7-1-2022

Mathieu-Zhao Subspaces of Burnside Algebras of Some Finite Groups

Andrew Burak Hatfield
Illinois State University, andrew.hatfield@me.com

MATHIEU-ZHAO SUBSPACES OF BURNSIDE ALGEBRAS OF SOME FINITE GROUPS

ANDREW B. HATFIELD

16 Pages

In 2010, W. Zhao introduced the notion of a Mathieu subspace as a common framework for study of the Jacobian conjecture and related topics. As a generalization of ideals, Mathieu subspaces provide a new viewpoint to investigate the structure of associative algebras and rings. In this paper, we classify Mathieu subspaces of the Burnside algebras $\mathscr{B}_k(G)$ and $\mathscr{B}_k(D_{2p})$ where k is a field of characteristic $p > 0$, $G = H \times K$ for a p-group H and a p'-group K, and D_{2p} is the dihedral group of order $2p$ (for p odd).

KEYWORDS: Mathieu subspaces (Mathieu-Zhao subspaces), Burnside rings (Burnside algebras), finite groups, p-groups, p'-groups, dihedral groups

MATHIEU-ZHAO SUBSPACES OF BURNSIDE ALGEBRAS OF SOME FINITE GROUPS

ANDREW B. HATFIELD

A Thesis Submitted in Partial
Fulfillment of the Requirements
for the Degree of

MASTER OF SCIENCE

Department of Mathematics

ILLINOIS STATE UNIVERSITY

2022

MATHIEU-ZHAO SUBSPACES OF BURNSIDE ALGEBRAS OF SOME FINITE GROUPS

ANDREW B. HATFIELD

COMMITTEE MEMBERS:

Wenhua Zhao, Chair

George F. Seelinger

CONTENTS

Page

CHAPTER I: INTRODUCTION

Let $f_1, \cdots, f_n$ be a set of polynomials over $\mathbb{C}$ in variables $x_1, \cdots, x_n$. Define the polynomial map $F : \mathbb{C}^n \to \mathbb{C}^n$ by

$$F(x_1, \cdots, x_n) = (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots x_n)) .$$

Denote by J_F the Jacobian of F, which is the determinant of the $n \times n$ matrix

$$\mathcal{M} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix} .$$

.

First formulated by O.-H. Keller in 1939, the Jacobian conjecture can be stated as follows.

Conjecture 1.1. *(Keller, [6]) Let $F : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If J_F is a nonzero constant, then F has an inverse polynomial map G.*

Although the statement of the conjecture is quite simple, the conjecture remains today wide open in general with very few special cases proven. For a survey of related results, we refer the reader to [1], [10], and [11].

Although direct proof attempts have been mostly unsuccessful, it has been shown that numerous conjectures imply the Jacobian conjecture. Motivated by Mathieu's conjecture [8] and the Image conjecture [13], W. Zhao introduced in [12] the following notion with the goal of creating a common framework for the study of the Jacobian conjecture and related conjectures.

Definition 1.2. *Let R be a commutative ring and $\mathcal{A}$ be a commutative R-algebra. We say that a subspace $\mathcal{M}$ of $\mathcal{A}$ is a* ***Mathieu subspace*** *of $\mathcal{A}$ if the following condition holds: for*

$a, b \in \mathcal{A}$ with $a^m \in \mathcal{M}$ for all $m \geq 1$, we have $a^m b \in \mathcal{M}$ when $m \gg 0$, i.e. there exists $N \geq 1$ (depending on a, b) such that $a^m b \in \mathcal{M}$ for all $m \geq N$.

Note that Mathieu subspaces are now commonly called Mathieu-Zhao subspaces in the literature.

Several conjectures related to the Jacobian conjecture can be restated in terms of Mathieu-Zhao subspaces (for example, the Mathieu and Image conjecture as in [12]). Mathieu-Zhao subspaces are also a natural generalization of the concept of ideals, and as such, the study of Mathieu-Zhao subspaces of associative algebras and rings has grown into a field of its own. In this paper, we investigate the Mathieu-Zhao subspaces of Burnside algebras of certain classes of finite groups over fields of prime characteristic. We begin by fixing some definitions.

Let G denote a finite group and R a commutative, unital ring. Let S be a finite set and denote by $A(S)$ the symmetric group of all permutations of S. We say that S is a *G-set* if there exists a group homomorphism $\tau : G \to A(S)$. We call τ a group action of G on S and typically write gs to denote $(\tau(g))(s)$ for all $s \in S$.

