ANALOGUE OF THE DUISTERMAAT-VAN DER KALLEN THEOREM FOR GROUP ALGEBRAS

WENHUA ZHAO AND ROEL WILLEMS

Abstract. Let G be a group, R an integral domain, and V_G the R-subspace of the group algebra $R[G]$ consisting of all the elements of $R[G]$ whose coefficient of the identity element 1_G of G is equal to zero. Motivated by the Mathieu conjecture [M], the Duistermaat-van der Kallen theorem [DK], and also by recent studies on the notion of Mathieu subspaces introduced in [Z4] and [Z6], we show that for finite groups G, V_G under certain conditions also forms a Mathieu subspace of the group algebra $R[G]$. We also show that for the free abelian groups $G = \mathbb{Z}^n$ $(n \geq 1)$ and any integral domain R of positive characteristic, V_G fails to be a Mathieu subspace of $R[G]$, which is equivalent to saying that the Duistermaat-van der Kallen theorem [DK] cannot be generalized to any field or integral domain of positive characteristic.

1. Introduction

Let's first recall the following notion introduced recently by the first author in [Z4] and [Z6], which can be viewed as a natural generalization of the notion of ideals.

Definition 1.1. *Let R be a commutative ring and $\mathcal{A}$ an associative R-algebra. A R-submodule or R-subspace M of $\mathcal{A}$ is said to be a left (resp., right; two-sided) Mathieu subspace of $\mathcal{A}$ if for any $a, b, c \in \mathcal{A}$ with $a^m \in M$ for all $m \geq 1$, we have $ba^m \in M$ (resp., $a^m b \in M$; $ba^m c \in M$) when $m \gg 0$, i.e., there exists $N \geq 1$ such that $ba^m \in M$ (resp., $a^m b \in M$; $ba^m c \in M$) for all $m \geq N$.*

Two-sided Mathieu subspaces will also simply be called Mathieu subspaces. A R-subspace M of $\mathcal{A}$ is said to be a *pre-two-sided* Mathieu

Date: September 30, 2010.

2000 *Mathematics Subject Classification.* 16S34, 16N40, 16D99.

Key words and phrases. Duistermaat-van der Kallen Theorem, Mathieu subspaces, groups algebras.

The first author has been partially supported by NSA Grant H98230-10-1-0168 and the second author is funded by Phd-grant of council for the physical sciences, Netherlands Organization for scientific research (NWO).

subspace of $\mathcal{A}$ if it is both left and right Mathieu subspace of $\mathcal{A}$. Note that the *pre-two-sided* Mathieu subspaces were previously called *two-sided* Mathieu subspace or *Mathieu subspaces* in [Z4].

The introduction of the notion of Mathieu subspaces in [Z4] and [Z6] was mainly motivated by the studies of *the Jacobian conjecture* [K] (see also [BCW] and [E1]), *the Mathieu conjecture* [M], *the vanishing conjecture* [Z1], [Z2], [Z5], [EWiZ] and more recently, *the image conjecture* [Z3] as well as many other related open problems. For some recent developments on Mathieu subspaces, see [Z6], [FPYZ], [EWrZ1], [EWrZ2], [EZ] and [Z7]. For a recent survey on the *the image conjecture* and it's connections with some other problems, see [E2].

The notion was named after Olivier Mathieu in [Z4] due to his conjecture mentioned above, which now in terms of the new notion can be re-stated as follows.

Conjecture 1.2. (**The Mathieu Conjecture**) *Let G be a compact connected real Lie group with the Haar measure σ. Let $\mathcal{A}$ be the algebra of complex-valued G-finite functions on G, and M the subspace of $\mathcal{A}$ consisting of $f \in \mathcal{A}$ such that $\int_G f\, d\sigma = 0$. Then M is a Mathieu subspace of $\mathcal{A}$.*

J. Duistermaat and W. van der Kallen [DK] proved *the Mathieu conjecture* for the case of tori, which now can be re-stated as follows.

Theorem 1.3. (**Duistermaat and van der Kallen**) *Let $z = (z_1, z_2, ..., z_n)$ be n commutative free variables and V the subspace of the Laurent polynomial algebra $\mathbb{C}[z^{-1}, z]$ consisting of the Laurent polynomials with no constant term. Then V is a Mathieu subspace of $\mathbb{C}[z^{-1}, z]$.*

Note that despite its innocent looking, the proof of the theorem above is surprisingly difficult. The proof in [DK] uses some heavy machineries such as toric varieties, resolutions of singularities, etc.

To discuss the main motivations and results of this paper, we start with the following observation on the Duistermaat-van der Kallen Theorem above.

Let G be the free abelian group $\mathbb{Z}^n$ ($n \geq 1$). Then the Laurent polynomial algebra $\mathbb{C}[z^{-1}, z]$ can be identified in the obvious way with the group algebra $\mathbb{C}[G]$. Under this identification, the subspace $V \subset \mathbb{C}[z^{-1}, z]$ in the theorem corresponds to the subspace V_G of the group algebra $\mathbb{C}[G]$ consisting of the elements of $\mathbb{C}[G]$ whose "*constant term*" (i.e., the coefficient of the identity element 1_G of G) is equal to zero. So, we are naturally led to the following (open) problem.

Problem 1.4. *Let R be a commutative ring and G a group. Let V_G be the R-subspace of the elements of the group algebra $R[G]$ with no* *"constant term", i.e., the coefficient of the identity element 1_G of G is equal to zero. Then under what conditions on R and G, V_G forms a Mathieu subspace of the group algebra $R[G]$?*

The problem above not only provides a different point of view to get further understanding on the remarkable Duistermaat-van der Kallen Theorem, but also gives a family of candidates for Mathieu subspaces, which may provide some new understandings on the still very mysterious notion of Mathieu subspaces. This makes the problem itself very interesting and worthy to investigate.

