statement ii) follows immediately from Lemma 2.5. \quad \Box

Next, we consider the extreme case that char. $K = 2$.

**Proposition 3.7.** Let $L$ be a field of characteristic $p = 2$, which is a splitting field of all subgroups of $G$ (e.g., when the polynomial $X^d - 1$ splits completely in $L[X]$, see Lemma 2.10). Then the following statements are equivalent:
Proof: Let \( e \) be an idempotent of \( LG \). Then by [Pa, Theorem 3.5 in p. 48], which was first proved by Zalesskii [Za] in 1972, \( \text{tr} \ e = 0 \), or 1. Hence the equivalence of statements \( i \) and \( ii \) follows immediately from Proposition 1.4. The \( iii \) \( \Rightarrow \) \( i \) part follows from Remark 3.2. So it suffices to show \( i \) \( \Rightarrow \) \( iii \).

Assume that \( i \) holds but \( iii \) fails. By Cauchy’s theorem there exists \( g \in G \) of odd order \( k \geq 3 \). Let \( H \) be the cyclic subgroup of \( G \) generated by \( g \). Then by Proposition 3.3, \( V_H \) is a MS of \( LH \), and the condition (*) in Theorem 1.6 holds for the degrees of irreducible representations of \( H \), which together with the assumption \( p = 2 \) implies that \( H \) has only one irreducible representation, namely, the trivial one.

On the other hand, since \( 2 \nmid k = |H| \), by [PD, Theorem 1.5] the number of irreducible modules of \( H \) over \( K \) is equal to the number of conjugacy classes of odd order elements of \( H \), which is \( k \) since \( H \) is abelian. Therefore \( k = 1 \), contradiction. \( \square \)

Finally, from Theorem 1.6 and Lemma 2.6, we see that, for the degrees \( n_i \ (1 \leq i \leq s) \) of irreducible representations of \( G \) over \( K \), the property (*) in Theorem 1.6 implies that \( p > \sum_{i=1}^{s} n_i \). Actually, this implication holds for all finite sequences of positive integers, as we will show in the next corollary.

**Corollary 3.8.** Let \( n_i \ (1 \leq i \leq s) \) be arbitrary positive integers which satisfy the property (*) in Theorem 1.6. Then \( p > \sum_{i=1}^{s} n_i \).

**Proof:** Let \( \overline{B} \) be a sequence of elements in \( \mathbb{Z}_p \) formed by \( n_i \)-copies of \( n_i \mod p \) with \( 1 \leq i \leq s \). Then as pointed out in Remark 1.7, the property (*) in Theorem 1.6 for integers \( n_i \ (1 \leq i \leq s) \) is equivalent to that \( \overline{B} \) is a zero-sum free sequence of elements of \( \mathbb{Z}_p \). Since the sequence \( \overline{B} \) is of length \( \sum_{i=1}^{s} n_i \), the corollary follows from [G, Theorem 10.2] for the abelian group \( \mathbb{Z}_p \). \( \square \)

The corollary above can also be proved directly by applying similar arguments as those given in the proof of Lemma 2.5 to the sequence of partial sums of \( \overline{B} \) in the proof above.

4. **Proof of Theorem 1.9**

Throughout this section \( G \) stands for a finite group and \( K \) a field (of arbitrary characteristic). Let \( f_i \ (1 \leq i \leq t) \) be all the (central) block
idempotents of $KG$. The notations fixed in the previous sections are still in force, e.g., $|G| = p^r d$ with $p \nmid d$.

In this section we mainly give a proof for Theorem 1.9.

**Lemma 4.1.** The following statements are equivalent:

i) $V_G \cap Z(KG)$ is a MS of $KG$;

ii) $KG$ does not contain any nonzero central trace-zero idempotent.

iii) \( \sum_{i \in J} \text{tr } f_i \neq 0 \) for all non-empty $J \subseteq \{1, 2, ..., t\}$.

**Proof:** i) $\Rightarrow$ ii) Assume that $KG$ contains a nonzero central idempotent $e$ with $\text{tr } e = 0$. Let $g \in G$ such that the coefficient $c_g$ of $g$ in $e$ is nonzero. Then $\text{tr} (g^{-1} e) = c_g \neq 0$, whence $g^{-1} e \notin V_G \cap Z(KG)$. Since $KG$ is of finite dimension over $K$ and hence algebraic over $K$, by [Z3, Theorem 4.2] $V_G \cap Z(KG)$ is not a MS of $KG$. Contradiction.