Let S, T be G-sets. We say that S and T are isomorphic as G-sets if there exists a bijection $f : S \to T$ such that f preserves the group actions of G on S and T, i.e. for any $g \in G$ and $s \in S$, we have $f(gs) = gf(s)$. The Cartesian product of S and T is also a G-set under the diagonal action $g(s,t) = (gs, gt)$ for all $g \in G, (s,t) \in S \times T$. We define the *orbit* of s to be the set $Gs = \{gs \mid g \in G\}$. We say that S is *transitive* if $S = Gs$ for some $s \in S$, or equivalently, the action of G on S has exactly one orbit. Let $s \in S, t \in T$. For transitive G-sets S and T, S and T are isomorphic as G-sets if and only if $\operatorname{stab}(s)$ is conjugate to $\operatorname{stab}(t)$, where $\operatorname{stab}(s) = \{g \in G \mid gs = s\}$ denotes the *stabilizer* (or *isotropy group*) of s [9]. For any G-set S, we may uniquely decompose S into the disjoint union of transitive G-sets which are precisely the orbits of S under the action of G. For any subgroup $H \leq G$, the left coset space G/H defines a transitive G-set with action given by left multiplication. For any $s \in S$, we have $S \cong G/\operatorname{stab}(s)$ if S is transitive.

Let P denote the set of conjugacy classes of subgroups of G. For each $a \in P$, let H_a denote a representative of the class a and $[G/H_a]$ denote the isomorphism class of G/H_a. Let $\mathscr{B}_R(G)$ denote the free R-module generated by the set $\{[G/H_a] \mid a \in P\}$. For any two basis elements $[G/H_a], [G/H_b] \in \mathscr{B}_R(G)$, define

$$[G/H_a] \cdot [G/H_b] = \sum [G/K_i]$$

where the sum is taken over all G-orbits in $G/H_a \times G/H_b$ and K_i is the stabilizer of the ith G-orbit. Extending the product by linearity makes $\mathscr{B}_R(G)$ a commutative ring with identity $[G/G]$, and we call $\mathscr{B}_R(G)$ the *Burnside ring of G over R*. If R is a field, we call $\mathscr{B}_R(G)$ the *Burnside algebra of G over R*. The Burnside ring is named after W. Burnside, who introduced the notion in [2].

We say that a finite group G is a *p-group* for a prime p if $|G| = p^k$ for some k, and say that G is a *p'-group* if $p \nmid |G|$.

Let $\mathcal{A}$ be an associative algebra and $\langle e \rangle$ denote the principal ideal of $\mathcal{A}$ generated by $e \in \mathcal{A}$. In this thesis, we prove the following main theorems.

Theorem 1.3. *Let k be a field of characteristic p and $G = H \times K$ where H is a p-group and K is a p'-group. Let V be a subspace of $\mathscr{B}_k(G)$. Then V is a Mathieu-Zhao subspace of $\mathscr{B}_k(G) \cong \mathscr{B}_k(H) \otimes_k \mathscr{B}_k(K)$ if and only if V contains no nonzero idempotents or $\mathscr{B}_k(H) \otimes \langle j \rangle \subseteq V$ for each nonzero idempotent j of $\mathscr{B}_k(K)$ such that $1 \otimes j \in V$, where $\langle j \rangle$ is the principal ideal of $\mathscr{B}_k(K)$ generated by j.*

Theorem 1.4. *Let p be an odd prime, k be a field of characteristic p, and $\mathcal{A} = \mathscr{B}_k(D_{2p})$. Then $\mathcal{A} \cong e_1\mathcal{A} \times e_2\mathcal{A} \times e_3\mathcal{A}$ for some nonzero idempotents e_i. A subspace V of $\mathcal{A}$ is a Mathieu-Zhao subspace of $\mathcal{A}$ if and only if V contains no nonzero idempotents or $\bigoplus_{j \in J} e_j\mathcal{A} \subseteq V$ for each nonzero idempotent $\sum_{j \in J} e_j$ contained in V, where $J \subseteq \{1, 2, 3\}$.*

The rest of the paper is organized as follows: in Chapter II, we discuss results necessary for the proof of Theorems 1.3 and 1.4. In Chapter III, we prove Theorem 1.3. In Chapter

IV, we prove Theorem 1.4.