One of the main results of this paper is that for any finite group G and an integral domain R of characteristic $p = 0$ or $p > |G|$ (the *order* of G), the R-subspace V_G does form a Mathieu subspace of $R[G]$ (see Theorem 3.5), i.e., Problem 1.4 in this case can be solved completely.

However, for the case that $0 < \mathit{char.}\, R = p \leq |G|$, the situation becomes much more subtle. For example, the magic condition $p \nmid |G|$ for the group algebras of finite groups G (e.g., see [P]) does not resolve the difficulty completely, i.e., under this condition V_G still may or may not be a Mathieu subspaces of $R[G]$ (e.g., see Theorem 4.1 and Example 4.2).

In this paper, we first study Problem 1.4 for the group algebras of finite groups G over integral domains R of any characteristics. In particular, besides the main result mention above, for finite abelian groups we also give a complete solution of Problem 1.4 for the case that the base integral domain R satisfies certain primitive root of unity conditions (see Theorems 3.5 and 4.1), e.g., when R is an algebraically closed field.

We then show that for the group algebras of the free abelian groups $G = \mathbb{Z}^n$ $(n \geq 1)$ over any integral domain R of positive characteristic, V_G is not a Mathieu subspace of $R[G]$, by showing that an example suggested by Arno van den Essen does provide a desired counter-example. Consequently, it follows that the Duistermaat-van der Kallen theorem, Theorem 1.3, cannot be generalized to the Laurent polynomial algebra $R[z^{-1}, z]$ over any field or integral domain R of positive characteristic.

The arrangement of this paper is as follows.

In Section 2, we recall some general results on Mathieu subspaces obtained in [Z4] and [Z6], which will be needed later in this paper. In Section 3, we prove some results on Problem 1.4 for the group algebras of finite groups G over arbitrary commutative rings or integral domains. In particular, we show in Theorem 3.5 that when the base ring R is an integral domain of characteristic $p = 0$ or $p > |G|$, the subspace V_G is always a Mathieu subspace of $R[G]$.

In Section 4, we focus on the group algebras of finite abelian groups G over integral domains R of characteristic $p > 0$. The main results of this section is Theorem 4.1, which combining with Theorem 3.5 provides a complete solution of Problem 1.4 for the group algebras of finite abelian groups G over the integral domains R which satisfies a primitive root of unity condition, e.g., when R is an algebraically closed field.

In Section 5, we consider Problem 1.4 for the group algebras of the free abelian groups $\mathbb{Z}^n$ ($n \geq 1$) over an integral domain R of characteristic $p > 0$. We prove that V_G in this case fails to be a Mathieu subspace of $R[\mathbb{Z}^n]$ by showing that the example in Lemma 5.2, which was suggested by Arno van den Essen to the authors, does provide a desired counter-example.

2. Some Results on Mathieu Subspaces

In this section, we recall some general facts on Mathieu subspaces which will be needed later in this paper. Although all the results below with certain modifications hold for all types of Mathieu subspaces (one-sided, pre-two-sided, etc.) We here only focus on the two-sided case, which by Corollary 3.2 in the next section will be enough for our purpose.

Throughout this paper, unless stated otherwise, R and K always stand respectively for a unital commutative ring and a field of any characteristic, and $\mathcal{A}$ a unital algebra over R or K.

Following [Z6], we define for any R-subspace V of a R-algebra $\mathcal{A}$ the *radical*, denoted by $\sqrt{V}$, to be the set of $a \in \mathcal{A}$ such that $a^m \in V$ when $m \gg 0$.

We start with the following equivalent formulation of Mathieu subspaces, which was given in Proposition 2.1 in [Z6].

Proposition 2.1. *Let $\mathcal{A}$ be a R-algebra and V a R-subspace of $\mathcal{A}$. Then V is a Mathieu subspace of $\mathcal{A}$ iff for any $a \in \sqrt{V}$ and $b, c \in \mathcal{A}$, we have $ba^m c \in V$ when $m \gg 0$.*

The following characterization of the Mathieu subspaces with algebraic radicals was also proved in Theorem 4.2 in [Z6].

Theorem 2.2. *Let A be a K-algebra and V a K-subspace of $\mathcal{A}$ such that $\sqrt{V}$ is algebraic over K (i.e., every element of $\sqrt{V}$ is algebraic over K). Then V is a Mathieu subspace of $\mathcal{A}$ iff for any idempotent $e \in V$ (i.e., $e^2 = e$), we have $(e) \subseteq V$, where (e) denotes the ideal of $\mathcal{A}$ generated by e.*

The next proposition is easy to check directly (or see Proposition 2.7 in [Z6]).

Proposition 2.3. *Let I be an ideal of $\mathcal{A}$ and V a R-subspace of $\mathcal{A}$ such that $I \subseteq V$. Then V is a Mathieu subspace of $\mathcal{A}$ iff V/I is a Mathieu subspace of the quotient algebra $\mathcal{A}/I$.*

Finally, let's recall the following family of Mathieu subspaces of the polynomial algebra $K[z]$ in n variables $z := (z_1, z_2, ..., z_n)$, which was given in Proposition 4.6 in [Z4].

Proposition 2.4. *Let $n, d \geq 1$ and R an arbitrary integral domain. Let $S = \{v_1, v_2, ..., v_d\} \subset R^n$ (with d distinct elements) and $0 \neq c_i \in R$ $(1 \leq i \leq d)$. Denote by V the subspace of $f(z) \in R[z]$ such that*

$$\sum_{i=1}^{d} c_i f(v_i) = 0. \tag{2.1}$$

Then V is a Mathieu subspace of $R[z]$ iff for any non-empty subset $J \subset \{1, 2, ..., d\}$, we have [1]

$$\sum_{i \in J} c_i \neq 0. \tag{2.2}$$

Note that the proposition above was only proved in [Z4] under the condition that R is a field. But, it is easy to see that the same proof actually goes through equally well for all integral domains.

