Noether Numbers via Jordan Blocks in the Theory of Modular Vector Invariants

Uğur Madran

Izmir University of Economics
Department of Mathematics
Balçova, 35330 Izmir, Turkey
ugur.madran@ieu.edu.tr, madran@member.ams.org

Abstract. Let $G$ be a finite group acting on a vector space $V$ over a field $F$ where the characteristic of the field divides the group order. The polynomial invariants of the diagonal action of $G$ on $\bigoplus_m V$ is known to be unbounded when $m \to \infty$. In this note, we express a lower bound for the $\beta$-number in terms of Jordan decomposition of an element of order $p = \text{char } F$.

Mathematics Subject Classification: Primary 13A50

Keywords: Invariant theory, Noether number, Jordan blocks, vector invariants

1. Introduction

Let $G$ be finite group and $\rho : G \to \text{GL}(V)$ be a faithful representation where $V$ is an $n$-dimensional vector space over a field $F$ of characteristic $p$, such that $p$ divides the group order. For any positive integer $m$, $G$ acts diagonally on the polynomial ring

$$F[\bigoplus_m V] = F[x_{i,1}, \ldots, x_{1,n}, \ldots, x_{m,1}, \ldots, x_{m,n}]$$

by algebra automorphisms given by

$$
\begin{bmatrix}
  g \cdot x_{i,1} \\
  g \cdot x_{i,2} \\
  \vdots \\
  g \cdot x_{i,n}
\end{bmatrix} =
\begin{bmatrix}
  g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\
  g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\
  \vdots & \vdots & \ddots & \vdots \\
  g_{n,1} & g_{n,2} & \cdots & g_{n,n}
\end{bmatrix}
\begin{bmatrix}
  x_{i,1} \\
  x_{i,2} \\
  \vdots \\
  x_{i,n}
\end{bmatrix}
$$

by
for all $1 \leq i \leq m$, where $\rho(g) = [g_{i,j}] \in \text{GL}(n, \mathbb{F}) \simeq \text{GL}(V)$. The ring of vector invariants is defined as

$$\mathbb{F}[\oplus_m V]^G = \{ f \in \mathbb{F}[\oplus_m V] \mid g \cdot f = f \forall g \in G \}.$$ 

The ring of invariants is known to be a finitely generated algebra, due to a result of Noether ([10]). One of the main objects in the study of polynomial invariants is the so-called Noether number or $\beta$-number, which is defined as the maximum degree of a polynomial in a minimal generating set. In the nonmodular case, i.e., when the order of $G$ is invertible in $\mathbb{F}$, then $\beta(\mathbb{F}[V]^G) \leq |G|$ by a well-known result of Noether ([9]) in characteristic zero, which was extended to the positive characteristic by Fleischmann ([4]) and Fogarty ([5]). We direct the reader to excellent books [1], [3], [8] for a detailed introduction to the theory.

In the modular case, i.e., when the characteristic of the field divides the order of the group, Richman proved in [11] that

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq \max\{2, \frac{m}{n-1}, \frac{m}{|G|-1}, \frac{p}{p-1} \cdot \frac{m}{n}\};$$

(1)

when $\mathbb{F}$ is the prime field.

Our aim, in this paper, is to refine this lower bound by using Jordan decomposition of an element of order $p$. More precisely, if an element of order $p$ in $G$ is represented by a matrix whose Jordan canonical form consists of $s$ blocks of elementary Jordan matrices such that $r \leq s$ of them are nontrivial, then

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq \frac{m-s+r}{n-s};$$

(2)

1.1. Notation. For the convenience of the reader, we will mostly use the notations of [7]. Throughout this paper, $\mathbb{F}$ will denote the prime field of characteristic $p$ and moreover, we will identify $G$ with its image $\rho(G)$ in $\text{GL}(n, \mathbb{F})$.

The indeterminates of the polynomial ring $\mathbb{F}[\oplus_m V]$ correspond to elements of the dual basis, i.e., $\{x_{i,1}, \ldots, x_{i,n}\}$ is a basis of $V^*$ corresponding to the dual space of the $i$-th copy of $V$ in $\oplus_m V$.

2. JORDAN BLOCK

Let $g \in G \leq \text{GL}(n, \mathbb{F})$ be a matrix of order $p$. Since, $(g-1)^p = g^p - 1 = 0$, the Jordan canonical form of $g$ can be given as

$$\begin{bmatrix}
J_1 \\
J_2 \\
\vdots \\
J_s
\end{bmatrix}$$
where $J_i$’s are elementary Jordan matrices of order $n_i \times n_i$

\[
J_i = \begin{bmatrix}
1 & 1 & 0 & \ldots & 0 \\
0 & 1 & 1 & \ldots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & 1 & 1 \\
0 & 0 & \ldots & 0 & 1
\end{bmatrix}
\]

such that $p \geq n_1 \geq n_2 \geq \cdots \geq n_r > n_{r+1} = \cdots = n_s = 1$. The size of the largest elementary block cannot exceed $p$ since $g \in G$ is chosen to be an element of order $p$.