CHAPTER II: PRELIMINARIES

The following theorem due to G. Karpilovsky allows the splitting of Burnside rings over the cross product of groups.

Theorem 2.1 (Karpilovsky, [5]). *Let G and H be groups with representatives of all conjugacy classes given by $G_1, \cdots, G_n$ and $H_1, \cdots, H_m$ respectively. Then the map $\phi : \mathscr{B}_{\mathbb{Z}}(G) \otimes_{\mathbb{Z}} \mathscr{B}_{\mathbb{Z}}(H) \to \mathscr{B}_{\mathbb{Z}}(G \times H)$ given by $\phi([G/G_i] \otimes_{\mathbb{Z}} [H/H_j]) = [(G \times H)/(G_i \times H_j)]$ is an injective ring homomorphism. Furthermore, if G and H are of relatively prime order, then ϕ is a ring isomorphism.*

Let p be a prime and let $\mathbb{Z}_p$ denote the field of integers modulo p. The following theorem due to E. Jacobson classifies local Burnside rings of the form $\mathscr{B}_{\mathbb{Z}_p}(G)$ where G is a finite group.

Theorem 2.2 (Jacobson, [4]). *Let G be a finite group. G is a p-group if and only if $\mathscr{B}_{\mathbb{Z}_p}(G)$ is local.*

The following theorem is an analogue of the well-known Maschke's theorem for group algebras. For a unital ring R, we say that $e \in R$ is *idempotent* if $e^2 = e$ and we call e *central* if $eR(1-e) = (1-e)Re = 0$. We say that idempotents e and f are orthogonal if $ef = fe = 0$, and we say that a central idempotent e is *centrally primitive* if $e \neq 0$ and e cannot be written as the sum of two nonzero orthogonal central idempotents in R. Furthermore, we say a set E of orthogonal centrally primitive idempotents is *complete* if $\sum_{e \in E} e = 1$. We note for the Burnside algebras $\mathscr{B}_k(G)$ that all idempotents are central as $\mathscr{B}_k(G)$ is commutative.

Theorem 2.3 (Solomon, [9]). *Let G be a finite group and let k be a field of characteristic 0 or coprime to $|G|$. Then the Burnside algebra $\mathscr{B}_k(G)$ is semisimple and isomorphic to $\bigoplus_{e \in E} ke$ for a complete set of orthogonal centrally primitive idempotents E.*

The following theorem is a standard result for Burnside rings describing the product of G-sets $[G/H]$ and $[G/K]$ such that H, K are normal subgroups of G.

Lemma 2.4. *Let G be a finite group and let k be a field of characteristic p. Let H, K be normal subgroups of G. Then the multiplication of transitive G-sets $[G/H], [G/K]$ in $\mathscr{B}_k(G)$ is given by*

$$[G/H] \cdot [G/K] = \frac{|H \cap K||G|}{|H||K|}[G/H \cap K].$$

Proof. Let $(aH, bK) \in G/H \times G/K$. As H, K are normal, the stabilizer $\text{stab}(aH, bK)$ is given by

$$\text{stab}(aH, bK) = aHa^{-1} \cap bKb^{-1} = H \cap K.$$

Counting the number of elements on both sides gives $[G/H] \cdot [G/K] = \frac{|H \cap K||G|}{|H||K|}[G/H \cap K]$. □

The following theorem due to W. Zhao allows for simple classification of the Mathieu-Zhao subspaces of some algebras given their idempotents. Let k be a field and $\mathcal{A}$ an associative algebra over k. We say $V \subseteq \mathcal{A}$ is *algebraic* over k if every element of V is the root of a monic polynomial with coefficients in k. Denote by $\sqrt{V}$ the radical of V, i.e., the set of all $a \in \mathcal{A}$ such that $a^m \in V$ for sufficiently large m.