The ii) $\Rightarrow$ i) part follows immediately from [Z3, Theorem 4.2].

ii) $\iff$ iii) Since $f_i$ (1 $\leq$ $i$ $\leq$ $t$) are all primitive idempotents of $Z(KG)$, by [N1, Theorem 3.11, p.55] every idempotent of $Z(KG)$ has the form $\sum_{i \in J} f_i$ for some non-empty $J \subseteq \{1, 2, ..., t\}$. Hence statements ii) and iii) are equivalent to one another. $\Box$

**Remark 4.2.** By a similar argument as the proof of [ZW, Proposition 3.1], one can actually show that, replacing the base field $K$ by any commutative base ring $R$, $V_{RG} \cap Z(RG)$ is a MS of $RG$, if and only if every $\beta \in V_{RG} \cap Z(RG)$ with $\beta^m \in V_{RG} \cap Z(RG)$ for all $m \geq 1$ is nilpotent.

**Corollary 4.3.** If $V_G$ is a MS of $KG$, then so does $V_G \cap Z(KG)$.

**Proof:** Since $V_G$ is a MS of $KG$, by Proposition 1.4, $V_G$ does not contain any nonzero idempotent of $KG$. Hence, neither does $V_G \cap Z(KG)$. Then by Lemma 4.1, $V_G \cap Z(KG)$ is a MS of $KG$. $\square$

**Corollary 4.4.** Assume that $\text{char. } K = p > 0$ with $p \mid |G|$, and $V_G \cap Z(KG)$ is a MS of $KG$. Then every block idempotent $f_i$ (1 $\leq$ $i$ $\leq$ $t$) is of full defect.

**Proof:** For each 1 $\leq$ $i$ $\leq$ $t$, let $r_i$ be the defect of the block idempotent $f_i$. Then by [Mi1, Theorem 2.1 (b)] $\text{tr } f_i = p^{r-x-y} \frac{1}{xy}$ (as elements of $K$) for some $x, y \in \mathbb{N}$ which are co-prime to $p$. If $r_i < r$ for some 1 $\leq$ $i$ $\leq$ $t$, then statement iii) in Lemma 4.1 fails for the subset $J = \{i\}$, and by the same lemma, $V_G \cap Z(KG)$ is not a MS of $KG$. Contradiction. $\square$

Now we can give a proof for Theorem 1.9. We will freely use the notation and conventions introduced in Section 1 related with Theorem...
Proof of Theorem 1.9: i) By Theorem 1.5 i), \( V_G \) is a MS of \( LG \), and by Corollary 4.3, \( V_G \cap Z(LG) \) is a MS of \( LG \).

ii) Assume that char. \( K = p > 0 \) with \( p \nmid |G| \), then by [PD, Theorem 3.5, ii], p. 75, \( s_i = 1 \) and \( n_{i,1} = n_i \) for all \( 1 \leq i \leq t \). Consequently, we have \( t = s \), and by [PD] eq. (8), p. 93 and [PD] Theorems 3.5 and 4.2D \( \text{tr} f_i = \frac{1}{|G|} n_i^2 \) (as an element of \( K' \)) for all \( 1 \leq i \leq s = t \). Then by Lemma 4.1 iii), \( V_G \cap Z(KG) \) is a MS of \( KG \), if and only if for each non-empty \( J \subseteq \{1, 2, ..., s\} \) we have

\[
\frac{1}{|G|} \sum_{i \in J} n_i^2 \neq 0_K.
\]

Since \( |G| \neq 0_K \) and \( n_i^2 \in \mathbb{N} \) for all \( 1 \leq i \leq s \), we see that the inequality above holds, if and only if \( \sum_{i \in J} n_i^2 \neq 0 \) (mod \( p \)). Hence statement ii) follows.

iii) By [PD] Theorem 4.2D, p. 99 (noting that the field \( K \) there is our \( \widehat{K} \)), \( \text{tr} f_i = \frac{1}{|G|} \left( \sum_{i=1}^{s_i} n_{i,j}^2 \right) \) (as an element of \( K' \)) for all \( 1 \leq i \leq t \). Then statement iii) follows immediately from Lemma 4.1 iii). \( \square \)

Acknowledgments The authors are grateful to an anonymous referee for some valuable suggestions on an earlier version of the paper. The first author also thanks Sunil Chebolu for some personal communications.

