MODULAR VECTOR INVARIANTS

A DISSERTATION SUBMITTED TO
THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By
Uğur Madran
August, 2006

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Prof. Dr. Alexander Klyachko(Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Assoc. Prof. Dr. Tuğrul Hakioğlu

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Assoc. Prof. Dr. A. Sinan Sertöz

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Asst. Prof. Dr. Müfit Sezer

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of doctor of philosophy.

Asst. Prof. Dr. Ergün Yalçın

Approved for the Institute of Engineering and Science:

Prof. Dr. Mehmet B. Baray
Director of the Institute

ABSTRACT

MODULAR VECTOR INVARIANTS

Uğur Madran
Ph.D. in Mathematics
Supervisor: Prof. Dr. Alexander Klyachko
August, 2006

Vector invariants of finite groups (see the introduction for definitions) provides, in general, counterexamples for many properties of the invariant theory when the characteristic of the ground field divides the group order. Noether number is such property.

In this thesis, we improve a lower bound for Noether number given by Richman in 1996: namely, we give a lower bound depending on the Jordan canonical form of an element of order equal to characteristic of the field. This method yields an effective bound by means of simple arithmetic arguments.

The results are valid for any faithful representation of the group, including reducible and irreducible ones. Also they are extended to any algebraic field extensions provided the characteristic of the field divides the group order.

Keywords: Modular invariants, polynomial invariants, vector invariants, Noether number, beta number.

ÖZET

MODÜLER VEKTÖR DEĞİŞMEZLERİ

Uğur Madran
Matematik, Doktora
Tez Yöneticisi: Prof. Dr. Alexander Klyachko
Ağustos, 2006

Sonlu grupların vektör değişmezleri, genellikle, değişmezlik teorisinin birçok özelliğinin kullanılan cismin karakteristiğinin grubun eleman sayısını böldüğü durumlarda geçerli olmadığını göstermek için kullanılır. Noether sayısı da bu özelliklerden biridir.

Bu tezde, 1996 yılında Richman tarafından Noether sayısı için verilen alt sınırı iyileştirdik: kısaca, uzunluğu kullanılan cismin karakteristiğine eşit olan bir elemanın Jordan standart formuna bağlı olarak alt sınır verdik. Bu metot, basit aritmetiksel argümanlarla etkili bir sınır getirmiştir.

Sonuçlar indirgenebilir ve indirgenemez durumları da kapsayarak grubun her tam gösterimi için geçerlidir. Aynı zamanda, sonuçlar, daha geniş alanlara da uygulanacak şekilde geliştirilmiştir.

Anahtar sözcükler: Modüler değişmezler, polinomal değişmezler, vektör değişmezleri, Noether sayısı, beta sayısı.

Acknowledgement

I would like to thank a number of people who helped and supported me. This work began under supervision of Prof. Serguei A. Stepanov, continued and expanded with excellent guidance and encouragements of Prof. Larry Smith and completed under the supervision of Prof. Alexander Klyachko.

I would like to thank Prof. Alexander Klyachko for his tolerance and readiness whenever I needed.

I must also express my gratitude to Prof. A. Sinan Sertöz for coordinating TÜBİTAK-BDP group in Bilkent and I thank to group members Prof. Alex Degtyarev, Prof. Alexander Klycahko, Prof. A. Sinan Sertöz, Prof. Sergui A. Stepanov for naming me a fellow and to Mrs. Ayşe Ataş from TÜBİTAK for her readiness whenever I needed help.

I am grateful to Prof. Larry Smith for accepting me to work together and for making my visit to Mathematisches Institut possible. I also thank him for the regular meetings where he introduced many interesting problems. I would like to thank Prof. Dagmar Meyer for her helps and for sharing her office during my studies in Göttingen.

I would like to thank Professors Klyachko, Hakioğlu, Sertöz, Sezer, and Yalçın for serving on my thesis committee.

I would like to express my special thanks to all my friends and colleague, particularly Fatma Altunbulak, Murat Altunbulak and İnan Utku Türkmen for invaluable discussions on daily news and politics.

Last but not least, I would like to thank my wife Sezin Madran, for her endless support and love.

`Peace at home, Peace in the world!`

Mustafa Kemal Atatürk

Contents

Chapter 1

Introduction

Invariant theory become popular again in last decades. Motivations vary but can be grouped as follows: geometric, computational, and algebraic. Topological and (co)homological aspects of the theory may be considered under algebraic invariant theory.