Theorem 2.5 (Zhao, [14])**.** *Let k be a field and $\mathcal{A}$ an associative algebra over k. Let V be a k-subspace such that $\sqrt{V}$ is algebraic over k. Then V is a Mathieu-Zhao subspace of $\mathcal{A}$ if and only if for each idempotent $e \in V$, we have the principal ideal $\langle e \rangle \subseteq V$.*

Lemma 2.6. *Let G be a finite group and k be a field. Then $\mathscr{B}_k(G)$ is algebraic.*

Proof. Let $b \in \mathscr{B}_k(G)$. Then the set $\{1, b, b^2, \cdots\}$ must be linearly dependent, so there exists a nonconstant polynomial q such that $q(b) = 0$. Let $\alpha \in k$ be the leading coefficient of q. Then $\alpha^{-1}p(b) = 0$, hence b is algebraic. Therefore, $\mathscr{B}_k(G)$ is algebraic. □

Let p be an odd prime and D_{2p} denote the dihedral group of order $2p$. Write D_{2p} as $\langle r, s \rangle$, where r has order p and s has order 2. In D_{2p}, conjugacy classes of some subgroups are nontrivial. The following theorem due to K. Conrad allows us to classify all subgroups of D_{2p} into one of 4 conjugacy classes.

Theorem 2.7 (Conrad, [3])**.** *Let n be odd and $m \mid 2n$. If m is odd, then all m subgroups of D_{2n} with index m are conjugate. If m is even, then the only subgroup of D_{2n} with index m is $\langle r^{m/2} \rangle$. In particular, all subgroups of D_{2n} with the same index are conjugate to each other.*

The following theorem is a well-known result relating the idempotents of a ring and its decomposition (e.g., [7]).

Theorem 2.8. *Let R be a (not necessarily commutative) ring. Then R can be expressed as a finite direct product of indecomposable rings if and only if $1 \in R$ can be written as a sum of orthogonal centrally primitive idempotents. If such a decomposition exists, each factor of the decomposition of R contains no nontrivial central idempotents.*

Let $G = H \times K$ where H is a p-group and K is a p'-group. Then by Theorem 2.1, we have $\mathscr{B}_k(G) \cong \mathscr{B}_k(H) \otimes_k \mathscr{B}_k(K)$. To find the Mathieu-Zhao subspaces of $\mathscr{B}_k(G)$, we first investigate the idempotents of each of $\mathscr{B}_k(H), \mathscr{B}_k(K)$.

Theorem 3.1. *Let H be a p-group and k be a field of characteristic p. Then $\mathscr{B}_k(H)$ is local.*

Proof. By Theorem 2.2, $\mathscr{B}_{\mathbb{Z}_p}(H)$ is local. As $\mathscr{B}_k(H) = k \otimes_{\mathbb{Z}_p} \mathscr{B}_{\mathbb{Z}_p}(H)$, we see that $\mathscr{B}_k(H)$ must also be local. □

Recall that K is a p'-group. Let $l = \dim_k \mathscr{B}_k(K)$. By Theorem 2.3, $\mathscr{B}_k(K) \cong \oplus_{i=1}^{l} k$, and $\mathscr{B}_k(K)$ has a complete set of primitive idempotents $\{e_1, \cdots, e_l\}$.

In some cases, it is simple to list the primitive idempotents of $\mathscr{B}_k(K)$. Let C_n denote the cyclic group with n elements.

Example 3.2. *Let $K = C_{q^s}$ with q prime and let $f_i = q^{i-s}[K/C_{q^i}]$. Then a complete set of primitive idempotents of $\mathscr{B}_k(K)$ is given by $F = \{f_0, f_1 - f_0, \cdots, f_s - f_{s-1}\}$.*

Proof. For $i \leq j$, we have

$$f_i \cdot f_j = q^{i-s}[K/C_{q^i}] \cdot q^{j-s}[K/C_{q^j}] = q^{i+j-2s} q^{s-j}[K/C_{q^i}] = f_i$$

by Lemma 2.4. Then $f_i^2 = f_i$, and for $i \geq 1$,

$$(f_i - f_{i-1})^2 = f_i^2 - 2f_{i-1} + f_{i-1}^2 = f_i - f_{i-1}.$$

For $1 \leq i \leq s$, we have

$$f_0(f_i - f_{i-1}) = f_0 - f_0 = 0$$

and for $1 \le i < j \le s$,

$$(f_i - f_{i-1})(f_j - f_{j-1}) = f_i - f_{i-1} - f_i + f_{i-1} = 0,$$

thus F is a set of orthogonal idempotents. As $\dim \mathscr{B}_k(K) = s+1 = |F|$, each $f \in F$ must be primitive. As $\sum_{f \in F} f = f_s = 1$, F is a complete set of primitive idempotents as desired. $\square$

We now investigate the idempotents of $\mathscr{B}_k(H) \otimes_k \mathscr{B}_k(K)$.