Without loss of generality, by changing basis elements, we may assume that

\[
g = \begin{bmatrix}
J_1 \\
J_2 \\
\vdots \\
J_s
\end{bmatrix}
\]

and hence we can explicitly state invariant variables. For the sake of simplicity of the notations, we define the following index sets which depend on the Jordan decomposition above.

Let $\mathcal{I} = \{1, 2, \ldots, m\}$ and $\mathcal{J} = \{1, 2, \ldots, n\}$ be index sets. For $1 \leq j \leq s$, define

\[
\nu_j = \sum_{k \leq j} n_k
\]

with the convention $\nu_0 = 0$, and then set

\[
\mathcal{J}_0 = \{\nu_r + 1, \nu_r + 2, \ldots, n\},
\]

\[
\mathcal{J}_1 = \{1, n_1 + 1 = \nu_1 + 1, \nu_2 + 1, \ldots, \nu_{r-1} + 1\},
\]

\[
\mathcal{J}_2 = \{n_1 = \nu_1, \nu_2, \ldots, \nu_r\}.
\]

Note that $\mathcal{I} \times (\mathcal{J}_0 \cup \mathcal{J}_2)$ lists all invariant variables. Moreover, the first partition of a set, $\mathcal{J}_0$, lists invariant variables which may split off, i.e.,

\[
\mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \in \mathcal{J}]^P = \mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \notin \mathcal{J}_0]^P \otimes \mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \in \mathcal{J}_0].
\]

where $P = \langle g \rangle$ is the cyclic group of order $p$ generated by $g$.

### 3. Leading Terms

We say that a variable $x_{i,j} \prec x_{k,l}$ if $(i, j) > (k, l)$ lexicographically, and we will extend the ordering $\prec$ to monomials by considering the graded lexicographical order induced by $\prec$. More precisely, the ordering is induced by:

\[
x_{1,1} \succ x_{1,2} \succ \cdots \succ x_{1,n} \succ x_{2,1} \succ x_{2,2} \succ \cdots \succ x_{m,n}.
\]

The leading monomial of a polynomial $f$ will be denoted by $\text{LM}(f)$. The term ordering defined above is compatible with the action of $g$ in the sense that $\text{LM}(f) \succeq \text{LM}(g(f))$. We direct the reader to [2] for a detailed discussion of monomial orders.
Proposition 1. Let $f \in \mathbb{F}[x_{1,1}, \ldots, x_{m,n}]^P$. If the degree of $f$ with respect to each vector $(x_{1,1}, \ldots, x_{i,n})$ is at most $p - 1$, and $f \not\in \mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \in \mathcal{J}_0 \cup \mathcal{J}_2]$ then there exists $(i_0, j_0)$ such that $x_{i_0,j_0}$ divides $\text{LM}(f)$ and $j_0 \in \mathcal{J}_2$.

Proof. Suppose for contradiction that none of the $x_{i,j}$ for $1 \leq i \leq n$, and $j \in \mathcal{J}_2$ divide $\text{LM}(f)$. Let $x_{i,j_1}$ be the smallest variable dividing $\text{LM}(f)$ with respect to monomial order given. Consider the monomial

$$w = \frac{\text{LM}(f)}{x_{i_1,j_1}} \cdot x_{i_1,j_1+1}.$$  

Note that $g \cdot (x_{i_1,j_1}) = x_{i_1,j_1} + x_{i_1,j_1+1}$ as $j_1 \notin \mathcal{J}_2$ and also note that there does not exist any monomial $u$ satisfying $\text{LM}(f) \preceq u \preceq w$ (since we consider graded lexicographical order, $\deg u$ is equal to $\deg \text{LM}(f) = \deg w$).

We will show that the coefficient of $w$ in the polynomial $f - g \cdot f$ is not zero, and get a contradiction to the fact that $f$ is invariant and $f - g \cdot f = 0$. But this is straightforward since the coefficient of $w$ in the expansion of $f - g \cdot f$ is $\deg_{(i_1,j_1)} \text{LM}(f)$ by construction and as stated in the hypothesis that this degree is at most $p - 1$, i.e., is nonzero. This completes the proof. \hfill \Box 

4. Main Result

Theorem 2. Let $G$ be a group acting on an $n$-dimensional vector space $V$ over a prime field $\mathbb{F}$ with $p$ elements. Suppose $p$ divides the group order $|G|$, and let $g$ be an element $G$ of order $p$. Then,

$$\beta(\mathbb{F}[\oplus_m V]^G) > \frac{m - s + r}{n - s}$$  

for $m \geq n$ where $r$ is the number of nontrivial Jordan blocks of $g$ and $s$ is the total number of Jordan blocks of $g$.