3. Some General Results for the Case of Finite Groups

Throughout the rest of this paper, unless stated otherwise, G stands for a finite group, R a commutative ring, and K a field of any characteristic. We denote by $R[G]$ and $K[G]$ the group algebra of G over R and K, respectively. Furthermore, we also fix the following terminologies and notations.

i) We denote by 1 or 1_G the identity element of the group G and also the identity element of the group algebra $R[G]$.

ii) For any $u \in R[G]$, we denote by $\mathrm{Const}(u)$ the coefficient of 1_G of u, and call it the *constant term* of u.

iii) The set of all the elements of $R[G]$ with no constant term will be denoted by $V_{G,R}$, or simply by V_G if the base ring R is clear in the context.

iv) When R is an integral domain, by the *characteristic* of R (denoted by *char.* R) we mean the *characteristic* of the field of fractions of R.

[1] Note that Eq. (2.2) in [Z4] had been misprinted.

Next, we start with the following equivalent formulation of Problem 1.4 for the group algebras of finite groups.

Proposition 3.1. *Let R be any commutative ring and G a finite group. Then V_G is a Mathieu subspace of any fixed type of $R[G]$ iff all elements of $\sqrt{V_G}$ are nilpotent.*

Proof: First, it is easy to see that the ($\Leftarrow$) part follows directly from the assumption and Definition 1.1.

For the ($\Rightarrow$) part, here we only give a proof for the left Mathieu subspace case. The proofs of the other three cases are similar.

Assume that V_G is a left Mathieu subspace and let $u \in \sqrt{V_G}$. Replacing u by a positive power of u, if necessary, we may assume that $u^m \in V_G$ for all $m \geq 1$.

Now, since G is finite, by Definition 1.1 there exists $N \geq 1$ such that $g^{-1}u^m \in V_G$ for all $g \in G$ and $m \geq N$. In particular, for each $g \in G$, the constant term of $g^{-1}u^N$, which is the same as the coefficient of g in u^N, is equal to 0, whence $u^N = 0$, i.e., u is nilpotent.

Another way to show the ($\Rightarrow$) part is as follows.

Assume otherwise and let $u \in \sqrt{V_G}$ such that $u^m \neq 0$ for all $m \geq 1$. Since G is finite, there exists $g \in G$ such that the coefficient of g in u^m is nonzero for infinitely many $m \geq 1$. Then the constant term of $g^{-1}u^m$ is nonzero for infinitely many $m \geq 1$. Then by Definition 1.1 V_G is not a Mathieu subspace of $R[G]$, which is a contradiction. $\square$

Two immediate consequences of Proposition 3.1 are the following two corollaries.

Corollary 3.2. *Let R and G be as in Proposition 3.1. Then V_G is a Mathieu subspace of any fixed type of $R[G]$ iff V_G is a (two-sided) Mathieu subspace of $R[G]$.*

Therefore, throughout the rest of this paper we may and will focus only on the two-sided case.

Corollary 3.3. *Let R and G be as in Proposition 3.1. Assume that V_G is a Mathieu subspace of $R[G]$. Then V_G contains no nonzero idempotent of $R[G]$.*

Proof: Assume otherwise. Let $e \in V_G$ be a nonzero idempotent, i.e., $e^2 = e \neq 0$. Then for any $m \geq 1$, we have $e^m = e \in V_G$, whence $e \in \sqrt{V_G}$. But, since e is clearly not nilpotent, by Proposition 3.1 V_G is not a Mathieu subspace of $R[G]$, which is a contradiction. $\square$

When the base ring R is a field, we show next that the converse of Corollary 3.3 actually also holds.

Proposition 3.4. *Let K be a field and G a finite group. Then V_G is a Mathieu subspace of $K[G]$ iff V_G contains no nonzero idempotent of $K[G]$.*

Proof: The ($\Rightarrow$) part is a special case of Corollary 3.3. To show the ($\Leftarrow$) part, note that $K[G]$ is algebraic over K, since it is of finite dimension over K. In particular, the radical $\sqrt{V_G}$ of V_G is algebraic over K. Then by Theorem 2.2, V_G is a Mathieu subspace of $K[G]$. $\square$

Next, we show that Problem 1.4 can be solved for the group algebras of all finite groups G over integral domains R such that *char.* $R = 0$ or *char.* $R = p > |G|$.

Theorem 3.5. *Let G be a finite group and R an integral domain such that char. $R = 0$ or char. $R = p > |G|$. Then V_G is a Mathieu subspace of $R[G]$.*

Proof: Let $u \in \sqrt{V_G}$. Then by Proposition 3.1 it suffices to show that u is nilpotent. Note that by replacing u by a positive power of u, if necessary, we may assume $u^m \in V_G$, i.e., $\text{Const}\,(u^m) = 0$, for all $m \geq 1$.

Let $\mu : R[G] \to \text{End}_R(R[G])$ be the R-algebra homomorphism which maps each $v \in R[G]$ to the R-endomorphism $m_v \in \text{End}_R(R[G])$ defined by the left multiplication by v on $R[G]$. Then it is easy to check that for any $v \in R[G]$, the trace of the linear map $\mu(v) = m_v$ is equal to $|G|\text{Const}\,(v)$. Consequently, for the $u \in \sqrt{V_G}$ fixed at the beginning and any $m \geq 1$, the trace of the m-th power $(\mu(u))^m = \mu(u^m)$ of the linear transformation $\mu(u)$ is equal to zero.

On the other hand, since *char.* $R = 0$ or *char.* $R = p > |G|$, it is well-known in linear algebra that in this case the linear transformation $\mu(u)$ must be nilpotent, i.e., $(\mu(u))^m = \mu(u^m) = 0$ for $m \gg 0$. Since μ is clearly injective (e.g., by applying $\mu(v)$ to $1 \in R[G]$ for all $v \in R[G]$), we also have $u^m = 0$ when $m \gg 0$, i.e., u is nilpotent, as desired. $\square$

One remark on Theorem 3.5 is that when the conditions *char.* $R = 0$ and *char.* $R = p > |G|$ fail, i.e., when $0 <$ *char.* $R = p \leq |G|$, the situation for Problem 1.4 becomes much more complicated.