We refer the reader to [1], [9], [15], [29], [32], [43], [51] for an introduction to different branches of invariant theory and problems there. Also, surveys [22], [28], [42], [44], [49], and [52] invite anyone interested in the topic.

Invariant theory finds many applications in the modern language. The following topics are listed in [15, Chapter 5]: Cohomology of finite groups, Galois groups, generic polynomials, graph theory, combinatorics, coding theory, computer vision, and many others. The very recent book [27] also emphasizes the importance of invariant theory of finite groups over fields of prime characteristic.

The present thesis is devoted to finding a lower bound on Noether number, improving the one given by Richman in [36]. The main result of Chapter 3 where very special case of the problem is discussed, has been accepted [25] for publication.

1.1 Polynomial Invariants

Let G be a finite group acting faithfully via ρ on an $\mathbb{F}$ vector space V, i.e., if $\dim_{\mathbb{F}} V = n$ then by choosing a basis for V we may consider G as a subgroup of general linear group $\mathrm{GL}(n, \mathbb{F})$ by $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ (if the representation of G is not faithful, then we may replace G by its quotient H such that $H \sim \rho(G)$). By choosing a basis $\{x_1, x_2, \ldots, x_n\}$ for the dual space V^*, we may and will regard the ring of regular functions on V, $\mathbb{F}[V]$, as the ring $\mathbb{F}[x_1, \ldots, x_n]$. There is an induced action of G on $\mathbb{F}[V]$ which can be given explicitly by

$$(g \cdot f)(v) = f(g^{-1} \cdot v) \tag{1.1}$$

for any $g \in G, f \in \mathbb{F}[V]$, and $v \in V$. (Actually, the equation should be written as $(\rho(g) \cdot f)(v) = f(\rho(g^{-1}) \cdot v)$, but we identify G with its image $\rho(G)$ and abuse the notation for simplicity.)

The ring of invariants is defined as

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid g \cdot f = f \text{ for all } g \in G\} \tag{1.2}$$

and any polynomial $f \in \mathbb{F}[V]^G$ is called an *invariant polynomial*.

Due to a theorem of Noether [31], $\mathbb{F}[V]^G$ is finitely generated as an $\mathbb{F}$-algebra. Moreover, if the order of the group is not divisible by $\operatorname{char} \mathbb{F}$, then $\mathbb{F}[V]^G$ can be generated by invariant polynomials of degree at most $|G|$. This case, where $|G|$ is invertible in $\mathbb{F}$, is referred to as the *non-modular case*. However, there is no such upper bound depending only on the size of the group in the *modular case*, i.e., where $\operatorname{char} \mathbb{F} = p$ divides $|G|$.

The *Noether number* is defined as the maximal degree of a generator and denoted by $\beta(\rho(G))$ or simply by $\beta(G)$. (More formal notation should be $\beta(\mathbb{F}[V]^{\rho(G)})$ but for the simplicity of notations we prefer the preceding whenever the representation is clear from the context.) Note that, $\mathbb{F}[V]^G$ can be generated by invariant polynomials of degree at most $\beta(G)$, and in the non-modular case $\beta(G) \leq |G|$ which is known as *Noether bound*.

1.2 Vector Invariants

For a positive integer $m \in \mathbb{N}$, the group G acts diagonally via ρ on $\oplus_m V = V \oplus \cdots \oplus V$ as follows: $\rho(g) \cdot (v_1, \ldots, v_m) = (\rho(g) \cdot v_1, \ldots, \rho(g) \cdot v_m)$ for each $(v_1, \ldots, v_m) \in \oplus_m V$. Also, there is an induced action of G on $\mathbb{F}[\oplus_m V]$.

The polynomials $f \in \mathbb{F}[\oplus_m V]^G$ are called *vector invariants.* Note that, $\beta(\mathbb{F}[\oplus_m V]^G) \leq |G|$ in the non-modular case, no matter how large m is. However, this is not true when $|G| = 0$ in $\mathbb{F}$.

In the modular case, Richman proved in [36] that there is a constant $\alpha > 0$ depending only on $|G|$ and the characteristic $p > 0$ of the ground field such that

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq \alpha \cdot m \tag{1.3}$$

for any finite group and for sufficiently large m. In particular, he also showed that if $\dim V = n$ then

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq \max\{2, \frac{m}{n-1}, \frac{m}{|G|-1}, \frac{p}{p-1} \cdot \frac{m}{n}\}. \tag{1.4}$$

when $\mathbb{F} = \mathbb{F}_p$ is the prime field, with the refinement that

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq (m - n + 2)(p - 1) \tag{1.5}$$

when G contains a pseudoreflection of order p (a pseudoreflection is an invertible linear map g such that $\operatorname{rank}(g - I) = 1$).