To prove the theorem, we need the following universal invariant from our previous result [7]. We include it here in full for the convenience of the reader.

For $m \geq n$ define the following auxiliary polynomial:

$$f_0 = \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n} (\alpha_1 x_{1,1} + \cdots + \alpha_n x_{1,n})^{p-1} \cdots (\alpha_1 x_{m,1} + \cdots + \alpha_n x_{m,n})^{p-1}$$

where the sum is over all possible $n$-tuples $(\alpha_1, \ldots, \alpha_n)$. The polynomial $f_0$ is known to be an invariant of the full linear group and hence, $f_0 \in \mathbb{F}[\oplus_m V]^G$ for any $G$.

Definition 3. For a given nonzero monomial $u = \prod x_{i,j}^{e_{i,j}}$ and a nonempty index set $S \subset \mathcal{I} \times \mathcal{J} = \{(1,1), \ldots, (m,n)\}$, define $S$-degree of $u$ as

$$\sum_{(i,j) \in S} e_{i,j}$$

and denote it by $\deg_S u$. Note that $\deg_S u \leq \deg u$. For simplicity, we also write $\deg_S u$ to denote the $\deg_{\mathcal{I} \times S} u$ for $S \subset \mathcal{J}$.
Lemma 4 ([7, Lemma 3]).

\[ LM(f_0) = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,1}^{p-1} \cdots x_{m,n}^{p-1} \]

Proof. First, we claim that the monomial

\[ u = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,1}^{p-1} \cdots x_{m,n}^{p-1} \]

appears in the expansion of \( f_0 \). Note that the coefficient of \( u \) in \( f_0 \) is

\[ \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n} \alpha_1^{p-1} \cdots \alpha_n^{p-1} \]

which is equal to \((-1)^m \neq 0\). Hence the claim is true.

Next, we will show that any monomial \( v \) for which \( v \not\succeq u \) holds does not appear in the expansion of \( f_0 \). If \( \deg_{(i) \times J} v \neq p - 1 \) for some \( 1 \leq i \leq m \) then \( v \) clearly does not appear in \( f_0 \) by (5). So, we can assume that \( \deg_{(i) \times J} v = p - 1 \) for all \( i \). Note that, as \( v \not\succeq u \) and \( \deg_{(i,1)}(v) = p - 1 \) for all \( 1 \leq i \leq m - n + 1 \), we have the same for \( v \), i.e., \( x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \) divides \( v \). Moreover, there exists \( j \geq 1 \) such that \( x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,1}^{p-1} \cdots x_{m,n}^{p-1} \mid v \) but \( x_{m-n+j,1}^{p-1} \cdots x_{m,n}^{p-1} \mid v \) for some \( k < j + 1 \). But then, \( \deg_{(j+1,1, \ldots, n)}(v) < (p - 1)(n - j) \) which implies that there exists \( j + 1 \leq \ell \leq n \) for which \( \deg_{(\ell)}(v) < (p - 1) \) holds. Hence, the coefficient of \( v \) in the expansion of \( f_0 \) cannot be nonzero, and the lemma follows. \( \square \)

Lemma 5. If \( \nu_1 \geq 3 \), then we have among all monomials greater than \( LM(f_0) \) which have the same degree with respect to each block of variables

\[ \max \{ \deg_{J_2} u \mid u \not\succeq LM(f), \deg u = \deg f_0, \deg_{\text{block}} u = \deg_{\text{block}} f_0 \} \]

\[ = (\nu_r - r)(p - 1) - 1 \]

where \( \deg_{\text{block}} \) stands for \( \deg_{(i) \times \{\nu_j, \nu_j+1, \nu_j+2, \ldots, \nu_{j+1}\}} \) for each \( 1 \leq i \leq n \) and \( 0 \leq j \leq s - 1 \).

Proof. Note that, as \( \deg_{(i) \times J_1} LM(f_0) = (m - n + r)(p - 1) \) and \( \deg_{\text{block}} u = \deg_{\text{block}} f_0 \), we should have \( \deg_{(i) \times J_1} u \geq (m - n + r)(p - 1) \) for any \( u \not\succeq f_0 \). Hence, \( \deg_{J_2} u \leq m(p - 1) - (m - n + r)(p - 1) - (s - r)(p - 1) \) with an equality only when there are no other variables except those \( x_{i,j} \) such that \( i \in I \) and \( j \in J_0 \cup J_1 \cup J_2 \). But this is not possible when \( \nu \geq 3 \).