For instance, as shown by the next lemma and also by Theorem 4.1 in Section 4, the magic condition $p \nmid |G|$ for the theory of group algebras $R[G]$ of finite groups G (e.g., see [P]) does not resolve the difficulty completely for Problem 1.4.

Lemma 3.6. *Let G be any finite group with $|G| \geq 2$, and R an integral domain of char. $R = p > 0$. Assume $p \mid (|G| - 1)$ (hence, $p \nmid |G|$). Then V_G is not a Mathieu subspace of $R[G]$.*

Proof: Let $u = -\sum_{g\in G\backslash\{1_G\}} g \in V_G$ and $v = 1_G - u = 1 - u$. Note that v is the sum of all the distinct elements of G in $R[G]$. Hence, for any $g \in G$, we have $vg = gv = v$. Consequently, we have $v^2 = |G|v$, which in terms of u is the same as

$$(1-u)^2 = 1 - 2u + u^2 = |G|(1-u).$$

Solving u^2 from the equation above, we get

$$u^2 = (|G|-1) - (|G|-2)u. \tag{3.1}$$

Since $p \,|\, (|G|-1)$, we have $(|G|-1) = 0$ and $(|G|-2) = -1$. Then by Eq. (3.1), we have $u^2 = u$. Since $u \neq 0$, by Corollary 3.3 V_G is not a Mathieu subspace of $R[G]$. $\square$

Next, we show the following lemma that will be needed later.

Lemma 3.7. *Let R be any commutative ring and G any group (not necessarily finite). Assume that V_G is a Mathieu subspace of $R[G]$. Then for each subgroup H of G, V_H is a Mathieu subspace of $R[H]$.*

Proof: Assume otherwise. Let H be a subgroup of G such that V_H is not a Mathieu subspace of $R[H]$. Then by Definition 1.1 and the definition of V_H, there exist $u, v \in R[H]$ such that $\mathrm{Const}\,(u^m) = 0$ for all $m \geq 1$, but $\mathrm{Const}\,(u^m v) \neq 0$ for infinitely many $m \geq 1$.

Since $R[H] \subseteq R[G]$, we have $u, v \in R[G]$, and $u^m \in V_G$ for all $m \geq 1$, but $u^m v \notin V_G$ for infinitely many $m \geq 1$. Hence, V_G is not a Mathieu subspace of $R[G]$, which is a contradiction. $\square$

Corollary 3.8. *Let R and G be as in Lemma 3.7 and H a subgroup of G. Assume that V_H is not a Mathieu subspace of $R[H]$. Then V_G is not a Mathieu subspace of $R[G]$.*

As an application of Lemma 3.7 or Corollary 3.8, we derive the following necessary condition for V_G to be a Mathieu subspace of $R[G]$ over integral domains R of positive characteristic.

Proposition 3.9. *Let R be an integral domain of characteristic $p > 0$ and G an arbitrary finite group. Write $|G| = p^r d$ for some $r \geq 0$ and $d \geq 1$ with $p \nmid d$. Assume that R contains a primitive d-th root of unity and V_G is a Mathieu subspace of $R[G]$. Then for each prime divisor q of $|G|$, we have $p \geq q$.*

Proof: Assume otherwise and let q be a prime divisor of $|G|$ such that $p < q$. Then we have $q \,|\, d$, whence R also contains a primitive q-th root of unity.

Write $|G| = q^s n$ with $s, n \geq 1$ such that $q \nmid n$. Then by the well-known Sylow's theorem in the theory of finite groups (e.g., see p. 105, Theorem 2.11.7 in [He]), G has at least one q-Sylow subgroup H, i.e., a subgroup H of G with $|H| = q^s$.

Now, pick up any non-identity element $h \in H$. Then h has order q^k for some $1 \leq k \leq r$. Let $g = h$ if $k = 1$; and $g = h^{k-1}$ if $k \geq 2$. Then g has order q and hence, generates a cyclic subgroup C_q of G of order $|C_q| = q$. Then by Theorem 4.1 to be proved in Section 4, V_{C_q} is not a Mathieu subspace of $R[C_q]$. Hence, by Corollary 3.8 V_G is not a Mathieu subspace of $R[G]$ either, which is a contradiction. $\square$

Finally, we point out that when the finite group G in Proposition 3.9 is abelian, a much stronger condition will be given in Theorem 4.1 of the next section.

4. **The Case for Finite Abelian Groups**

In this section, we study Problem 1.4 for finite abelian groups over certain integral domains. The main result of this section is the following theorem.

Theorem 4.1. *Let R be an integral domain of characteristic $p > 0$, and G a finite abelian group with $|G| = p^r d$ for some $r \geq 0$ and $d \geq 1$ with $p \nmid d$. Assume that R contains a primitive d-th root of unity. Then V_G is a Mathieu subspace of $R[G]$ iff $p > d$.*

Two remarks on Theorem 4.1 are as follows.

First, when the integral domain R has $\textit{char.}\, R = 0$ (or $\textit{char.}\, R = p > |G|$), Problem 1.4 has been solved by Theorem 3.5, together with which Theorem 4.1 provides a complete solution of Problem 1.4 for the group algebras of all finite abelian groups when the base integral domain R satisfies the primitive root of unity condition in Theorem 4.1, e.g., when R is an algebraically closed field.

Second, from the example below we see that the d-th primitive root of unity condition on the integral domain R in Theorem 4.1 is necessary.