For permutation groups, the given lower bounds are sharpened by Kemper and Stepanov independently to

$$\beta(G) \geq m(p - 1). \tag{1.6}$$

Campbell and Hughes describe a generating set for the vector invariants of 2-dimensional representation of the cyclic group of order p over $\mathbb{F}_p$ in [7], proving a conjecture of Richman.

1.2.1 Notations

In order to make this more transparent, we will use the following notations for the rest of this thesis. Let $V = \mathbb{F}^n$ and consider the m-fold direct sum, $\oplus_{i=1}^m V$. By choosing a basis $\{x_{i,1}, \ldots, x_{i,n}\}$ for V^*, the dual space of the i-th copy of V in $\oplus_m V$, for each $1 \leq i \leq m$, we may give the action of G on $\mathbb{F}[\oplus_m V] = \mathbb{F}[x_{i,j} \,|\, 1 \leq i \leq m,\ 1 \leq j \leq n]$ explicitly as

$$\begin{bmatrix} g \cdot x_{i,1} \\ g \cdot x_{i,2} \\ \vdots \\ g \cdot x_{i,n} \end{bmatrix} = \begin{bmatrix} \alpha_{1,1}(g) & \alpha_{1,2}(g) & \ldots & \alpha_{1,n}(g) \\ \alpha_{2,1}(g) & \alpha_{2,2}(g) & \ldots & \alpha_{2,n}(g) \\ \vdots & \vdots & & \vdots \\ \alpha_{n,1}(g) & \alpha_{n,2}(g) & \ldots & \alpha_{n,n}(g) \end{bmatrix} \begin{bmatrix} x_{i,1} \\ x_{i,2} \\ \vdots \\ x_{i,n} \end{bmatrix}$$

for all $1 \leq i \leq m$ and $g \in G$ where $\rho(g) = [\alpha_{i,j}(g)] \in \mathrm{GL}(n, \mathbb{F})$.

Also note that the action of G preserves the degrees of polynomials. Hence we may without loss of generality consider only homogeneous polynomials. So, any polynomial appearing in this thesis is homogeneous unless stated otherwise.

1.3 Statement of Results

Theorem 1.1 *Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation, where $\mathbb{F}$ is a field with p elements, p prime. If there exists $g \in G$ of order p such that $\rho(g)$'s Jordan blocks have sizes at most 2 and $\rho(g)$ has r nontrivial Jordan blocks, then*

$$\beta(\mathbb{F}[\oplus_m V]^G) \geq \frac{m - n + 2r}{r}(p-1) \tag{1.7}$$

where $V = \mathbb{F}^n$ and $m > n$.

Later we will be show that $\frac{m-n+2r}{r}(p-1) \geq 2(p-1)\frac{m}{n}$, so, we obtain a refinement of (1.4). This gives us the following corollary:

Corollary 1.2 *Let $\mathrm{SL}(n, \mathbb{F})$ denote the special linear group. Then*

$$\beta(F[\oplus_m V]^{\mathrm{SL}(n,\mathbb{F})}) \geq (m - n + 2)(p-1). \tag{1.8}$$

This result is given by Richman in [34] for arbitrary finite fields. Actually, $\mathrm{SL}(n,\mathbb{F})$ contains a pseudoreflection of order p (which will imply that $r = 1$) and hence gives the result. Same result also holds for $\mathrm{GL}(n,\mathbb{F}), UT(n,\mathbb{F}), O(n,\mathbb{F})$ using the same argument.

Theorem 1.3 *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,*

$$\beta(\mathbb{F}[\oplus_m V]^G) > \frac{m-s+r}{n-s} \tag{1.9}$$

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

Also here we have $\frac{m-s+r}{n-s} \geq \frac{p}{p-1}\frac{m}{n}$ and hence the theorem provides an immediate but slight improvement of (1.4). Although it does not seem to be a better result, it will serve us a step in the next result. Moreover, giving a bound in terms of numbers of Jordan blocks will help understanding the invariant ring in the modular case.

Theorem 1.4 *Let G be a group acting on an n-dimensional vector space V over a field $\mathbb{F}$ which is an algebraic extension of its prime field of characteristic $p > 0$. Suppose p divides the group order $|G|$. Then,*

$$\beta(\mathbb{F}[\oplus_m V]^G) > \frac{m''-s+r}{n-s} \geq \frac{p}{q-1}\frac{m'}{n} \tag{1.10}$$

for sufficiently large m, where q, m', m'', r, and s depends on the representation of G.