Consider the monomial

\[ u = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,1}^{p-1} \cdots x_{m,n}^{p-1} \]

which we obtain from \( LM(f_0) \) first by multiplying with \( x_{m-n+2,1}^{p-1} \) (note that \( x_{m-n+2,2} \) divides \( LM(f_0) \)) and then pushing all variables which do not belong to class \( J_0 \cup J_1 \cup J_2 \) to variables of class \( J_2 \) contained in the same block.

Notice that \( \deg_{J_2} u = m(p - 1) - (m - n + r)(p - 1) - (s - r)(p - 1) - 1 = (n - s)(p - 1) - 1 = (\nu_r - r)(p - 1) - 1 \) that finishes the proof. \( \square \)
Remark 6. The case $\nu_1 = 2$ has been studied with a more sharp result in [7].

Proof of Theorem 2. Let

$$f_0 = \sum \alpha_{a_1, \ldots, a_\ell} h_1^{a_1} \cdots h_\ell^{a_\ell}; \quad \alpha \in \mathbb{F}, a_i \in \mathbb{N}_0, h_i \in \mathbb{F}[\oplus_m V]^P$$

be a decomposition of $f_0$ where $h_i$ are among the generators of the invariant ring $\mathbb{F}[\oplus_m V]^P$. Note that as $\text{LM}(f_0)$ appear with a nonzero coefficient on the left hand side of the equation, it should also appear on the right hand side. Hence, there exist an exponent sequence $a_1, \ldots, a_\ell$ such that $\alpha_{a_1, \ldots, a_\ell}$ is not zero and $\text{LM}(f_0)$ appears as a monomial in the expansion of $h_1^{a_1} \cdots h_\ell^{a_\ell}$.

Moreover, as $\text{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \geq \text{LM}(f_0)$ we can apply previous lemma to get a bound on $a_1 + \cdots + a_\ell$. By Lemma 5, $\deg_{J_2} \text{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \leq (\nu_r - r)(p - 1) - 1$.

Now our first observation gives the required bound: By Proposition 1, $\deg_{J_2} h_i \geq 1$ for all $1 \leq i \leq \ell$, and thus we should have $a_1 + \cdots + a_\ell \leq (\nu_r - r)(p - 1) - 1$.

We will combine this bound with the result of Proposition 1 of [7] to finish the proof. Note that we get the bound

\[ \beta(\mathbb{F}[\oplus_m V]^G) \geq \frac{(m - (s - r))(p - 1)}{(\nu_r - r)(p - 1) - 1} \text{ by splitting off } s - r \text{ variables} \]

\[ \geq \frac{(m - s + r)(p - 1)}{(\nu_r - r)(p - 1) - 1} = \frac{(m - s + r)(p - 1)}{(n - s)(p - 1) - 1} \quad \text{as } \nu_r - r = \nu_s - s = n - s \]

\[ > \frac{(m - s + r)(p - 1)}{(n - s)(p - 1)} \]

\[ = \frac{m - s + r}{n - s} \quad (9) \]

5. Comparing previous results

Note that the bound given above extends Richman’s bound as

\[ \beta(\mathbb{F}[\oplus_m V]^G) > \frac{m - s + r}{n - s} \]

\[ \geq \frac{m}{n - r} \quad \text{since } m > n \text{ and } s - r \geq 0. \]

For small $n$ where $n \leq p$, we may have only one nontrivial Jordan block and no trivial Jordan block, i.e., $r = s = 1$. Thus, the above bound gives

\[ \beta(\mathbb{F}[\oplus_m V]^G) > \frac{m}{n - r} = \frac{m}{n - 1}. \]

In general, we have more than 1 block and we obtain the following bound

\[ \beta(\mathbb{F}[\oplus_m V]^G) > \frac{m}{n - r} \geq \frac{m}{n - \frac{n}{p}} = \frac{m}{n(1 - \frac{1}{p})} = \frac{p}{p - 1} \frac{m}{n}. \]
Noether numbers via Jordan blocks

where we used the fact that when $s = r$ we have $r \geq n/p$. The last extreme case might be the case where $r = 1$ and $s = n - p + 1$. In that case, we get the bound

$$\beta(G) > \frac{m - s + r}{n - s} = \frac{m - n + p}{p - 1}.$$ 

Recall the previous result of Richman given in equation (1), we obtain here better and more dynamic results in general.

ACKNOWLEDGEMENTS

This note is a part of author’s Ph. D. thesis at Bilkent University and a continuation of his paper [7]. The author also thanks the anonymous referee for helpful comments.

REFERENCES


Received: February 1, 2013