Example 4.2. *Let $\mathbb{F}_3$ be the field with three elements. Note that $\mathbb{F}_3$ obviously does not contain any primitive 5th root of unity. But, $V_{\mathbb{Z}_5}$ is a Mathieu subspace of $\mathbb{F}_3[\mathbb{Z}_5]$, although $\textit{char.}\, \mathbb{F}_3 = 3 < d = 5$.*

Proof: Assume otherwise. Then by Proposition 3.4, there exists a nonzero idempotent $f \in V_{\mathbb{Z}_5}$. By identifying the group algebra $\mathbb{F}_3[\mathbb{Z}_5]$ with the quotient algebra $\mathbb{F}_3[t]/(t^5 - 1)$ of the polynomial algebra $\mathbb{F}_3[t]$ in one variable t, we may write $f = c_1 t + c_2 t^2 + c_3 t^3 + c_4 t^4$. Then it is easy to check that the following equations hold:

$$\mathrm{Const}\,(f^2) = 2(c_1c_4 + c_2c_3),$$
$$f^3 = c_1^3t^3 + c_2^3t + c_3^3t^4 + c_4^3t^2.$$

Since $f^2 = f^3 = f \in V_{\mathbb{Z}_5}$, hence we also have

$$c_1c_4 = -c_2c_3, \tag{4.1}$$

$$c_1 = c_2^3; \quad c_2 = c_4^3; \quad c_3 = c_1^3; \quad c_4 = c_3^3. \tag{4.2}$$

From the four equations in Eq. (4.2), it is easy to see that if one of the c_i's is equal to zero, then so are all the c_i's. Since $f \neq 0$, we see that all the c_i's are nonzero.

By combining equations in Eqs. (4.1)-(4.2), it is also easy to see that $(c_2c_3)^3 = -(c_2c_3)$, whence $(c_2c_3)^2 = -1$. However, the base field $\mathbb{F}_3$ contains no square root of -1. Hence, we get a contradiction. $\square$

Next, we will devote the rest of this section to give a proof for Theorem 4.1. First, we need to show the following reduction lemma.

Lemma 4.3. *Let R be an integral domain of characteristic $p > 0$ and H a finite abelian group. Let $q = p^r$ for some $r \geq 1$ and $G = H \times \mathbb{Z}_q$. Then V_H is a Mathieu subspace of $R[H]$ iff V_G is a Mathieu subspace of $R[G]$.*

Proof: For convenience, we identify $\mathbb{Z}_q$ with the multiplicative cyclic group C_q with q-element. We also identify H and C_q with the subgroups $H \times \{1_{C_q}\}$ and $\{1_H\} \times C_q$ of G, respectively.

Under these identifications, G is also the inner product of its subgroups H and C_q, and the group algebras $R[H]$ and $R[C_q]$ become subalgebras of $R[G]$. Then the $(\Leftarrow)$ part of the lemma follows immediately from Lemma 3.7.

To show the $(\Rightarrow)$ part, pick up any $u \in \sqrt{V_G}$. Then by Proposition 3.1, it suffices to show that u is nilpotent. To do so, replacing u by a positive power of u, if necessary, we assume that $u^m \in V_G$ for all $m \geq 1$.

Write $u = \sum_{s \in C_q} \alpha_s s$ with $\alpha_s \in R[H]$ for each $s \in C_q$. Note that for any $k \geq 1$ and $s \in C_q$, we have $s^{q^k} = 1_{C_q}$, since $|C_q| = q$. Then by the conditions that *char.* $R = p > 0$ and q is a positive power of p, for any $k \geq 1$ we also have

$$u^{q^k} = \sum_{s \in C_q} \alpha_s^{q^k} s^{q^k} = \sum_{s \in C_q} \alpha_s^{q^k} \in R[H].$$

Moreover, since $u^m \in V_G$ for all $m \geq 1$, we have $(u^q)^k = u^{q^k} \in R[H] \cap V_G = V_H$ for all $k \geq 1$, whence $u^q \in \sqrt{V_H}$. Since by assumption V_H is a Mathieu subspace of $R[H]$, applying Proposition 3.1 to the group algebra $R[H]$ we see that u^q is nilpotent, whence so is u. $\square$

Next, let's recall the following well-known fundamental theorem of finite abelian groups.

Theorem 4.4. *Any finite abelian group can be written as a direct product of cyclic groups whose orders are powers of primes.*

For the proof of the theorem above, see any abstract algebra text book (e.g., see Th.2.2, Ch.II, [Hu]).

Note that by applying Theorem 4.4 and Lemma 4.3 (inductively), it is easy to see that we may actually assume that the exponent r in Theorem 4.1 is equal to zero, i.e., it suffices to show the following lemma.

Lemma 4.5. *Let G be a finite abelian group and R an integral domain of characteristic $p > 0$ such that $p \nmid d := |G|$. Assume that R contains a primitive d-th root of unity. Then V_G is a Mathieu subspace of $R[G]$ iff $p > d = |G|$.*

From now on and throughout the rest of this section, we let G and R be as in the lemma above.

Note first that when $d = |G| = 1$, we have $V_G = \{0\}$, which is obviously a Mathieu subspace of $R[G]$. Hence, Lemma 4.5 holds in this trivial case. So we will assume $d = |G| \geq 2$.

Note also that by Theorem 4.4, we may (and will) further assume that the abelian group G is given by

$$G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n} \tag{4.3}$$

for some $n \geq 1$ and $d_i \geq 2$ $(1 \leq i \leq n)$.

But, here we do not need to assume that the integers $d_i \geq 2$ $(1 \leq i \leq n)$ are powers of primes.