Lemma 3.3. *Let $\{e_1, \cdots, e_l\}$ be a complete set of orthogonal primitive idempotents of $\mathscr{B}_k(K)$. Then the set $E = \{1 \otimes e_1, \cdots, 1 \otimes e_l\}$ is a complete set of orthogonal primitive idempotents in $\mathscr{B}_k(G) \cong \mathscr{B}_k(H) \otimes_k \mathscr{B}_k(K)$.*

Proof. We have

$$\begin{aligned} \mathscr{B}_k(G) &\cong \mathscr{B}_k(H) \otimes_k \mathscr{B}_k(K) \\ &\cong \mathscr{B}_k(H) \otimes_k \left(\bigoplus_{i=1}^{l} k \right) \\ &\cong \bigoplus_{i=1}^{l} (\mathscr{B}_k(H) \otimes_k k) \\ &\cong \bigoplus_{i=1}^{l} \mathscr{B}_k(H) \end{aligned}$$

as $\mathscr{B}_k(H) \otimes_k k \cong \mathscr{B}_k(H)$. Note that every $1 \otimes e_i \in E$ satisfies $(1 \otimes e_i)^2 = 1 \otimes e_i^2 = 1 \otimes e_i$, so each $1 \otimes e_i$ is idempotent. For $i \neq j$, $(1 \otimes e_i)(1 \otimes e_j) = 1 \otimes e_i e_j = 0$, so the elements of E are pairwise orthogonal. Let $f = (f_i)_{i=1}^{l}$ be an idempotent of $\mathscr{B}_k(G) \cong \bigoplus_{i=1}^{l} \mathscr{B}_k(H)$. Then

$$f = f \cdot \left(\sum_{i=i}^{l} 1 \otimes e_i \right) = \sum_{i=1}^{l} f(1 \otimes e_i).$$

As $\mathscr{B}_k(H)$ is local by Theorem 3.1, any nonzero idempotent f that is not the identity must be in the unique maximal ideal. Similarly, $1 - f$ must also be in the same maximal ideal, which implies 1 is in this maximal ideal. This is a contradiction, thus each f_i is either 0 or 1. Then either $f = 0$ or

$$f = \sum_{j \in J} (1 \otimes e_j) = 1 \otimes \sum_{j \in J} e_j$$

for some $J \subseteq \{1, \cdots, l\}$. As each nonzero idempotent f has such a decomposition, we see that E is a primitive set of idempotents. We have $\sum_{i=1}^{l} 1 \otimes e_l = 1$, so E is a complete set. □

With the idempotents of $\mathscr{B}_k(G)$ clear, Theorem 1.3 becomes a consequence of Theorem 2.5.

Proof of Theorem 1.3. (⇒) Let V be a Mathieu-Zhao subspace of $\mathscr{B}_k(H) \otimes \mathscr{B}_k(K)$. If V contains no nonzero idempotents, then the proof is complete. If V contains a nonzero idempotent, it must be of the form $1 \otimes j$ by Lemma 3.3. As V is a Mathieu-Zhao subspace, $\langle 1 \otimes j \rangle = \mathscr{B}_k(H) \otimes \langle j \rangle$ must be contained in V by Theorem 2.5.

(⇐). Let V be a subspace of $\mathscr{B}_k(H) \otimes \mathscr{B}_k(K)$. Then by Lemma 2.6, $\sqrt{V}$ is algebraic. If V contains no nonzero idempotents, then V is a Mathieu-Zhao subspace by Theorem 2.5. If V contains a nonzero idempotent f, then by Lemma 3.3, $f = 1 \otimes j$ for some idempotent j of $\mathscr{B}_k(K)$. By assumption, $\langle 1 \otimes j \rangle \subseteq V$, so V satisfies Theorem 2.5 and is therefore a Mathieu-Zhao subspace. □

Corollary 3.4. *Let V be a subspace of $\mathscr{B}_k(H)$ not containing 1. Then for any subspace W of $\mathscr{B}_k(K)$, $V \otimes W$ does not contain any nonzero idempotents, hence is a Mathieu-Zhao subspace of $\mathscr{B}_k(G)$.*