The precise definitions of q, m', m'', will be given before we prove this theorem. As in the previous theorem, here r and s denote again the number of Jordan blocks.

Note that we do not need any further assumptions on the group G or the representation ρ, e.g., we do not require any symmetry, or G to be cyclic, or any other property which may provide extra theoretical arguments. Moreover, it is

known that invariant ring in the modular case may fail to be Cohen-Macaulay which makes computations rather difficult.

The dissertation is organized as follows. In Chapter 2, we will introduce the tools needed. In Chapter 3 we will prove the first theorem. In Chapter 4 we will extend the methods and prove the second theorem. In Chapter 5, we extend the results further and consider not only prime fields but also their arbitrary (and possibly infinite) algebraic extensions. We provide some examples in the Appendix (Chapter 6) which illustrates failure of Noether bound in the modular case.

Chapter 2

Cyclic Subgroups and Jordan Blocks

2.1 Jordan Blocks

Choose and fix an element $g \in G$ of order p and let T be its image under given representation ρ. Without loss of generality, we may suppose that T is in its Jordan canonical form, i.e.,

$$\mathsf{T} = \begin{bmatrix} \mathsf{J}_1 & & & \\ & \mathsf{J}_2 & & \\ & & \ddots & \\ & & & \mathsf{J}_s \end{bmatrix}$$

where J_i's are elementary Jordan matrices of order $n_i \times n_i$

$$\mathsf{J}_i = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

such that $p \geq n_1 \geq n_2 \geq \cdots \geq n_r > n_{r+1} = \cdots = n_s = 1$. (If $n_1 > p$ then the order of T will be greater than p.)

2.1.1 Restrictions on Number of Jordan Blocks

It should be wise to mention the restrictions on r and s here and let us state the obvious ones first:

$$r \leq s \quad \& \quad r \geq 1. \tag{2.1}$$

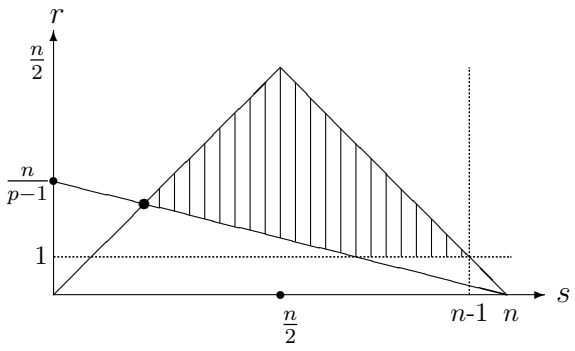
Note that since $n_i \geq 2$ for each $1 \leq i \leq r$ we have

$$2r + (s - r) \leq n \quad \Rightarrow \quad r + s \leq n. \tag{2.2}$$

Moreover, the condition $n_i \leq p$ imply that

$$pr + (s - r) \geq n \quad \Rightarrow \quad (p - 1)r + s \geq n. \tag{2.3}$$

We will use these restrictions when giving the bound independent of the decomposition, hence by taking the worse case. The possible values of r and s can be pictured as:



2.2 Cyclic Subgroup and an Auxiliary Invariant

Throughout this section, let $\mathbb{F}$ be the prime field with p elements and define H to be the subgroup of G generated by T (here we consider H as a subgroup of G by identifying G with $\rho(G)$). Hence $\langle \mathsf{T} \rangle = H \leq G \leq \mathrm{GL}(n, \mathbb{F})$. This inclusion implies that

$$\mathbb{F}[\oplus_m V]^{\mathrm{GL}(n,\mathbb{F})} \subset \mathbb{F}[\oplus_m V]^G \subset \mathbb{F}[\oplus_m V]^H.$$

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

$$f_0 = \sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}^n} (\alpha_1 x_{1,1} + \cdots + \alpha_n x_{1,n})^{p-1} \cdots (\alpha_1 x_{m,1} + \cdots + \alpha_n x_{m,n})^{p-1} \tag{2.4}$$

where the sum is over all possible n-tuples $(\alpha_1, \ldots, \alpha_n)$. The polynomial f_0 is invariant under the action of $\mathrm{GL}(n, \mathbb{F})$ by [36, p. 30] and hence

$$f_0 \in \mathbb{F}[\oplus_m V]^{\mathrm{GL}(n,\mathbb{F})} \subset \mathbb{F}[\oplus_m V]^G \subset \mathbb{F}[\oplus_m V]^H. \tag{2.5}$$

(Note here that, $\mathbb{F}$ should be a finite field in order to make the sum meaningful. Also, the restriction $m \geq n$ ensures here that $f_0 \neq 0$, which we will discuss later.)