In order to study the group algebra $R[G]$ of G in Eq. (4.3), we need to write the factor groups $\mathbb{Z}_{d_i}$ $(1 \leq i \leq n)$ in Eq. (4.3) as multiplicative groups H_i with a fixed generator $e_i \in H_i$, i.e., for each $1 \leq i \leq n$, we let

$$H_i = \{e_i^k \,|\, 0 \leq k \leq d_i - 1\} \simeq \mathbb{Z}_{d_i}. \tag{4.4}$$

For convenience, for each $1 \leq i \leq n$, we also identify H_i (implicitly) with the subgroup of G in Eq. (4.3) consisting of all the n-tuples whose j-th $(j \neq i)$ component being the identity element of $H_j \simeq \mathbb{Z}_{d_j}$. Note that under this identification, we have $H_i \subset G$, whence G is also the *inner product* of the subgroups H_i ($1 \leq i \leq n$), i.e., with the abusive notations fixed above, we have

$$G = H_1 \cdot H_2 \cdots H_n = H_1 \times H_2 \times \cdots \times H_n \tag{4.5}$$

Furthermore, we also need to introduce the following two sets:

$$D := \{\beta = (\beta_1, \beta_2, ..., \beta_n) \in \mathbb{N}^n \,|\, 0 \leq \beta_i \leq d_i - 1\} \tag{4.6}$$

$$S := \left\{a = (a_1, a_2, ..., a_n) \in R^n \mid a_i^{d_i} = 1\right\}. \tag{4.7}$$

Note that since R contains a primitive d-th root of unity, R also contains a primitive d_i-th ($1 \leq i \leq n$) root of unity, since $d_i \,|\, d$. Then from Eqs. (4.6) and (4.7), we have $|S| = d = |D| = |G|$.

Next, with the notations fixed above we give an equivalent formulation of Lemma 4.5 in terms of the polynomial algebra $R[z]$ over R in n variables $z := (z_1, z_2, ..., z_n)$.

First, we define and consider the following R-linear functional:

$$\begin{aligned} \mathcal{L} \colon R[z] &\to \quad R \\ f \quad &\to \sum_{a \in S} f(a). \end{aligned} \tag{4.8}$$

Lemma 4.6. *Let G and R be fixed as above. Then for any $\alpha \in D$, we have*

$$\mathcal{L}(z^\alpha) = \begin{cases} d & \text{if } \alpha = 0; \\ 0 & \text{if } \alpha \neq 0. \end{cases} \tag{4.9}$$

Proof: If $\alpha = 0$, then $\mathcal{L}(z^\alpha) = \sum_{a \in S} 1 = |S| = d$. So we let $\alpha \neq 0$. Without losing any generality, we assume that the first component of α is nonzero, and denote it by k (for short).

Let ξ_1 be a primitive d_1-th root of unity in R. Then we have $\xi_1^k \neq 1$, since $1 \leq k \leq d_1 - 1$. Note that for each root $1 \neq r \in R$ of the polynomial $z_1^{d_1} - 1 \in R[z_1]$, r is also a root of the polynomial $\sum_{\ell=0}^{d_1-1} z_1^\ell$, for $z_1^{d_1} - 1 = (z_1 - 1) \sum_{\ell=0}^{d_1-1} z_1^\ell$. Therefore, for the fixed primitive d_1-th root of unity $\xi_1 \in R$, we have

$$\sum_{\ell=0}^{d_1-1} (\xi_1^\ell)^k = \sum_{\ell=0}^{d_1-1} (\xi_1^k)^\ell = 0. \tag{4.10}$$

Now, for each $1 \leq i \leq n$, set $C_i := \{\xi_i^\ell \,|\, 0 \leq \ell \leq d_i - 1\}$, where ξ_i is any fixed primitive d_i-th root of unity in R. Then from the definition of the set S in Eq. (4.7), we have $S = C_1 \times C_2 \times \cdots \times C_n$. By taking the sum $\mathcal{L}(z^\alpha) = \sum_{a \in S} a^\alpha$ first over the set C_1, it follows immediately from Eq. (4.10) that $\mathcal{L}(z^\alpha) = 0$. $\square$

Next, we define the following R-algebra homomorphism:

$$\begin{aligned} \varphi : R[z] &\to R[G] \\ z_i &\to e_i. \end{aligned} \tag{4.11}$$

Note that the kernel of the R-algebra homomorphism φ above is the ideal of $R[z]$ generated by the polynomials $z_i^{d_i} - 1$ ($1 \leq i \leq n$). We will denote this ideal by $I_{\vec{d}}$, where $\vec{d}$ stands for the n-tuple $(d_1, d_2, ..., d_n)$.

The pre-image of $V_G \subset R[G]$ under the linear map φ is given by the following lemma.

Lemma 4.7. *With the setting above, we have*

$$\varphi^{-1}(V_G) = \text{Ker } \mathcal{L}. \tag{4.12}$$

Proof: First, let V_0 be the R-subspace of $R[z]$ spanned by z^α ($0 \neq \alpha \in D$) and $V := R \cdot 1 \oplus V_0$. Then by the definition of φ in Eq. (4.11), it is easy to see that we have

$$\varphi^{-1}(V_G) = \left\{ f \in R[z] \,\middle|\, f \equiv r \pmod{I_{\vec{d}}} \text{ for some } r \in V_0 \right\}. \tag{4.13}$$

Therefore, it suffices to show that Ker $\mathcal{L}$ coincides with the set on the right-hand side of the equation above.

Now, let $f \in R[z]$. Then there exists a unique $r \in V$ such that $f \equiv r \pmod{I_{\vec{d}}}$. By Eq. (4.13) we have

$$f \in \varphi^{-1}(V_G) \quad \Leftrightarrow \quad r \in V_0. \tag{4.14}$$

Furthermore, since S is the zero-set of the ideal $I_{\vec{d}}$ in R^n, we have $f(a) = r(a)$ for all $a \in S$. In particular, we have $\mathcal{L}(f) = \mathcal{L}(r)$ and hence,

$$f \in \operatorname{Ker} \mathcal{L} \quad \Leftrightarrow \quad r \in \operatorname{Ker} \mathcal{L}. \tag{4.15}$$

Write $r(z) = \sum_{\alpha \in D} c_\alpha z^\alpha$. Then by Eq. (4.9) we have

$$\mathcal{L}(r) = \mathcal{L}(c_0) + \sum_{0 \neq \alpha \in D} c_\alpha \mathcal{L}(z^\alpha) = dc_0.$$

Since $p \nmid d$, we see that $r \in \operatorname{Ker} \mathcal{L}$ iff $c_0 = 0$ iff $r \in V_0$. Then by the equivalences in Eqs. (4.14) and (4.15), we have that $f \in \varphi^{-1}(V_G)$ iff $f \in \operatorname{Ker} \mathcal{L}$, whence the lemma follows. $\square$

Finally, we can give a proof for Lemma 4.5 as follows, from which the proof of the main result Theorem 4.1 will be completed.