Proof. Note that $\sqrt{V \otimes W}$ is algebraic by Lemma 2.6. Let $\{v_1, \cdots, v_m\}$ be a basis of V and let $\{w_1, \cdots, w_n\}$ be a basis of W. If $V \otimes W$ contains a nonzero idempotent f, then by Lemma 3.3, $f = 1 \otimes j$ for some idempotent j in $\mathscr{B}_k(K)$. Then

$$1 \otimes j = \sum_{s,t} \alpha_{s,t} v_s \otimes w_t,$$

for some $\alpha_{s,t} \in k$, so $1 \in \operatorname{span}\{v_1, \cdots, v_m\}$, contradicting the assumption that $1 \notin V$. So $V \otimes W$ contains no nonzero idempotents, and by Theorem 1.3, $V \otimes W$ is a Mathieu-Zhao subspace of $\mathscr{B}_k(G)$. □

Corollary 3.5. *Let W be a subspace of $\mathscr{B}_k(K)$ containing no nonzero idempotents. Then for any subspace V of $\mathscr{B}_k(H)$, $V \otimes W$ contains no nonzero idempotents, hence is a Mathieu-Zhao subspace of $\mathscr{B}_k(G)$.*

Proof. Again, note $\sqrt{V \otimes W}$ is algebraic over k by Lemma 2.6. By Corollary 3.4, we may assume V contains 1. Let $\{v_1, \cdots, v_m\}$ be a basis of V with $v_1 = 1$ and $\{w_1, \cdots, w_n\}$ be a basis of W. Let f be a nonzero idempotent contained in $V \otimes W$. Then by Lemma 3.3, $f = 1 \otimes j$ for some idempotent j in $\mathscr{B}_k(K)$. Then

$$\begin{aligned} f = 1 \otimes j &= \sum_{s,t} \alpha_{s,t} v_s \otimes w_t \\ &= \sum_{t} \alpha_{1,t} 1 \otimes w_t + \sum_{\substack{s,t \\ s \neq 1}} \alpha_{s,t} v_s \otimes w_t, \end{aligned}$$

but as $\{v_s \otimes w_t \mid 1 \leq s \leq m, 1 \leq t \leq n\}$ are linearly independent, we see that the second summand must be 0. Then

$$1 \otimes j = \sum_t 1 \otimes \alpha_{1,t} w_t = 1 \otimes \left(\sum_t \alpha_{1,t} w_t \right)$$

and we see that j is a linear combination of basis vectors of W and therefore $j \in W$. But j is an idempotent and W contains no nonzero idempotents, so we must have $j = 0$. Then $1 \otimes j = 0$, and by Theorem 1.3, $V \otimes W$ is a Mathieu-Zhao subspace of $\mathscr{B}_k(G)$. □

Remark 3.6. *By the Classification Theorem of Finite Abelian Groups, every finite abelian group G is isomorphic to $H \times K$ for some p-group H and p'-group K. Therefore, Theorem 1.3 and Corollaries 3.4 and 3.5 hold for all finite abelian groups.*

CHAPTER IV: MATHIEU-ZHAO SUBSPACES OF $\mathscr{B}_k(D_{2p})$

Throughout this chapter, let p be an odd prime, k be a field of characteristic p, and $G = D_{2p}$ denote the dihedral group of order $2p$. Write G as $\langle r, s\rangle$, where r has order p and s has order 2. Let $\mathcal{A}$ denote the Burnside algebra $\mathscr{B}_k(G)$. As G is not abelian, conjugacy classes of subgroups are sometimes nontrivial, therefore the structure of $\mathcal{A}$ is slightly more complex than the cyclic case.

Let C_n denote the cyclic subgroup of G with n elements and let S be the subgroup $\{1, s\}$. By Theorem 2.7, a complete set of representatives of conjugacy classes of subgroups of G is given by $\{G, C_p, S, C_1\}$. For each representative subgroup H, let T_H denote the class $[G/H]$. Note that C_1, C_p, and G are all normal subgroups of G.

Lemma 4.1. *Let $G = D_{2p}$. The product of G-sets in $\mathcal{A}$ is given by the table below.*

$\cdot$	T_G	T_{C_p}	T_S	T_{C_1}
T_G	T_G	T_{C_p}	T_S	T_{C_1}
T_{C_p}	T_{C_p}	$2T_{C_p}$	T_{C_1}	$2T_{C_1}$
T_S	T_S	T_{C_1}	$T_S - \frac{1}{2}T_{C_1}$	0
T_{C_1}	T_{C_1}	$2T_{C_1}$	0	0

Proof. For the product of G-sets corresponding to normal subgroups, use Lemma 2.4.