References

[BCW] H. Bass, E. Connell and D. Wright, The Jacobian Conjecture, Reduction of Degree and Formal Expansion of the Inverse. Bull. Amer. Math. Soc. 7, (1982), 287–330.

[DEZ] H. Derksen, A. van den Essen and W. Zhao, The Gaussian Moments Conjecture and the Jacobian Conjecture. Israel J. Math. 219 (2017), no. 2, 917–928. See also arXiv:1506.05192 [math.AC].

[DK] J. J. Duistermaat and W. van der Kallen, Constant Terms in Powers of a Laurent Polynomial. Indag. Math. (N.S.) 9 (1998), no. 2, 221–231.

[E] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture. Prog. Math., Vol.190, Birkhäuser Verlag, Basel, 2000.

[EKC] A. van den Essen, S. Kuroda and A. J. Crachiola, Polynomial Automorphisms and the Jacobian Conjecture: New Results from the Beginning of the 21st Century. Frontiers in Mathematics. Birkhäuser 2021.

[G] D. J. Grynkiewicz, Structural additive theory. Developments in Mathematics. 30. Springer, Cham, 2013.

[I] N. Itô, Some Studies on Group Characters. Nagoya Math. J. 2, (1951), 17–28.
EXISTENCE OF NONZERO TRACE-ZERO IDEMPOTENTS

[Ka] I. Kaplansky, Fields and Rings. Chicago Lectures in Math., Univ. of Chicago Press, 1969.

[Ke] O. H. Keller, Ganze Gremona-Transformationen. Monats. Math. Physik 47 (1939), no. 1, 299-306.

[Ko] A. Konijjenberg, Mathieu Subspaces of Finite Products of Matrix Rings. Master Thesis, Radboud University Nijmegen, The Netherlands, 2012.

[Man] O. Manz, On the Modular Version of Itô-Michler Theorem on Character Degrees for Groups of Odd Order. Nagoya Math. J. Vol. 105 (1987), 121-128.

[Mat] O. Mathieu, Some Conjectures about Invariant Theory and Their Applications. Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), 263–279, Sém. Congr., 2, Soc. Math. France, Paris, 1997.

[Mi1] G.O. Michler, Trace and Defect of a Block Idempotent, J. Alg. 131 (1990) 496-501.

[Mi2] G.O. Michler, Brauer’s Conjectures and the Classification of Finite Simple Groups. Lect. Notes Math. 1178, Springer, Berlin, 1986.

[N1] G. Navarro, Characters and Blocks of Finite Groups. London Mathematical Society Lecture Notes Series, Cambridge University Press, 1998.

[N2] G. Navarro, Variations on the Itô-Michler Theorem on Character Degrees. Rocky Mountain J. Math. V. 46, No. 4 (2016), 1363-1377.

[Pa] D.S. Passman, The Algebraic Structure of Group Rings, Pure and Applied mathematics, A Wiley-Interscience publication. John Wiley and Sons, Inc. 1977.

[Pi] R. S. Pierce, Associative Algebras. Graduate Texts in Mathematics, 88. Springer-Verlag, New York-Berlin, 1982.

[PD] B.M. Puttaswamaiah and J.D. Dixon, Modular representations of finite groups. Pure and Applied mathematics, Academic Press Inc., 1977.

[R] G. R. Robinson, On finite groups with all simple modules of low dimension in characteristic p. arXiv:2009.10602 [math.GR].

[Za] A. E. Zalesskii, On a Problem of Kaplansky. Soviet Math. 13 (1972), 449-452.

[Z1] W. Zhao, Images of Commuting Differential Operators of Order One with Constant Leading Coefficients. J. Alg. 324 (2010), no. 2, 231–247. [MR2651354]. See also arXiv:0902.0210 [math.CV].

[Z2] W. Zhao, Generalizations of the Image Conjecture and the Mathieu Conjecture. J. Pure Appl. Alg. 214 (2010), 1200-1216. See also arXiv:0902.0212 [math.CV].

[Z3] W. Zhao, Mathieu Subspaces of Associative Algebras. J. Alg. 350 (2012), no. 2, 245-272. See also arXiv:1005.4260 [math.RA].

[ZW] W. Zhao and R. Willems, Analogue of the Duistermaat-Van Der Kallen Theorem for Group Algebras. Cent. Eur. J. Math. 10 (3) (2012), 974-986.

W. Zhao, Department of Mathematics, Illinois State University, Normal, IL 61761. Email: wzhao@ilstu.edu

D. Yan, MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, China. Email: yan-dan-hi@163.com