Proof of Lemma 4.5: Note that the ($\Leftarrow$) part of the lemma follows directly from Theorem 3.5, which actually does not need the primitive root of unity condition on R in the lemma. But, with the primitive root of unity condition on R it also follows from the arguments below.

First, we consider the R-homomorphism $\varphi : R[z] \to R[G]$ defined in Eq. (4.11). Note that φ is surjective with the kernel $I_{\vec{d}}$. Hence, from Eq. (4.12) we have $I_{\vec{d}} \subseteq \operatorname{Ker}\mathcal{L}$ and $\varphi(\operatorname{Ker}\mathcal{L}) = V_G$.

Therefore, we may identify $R[G]$ with the quotient algebra $R[z]/I_{\vec{d}}$, and V_G with $\operatorname{Ker}\mathcal{L}/I_{\vec{d}}$. Via these identifications and by Proposition 2.3, we have that V_G is a Mathieu subspace of $R[G]$, iff $\operatorname{Ker}\mathcal{L}$ is a Mathieu subspace of the polynomial algebra $R[z]$.

Second, by applying Proposition 2.4 to the set S in Eq. (4.7) with $c_i = 1$ $(1 \leq i \leq d)$, we have that $\operatorname{Ker}\mathcal{L}$ is a Mathieu subspace of $R[z]$, iff for any non-empty subset $J \subseteq \{1, 2, ..., d\}$, the cardinal number $|J| \neq 0$ in R, i.e., $|J| \not\equiv 0 \mod p$. Furthermore, it is easy to see that the latter property holds iff $p > d = |G|$.

Finally, by combining the three equivalences above, we see that the lemma follows. $\square$

5. **The Case for the Group Algebra** $R[\mathbb{Z}^n]$ **with** *char.* $R = p > 0$

In this section, we show that Problem 1.4 has a negative answer for the group algebras of the free abelian groups $\mathbb{Z}^n$ $(n \geq 1)$ over all integral domains R of positive characteristics. More precisely, we have the following proposition.

Proposition 5.1. *For any integral domain R of char. $R = p > 0$, $V_{\mathbb{Z}^n}$ is not a Mathieu subspace of the group algebra $R[\mathbb{Z}^n]$.*

Note that under the natural identification $R[\mathbb{Z}^n] \simeq R[z^{-1}, z]$ (the Laurent polynomial algebra in n variables $z = (z_1, z_2, ..., z_n)$ over R), the proposition above is equivalent to saying that for any integral domain R of *char.* $R = p > 0$, the subspace V of all the Laurent polynomials in $R[z^{-1}, z]$ with no constant term does not form a Mathieu subspace of the Laurent polynomial algebra $R[z^{-1}, z]$. In particular, it follows that the Duistermaat-van der Kallen Theorem, Theorem 1.3, cannot be generalized to any field of characteristic $p > 0$.

To show Proposition 5.1, note first that we may identify $\mathbb{Z}$ as the subgroup of $\mathbb{Z}^n$ consisting of all the elements $(a, a, ..., a) \in \mathbb{Z}^n$ with $a \in \mathbb{Z}$. Then by Corollary 3.8, we may actually assume $n = 1$. Furthermore, via the identification $R[\mathbb{Z}] \simeq R[z, z^{-1}]$ mentioned above, it will be enough to show the following lemma. The example in the lemma was suggested to the authors by Arno van den Essen.

Lemma 5.2. *Let p be a prime and z a free variable. Set $f := z^{-1} + z^{p-1} \in \mathbb{Z}_p[z^{-1}, z]$. Then the following two statements hold:*

i) $\mathrm{Const}\,(f^m) = 0$ *for all* $m \geq 1$;
ii) $\mathrm{Const}\left(z^{-1} f^{p^k-1}\right) = (-1)^{p^{k-1}}$ *for all* $k \geq 1$.

In order to prove the lemma above, we need first to show the following lemma.

Lemma 5.3. *For any prime number* $p > 0$*, the following statements hold.*

i) For any $k, a \in \mathbb{N}$ *such that* $k \geq 1$ *and* $a \leq p^k - 1$*, we have*

$$\binom{p^k-1}{a} \equiv (-1)^a \mod p. \tag{5.1}$$

ii) For any integer $b \geq 1$*, we have*

$$\binom{bp}{b} \equiv 0 \mod p. \tag{5.2}$$

Proof: i) Let x be a free variable. We consider the polynomial $(x-1)^{p^k-1}$ in the rational function field $\mathbb{Z}_p(x)$, for which we have the following two equations:

$$(1-x)^{p^k-1} = \sum_{a=0}^{p^k-1} (-1)^a \binom{p^k-1}{a} x^a, \tag{5.3}$$

$$(1-x)^{p^k-1} = \frac{(1-x)^{p^k}}{1-x} = \frac{1-x^{p^k}}{1-x} = \sum_{a=0}^{p^k-1} x^a. \tag{5.4}$$

Note that Eq. (5.4) above also holds for the case $p = 2$, since $1 = -1$ in $\mathbb{Z}_2$. Now, by comparing the coefficients of x^a in the polynomials on the right-hand sides of Eqs. (5.3) and (5.4), we see that *i)* follows.

ii) Write $b = p^r n$ for some $r \geq 0$ and $n \geq 1$ such that $p \nmid n$. In particular, we have $p^{r+1} \nmid b$.