For the product of T_S and T_N where N is a normal subgroup of G, note that the stabilizer of a pair $(aS, bN) \in G/S \times G/N$ is given by

$$\operatorname{stab}(aS, bN) = aSa^{-1} \cap bNb^{-1} = aSa^{-1} \cap N.$$

If $N = C_1$ or C_p, then $aSa^{-1} \cap N = C_1$ as all conjugates of S are of the form $\{1, r^i s\}$ for some i. Then every element of $G/S \times G/N$ has stabilizer C_1 and counting the number of elements on both sides gives

$$T_S \cdot [G/N] = \frac{|G||C_1|}{|S||N|}T_{C_1} = \frac{p}{|N|}T_{C_1},$$

which is 0 for $N = C_1$ and T_{C_1} for $N = C_p$. If $N = G$, the G-set T_G is the identity element of $\mathscr{B}_k(G)$ and the product is trivial.

Finally, consider the product $T_S \cdot T_S$. Again, let $(aS, bS) \in G/S \times G/S$. We may assume $a, b \in C_p$. Then

$$\operatorname{stab}(aS, bS) = aSa^{-1} \cap bSb^{-1},$$

so we see that the stabilizer depends on the choice of (aS, bS). The intersection $aSa^{-1} \cap bSb^{-1}$ is trivial unless $aSa^{-1} = bSb^{-1}$, which is the case if and only if $a \equiv b \mod N(S)$ where $N(S)$ denotes the normalizer of S. But $N(S) = S$ in D_{2p}, and therefore (aS, bS) has stabilizer conjugate to S if and only if $a \equiv b \mod S$ if and only if $a = b$, since $ab^{-1} \in S$ if and only if $ab^{-1} = 1$. Then there are p^2 total elements in $G/S \times G/S$, of which p of them have stabilizer conjugate to S and $p^2 - p$ of them have stabilizer conjugate to C_1. Then

$$\begin{aligned}
T_S \cdot T_S &= \frac{|S|}{|G|} p T_S + \frac{|C_1|}{|G|}(p^2 - p) T_{C_1} \\
&= \frac{2p}{2p} T_S + \frac{(p^2 - p)}{2p} T_{C_1} \\
&= T_S + \frac{p-1}{2} T_{C_1} \\
&= T_S - \frac{1}{2} T_{C_1}
\end{aligned}$$

as k has characteristic p. ☐

Lemma 4.2. *Let $e_1 = \frac{1}{2}T_{C_p}, e_2 = T_S - \frac{1}{2}T_{C_1}$ and $e_3 = 1 - e_1 - e_2$. Then $E = \{e_1, e_2, e_3\}$ is a complete set of orthogonal primitive idempotents in $\mathcal{A}$.*

Proof. Note that $e_1^2 = (\frac{1}{2}T_{C_p})^2 = \frac{1}{2}T_{C_p}$ and $e_2^2 = (T_S - \frac{1}{2}T_{C_1})^2 = T_S - \frac{1}{2}T_{C_1}$, so e_1 and e_2 are idempotent. Then

$$e_1 e_2 = \left(\frac{1}{2}T_{C_p}\right)\left(T_S - \frac{1}{2}T_{C_1}\right) = \frac{1}{2}T_{C_1} - \frac{2}{4}T_{C_1} = 0,$$

so $e_1e_3 = e_1(1-e_1-e_2) = e_1 - e_1^2 - e_1e_2 = 0$ and $e_2e_3 = e_2(1-e_1-e_2) = e_2 - e_2e_1 - e_2^2 = 0$ and we see the elements of E are pairwise orthogonal. Then e_3 is also idempotent, as

$$e_3^2 = (1-e_1-e_2)^2 = 1 - e_1 - e_2 - e_1 + e_1 - e_1e_2 - e_2 - e_2e_1 + e_2 = 1 - e_1 - e_2 = e_3.$$

By Lemma 4.1, $e_1\mathcal{A} = \text{span}\{T_{C_p}, T_{C_1}\}$, $e_2\mathcal{A} = \text{span}\{e_2\}$, $e_3\mathcal{A} = \text{span}\{e_3\}$. Note that $e_2\mathcal{A}, e_3\mathcal{A}$ are simple and therefore e_2, e_3 are primitive. Assume that e_1 is not primitive. Then there exist some orthogonal idempotents f, f' such that $e_1 = f + f'$ and $e_1\mathcal{A} = f\mathcal{A} \oplus f'\mathcal{A}$ with each of $f\mathcal{A}$, $f'\mathcal{A}$ simple. Then

$$\mathcal{A} = f\mathcal{A} \oplus f'\mathcal{A} \oplus e_2\mathcal{A} \oplus e_3\mathcal{A} \cong k \oplus k \oplus k \oplus k,$$

so $\mathcal{A}$ has no nonzero nilpotent element. But $T_{C_1}^2 = 0$ is nilpotent in $\mathcal{A}$, which is a contradiction. As $\sum_{e\in E} e = 1$, we see that E is a complete set of orthogonal primitive idempotents. □

Proof of Theorem 1.4. By Lemma 4.2, $E = \{e_1, e_2, e_3\}$ is a complete set of orthogonal primitive idempotents. Then by Theorem 2.8, we have $\mathcal{A} = \bigoplus_{i=1}^{3} e_i\mathcal{A}$ where the idempotents of each subalgebra $e_i\mathcal{A}$ are exactly 0 and e_i.

($\Rightarrow$) Let V be a Mathieu-Zhao subspace of $\mathcal{A}$. Assume V contains some nonzero idempotent f. Then by Lemma 4.2, $f = \sum_{j\in J} e_j$ where J is a nonempty subset of $\{1, 2, 3\}$. As V is a Mathieu-Zhao subspace, $\langle f\rangle = \bigoplus_{j\in J} e_j\mathcal{A}$ is a subset of V by Theorem 2.5.

($\Leftarrow$) Let V be a subspace of $\mathcal{A}$. By Lemma 2.6, $\sqrt{V}$ is algebraic. If V contains no nonzero idempotents, then V is a Mathieu-Zhao subspace of $\mathcal{A}$ by Theorem 2.5. If V contains a nonzero idempotent f, then by Lemma 4.2, $f = \sum_{j\in J} e_j$ for some nonempty subset J of $\{1, 2, 3\}$. By assumption, $\bigoplus_{j\in J} e_j\mathcal{A}$ is contained in V, therefore V satisfies Theorem 2.5 and is a Mathieu-Zhao subspace. □

REFERENCES

[1] H. Bass, E. H. Connell, and D. Wright. The Jacobian Conjecture: Reduction of Degree and Formal Expansion of the Inverse. *Bulletin (New Series) of the American Mathematical Society*, 7(2):287 – 330, 1982.

[2] W. Burnside. On the Representation of a Group of Finite Order as a Permutation Group, and on the Composition of Permutation Groups. *Proceedings of the London Mathematical Society*, 1(1):159–168, 1901.

[3] K. Conrad. Dihedral Groups II. https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf, 2009. Accessed: 2022-7-27.

[4] E. Jacobson. The Burnside Ring Modulo a Prime. *Journal of Algebra*, 99(1):58–71, 1986.

[5] G. Karpilovsky. Group Representations, volume 4 of *Ecosystems of the World*. North-Holland, 1992.

[6] O.-H. Keller. Ganze Cremona-Transformationen. *Monatshefte für Mathematik und Physik*, 47, 1939.

[7] T. Y. Lam. A First Course in Noncommutative Rings, volume 131 of *Grad. Texts in Math*. Springer New York, NY, 2001.

[8] O. Mathieu. Some Conjectures about Invariant Theory and their Applications. *Algebre non commutative, groupes quantiques et invariants (Reims, 1995)*, 2:263–279, 1995.

[9] L. Solomon. The Burnside Algebra of a Finite Group. *J. Combinatorial Theory*, 2:603–615, 1967.

[10] A. van den Essen. Polynomial Automorphisms and the Jacobian Conjecture. In *Algèbre non commutative, groupes quantiques et invariants, septiéme contact*, 1995.

[11] A. van den Essen, S. Kuroda, and A. J. Crachiola. Polynomial Automorphisms and the Jacobian Conjecture. Birkhäuser Cham, 2021.

[12] W. Zhao. Generalizations of the Image Conjecture and the Mathieu Conjecture. *Journal of Pure and Applied Algebra*, 214(7):1200–1216, 2010.

[13] W. Zhao. Images of Commuting Differential Operators of Order One with Constant Leading Coefficients. *Journal of Algebra*, 324(2):231–247, 2010.

[14] W. Zhao. Mathieu Subspaces of Associative Algebras. *Journal of Algebra*, 350(1):245–272, 2012.