We consider the polynomial $(x+1)^{bp} \in \mathbb{Z}_p[x]$. Note that the coefficient of x^b in $(x+1)^{bp}$ is equal to $\binom{bp}{b}$. On the other hand, we also have

$$(x+1)^{bp} = (x+1)^{np^{r+1}} = (x^{p^{r+1}} + 1)^n.$$

Now, assume that $\binom{bp}{b} \not\equiv 0 \mod p$. Then by the equation above, x^b appears in the polynomial $(x^{p^{r+1}} + 1)^n$ with a nonzero coefficient, whence $b = p^{r+1}k$ for some $1 \leq k \leq n$. But this implies $p^{r+1} \,|\, b$, which is a contradiction. $\square$

Proof of Lemma 5.2: i) Since $f = z^{-1} + z^{p-1}$, the constant term of f^m $(m \geq 1)$ is given by the sum of $\binom{m}{b}$ for all the integers $0 \leq b \leq m$

such that $-(m-b)+b(p-1)=0$, which is the same as $m=bp$. Therefore, there is at most one such an integer b, which is m/p if (and only if) $p\,|\,m$. Hence we have

$$\text{Const}\,(f^m)=\begin{cases}\binom{bp}{b} & \text{if } p\,|\,m \text{ and } b=m/p;\\ 0 & \text{if } p\nmid m.\end{cases} \tag{5.5}$$

Then from the equation above and Eq. (5.2), we see that $i)$ follows.

$ii)$ By a similar argument as in $i)$, it is easy to check that for any $k\geq 1$, the coefficient of z in f^{p^k-1} is given by $\binom{p^k-1}{p^{k-1}}$, which by Eq. (5.1) is equal to $(-1)^{p^{k-1}}$. Hence, we have $\text{Const}\,(z^{-1}f^{p^k-1})=(-1)^{p^{k-1}}$ for all $k\geq 1$, i.e., $ii)$ holds. □

Acknowledgments The authors are very grateful to Professor Arno van den Essen for suggesting the example in Lemma 5.2.

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. [MR 83k:14028].

[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. [MR1691479].

[E1] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture.* Progress in Mathematics, 190. Birkhäuser Verlag, Basel, 2000. [MR1790619].

[E2] A. van den Essen, *The Amazing Image Conjecture.* Preprint. See arXiv:1006.5801v1 [math.AG].

[EWiZ] A. van den Essen, R. Willems and W. Zhao, *Some Results on the Vanishing Conjecture of Differential Operators with Constant Coefficients.* Under submission. See also arXiv:0903.1478 [math.AC].

[EWrZ1] A. van den Essen, D. Wright and W. Zhao, *Images of Locally Finite Derivations of Polynomial Algebras in Two Variables.* Under submission. See also arXiv:1004.0521v1 [math.AC].

[EWrZ2] A. van den Essen, D. Wright and W. Zhao, *On the Image Conjecture.* Preprint. See arXiv:1008.3962 [math.RA].

[EZ] A. van den Essen and W. Zhao, *Mathieu Subspaces of Univariate Polynomial Algebras.* In preparation.

[FPYZ] J. P. Francoise, F. Pakovich, Y. Yomdin and W. Zhao, *Moment Vanishing Problem and Positivity: Some Examples.* To appear in *Bulletin des Sciences Mathématiques.* doi:10.1016/j.bulsci.2010.06.002.

[He] I. N. Herstein, *Abstract Algebra* (3rd ed.). With a preface by Barbara Cortzen and David J. Winter. Prentice Hall, Inc., Upper Saddle River, NJ, 1996. [MR1375019].

[Hu] T.W. Hungerford, *Algebra.* Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980. [MR0600654].

[K] O. H. Keller, *Ganze Gremona-Transformationen.* Monats. Math. Physik **47** (1939), no. 1, 299-306. [MR1550818].

[M] O. Mathieu, *Some Conjectures about Invariant Theory and Their Applications.* Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), 263–279, Sémin. Congr., 2, Soc. Math. France, Paris, 1997. [MR1601155].

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

[Z1] W. Zhao, *Hessian Nilpotent Polynomials and the Jacobian Conjecture*, Trans. Amer. Math. Soc. **359** (2007), no. 1, 249–274 (electronic). [MR2247890]. See also math.CV/0409534.

[Z2] W. Zhao, *A Vanishing Conjecture on Differential Operators with Constant Coefficients*, Acta Mathematica Vietnamica, vol 32 (2007), no. 3, 259–286. [MR2368014]. See also arXiv:0704.1691v2 [math.CV].

[Z3] W. Zhao, *Images of Commuting Differential Operators of Order One with Constant Leading Coefficients.* J. Alg. **324** (2010), no. 2, 231–247. See also arXiv:0902.0210 [math.CV].

[Z4] W. Zhao, *Generalizations of the Image Conjecture and the Mathieu Conjecture.* J. Pure Appl. Algebra. **214** (2010), no. 7, 1200–1216. [MR2586998]. See also arXiv:0902.0212v3 [math.CV].

[Z5] W. Zhao, *New Proofs for the Abhyankar-Gurjar Inversion Formula and the Equivalence of the Jacobian Conjecture and the Vanishing Conjecture.* To appear in *Proc. AMS.* See also arXiv:0907.3991 [math.AG].

[Z6] W. Zhao, *Mathieu Subspaces of Associative Algebras.* Under Submission. See also arXiv:1005.4260 [math.RA].

[Z7] W. Zhao, *A Generalization of Mathieu Subspaces to Modules of Associative Algebras.* To appear in *Centr. Eur. J. Math.*. See also arXiv:1005.4259 [math.RT].

W. Zhao, Illinois State University, Normal, IL 61790-4520, USA. *Email*: wzhao@ilstu.edu

R. Willems, Radboud University Nijmegen, Postbus 9010, 6500 GL Nijmegen, The Netherlands. *Email*: r.willems@math.ru.nl