Our aim is first to describe some properties of generators of $\mathbb{F}[\oplus_m V]^H$ and then to conclude about their degrees by writing f_0 in terms of these generators. The main result depends on the maximum number of (indecomposable) invariant factors that appear in any summand of a decomposition.

Proposition 2.1 *Let*

$$f_0 = \sum \alpha_{a_1,\ldots,a_\ell} h_1^{a_1} \cdots h_\ell^{a_\ell} \; ; \quad \alpha \in \mathbb{F}, a_i \in \mathbb{N}_0, h_i \in \mathbb{F}[\oplus_m V]^H \tag{2.6}$$

be a decomposition of f_0 where h_i are among the generators of the invariant ring $\mathbb{F}[\oplus_m V]^H$. Suppose that for any such decomposition, we have $a_1 + \cdots + a_\ell \leq N$ whenever $\alpha_{a_1,\ldots,a_\ell} \neq 0$. Then

$$\beta(H) \geq \frac{m(p-1)}{N} \tag{2.7}$$

and moreover,

$$\beta(G) \geq \frac{m(p-1)}{N}. \tag{2.8}$$

Proof. Since the invariant polynomials h_i are among the generators of $\mathbb{F}[\oplus_m V]^H$ we have $\deg h_i \leq \beta(H)$. Therefore, $m(p-1) = \deg f_0 \leq N \cdot \beta(H)$ which completes the first part of the proof.

For the second part, assume to the contrary that f_0 can be written as a polynomial in the elements of $\mathbb{F}[\oplus_m V]^G$ having degrees smaller than the above bound. Since $H \leq G$ we obtain a contradiction to the first part. □

Remark. This proposition is also an illustration of Theorem 1.1 and here we consider a more simple situation where the analysis of the invariants appearing in the decomposition (2.6) is missing.

2.3 Monomial Order

Definition. Let $\mathcal{I} = \{1, 2, \ldots, m\}$ and $\mathcal{J} = \{1, 2, \ldots, n\}$ be index sets. For a given nonzero monomial $u = \prod x_{i,j}^{e_{i,j}}$ and a nonempty index set $\mathcal{S} \subset \mathcal{I} \times \mathcal{J} = \{(1,1), \ldots, (m,n)\}$, define $\mathcal{S}$-degree of u as

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

and denote it by $\deg_{\mathcal{S}} u$. Note that $\deg_{\mathcal{S}} u \leq \deg u$. For simplicity, we also write $\deg_{\mathcal{S}} u$ to denote the $\deg_{\mathcal{I}\times\mathcal{S}} u$ for $\mathcal{S} \subset \mathcal{J}$.

For $1 \leq j \leq s$, set

$$\nu_j = \sum_{k\leq j} n_k$$

with the convention $\nu_0 = 0$. For the simplicity of the notations and calculations, we introduce the following index sets:

$$\begin{aligned}
\mathcal{J}_0 &= \{\nu_r + 1, \nu_r + 2, \ldots, n\} \\
\mathcal{J}_1 &= \{1, n_1 + 1 = \nu_1 + 1, \nu_2 + 1, \ldots, \nu_{r-1} + 1\} \\
\mathcal{J}_2 &= \{n_1 = \nu_1, \nu_2, \ldots, \nu_r\}
\end{aligned}$$

Note that the first set, $\mathcal{J}_0$, lists invariant variables which may split off, i.e.,

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

and, in particular, we have

$$f_0 = f_1 u_1 + f_2 u_2 + \cdots + f_\ell u_\ell \tag{2.9}$$

where $f_k \in \mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \notin \mathcal{J}_0]^H$ and $u_k = \prod_{i\in\mathcal{I}, j\in\mathcal{J}_0} x_{i,j}^{e_{i,j}}$ for all $1 \leq k \leq \ell$. Also, the index set $\mathcal{J}_2$ consists of the indices of invariant variables (which can not split off).

Lemma 2.2 *For each u_k appearing in the above decomposition (2.9), we have*

$$\deg u_k \geq (p-1)(s-r).$$

Proof. Let v be an arbitrary monomial appearing in f_0. Then, by expanding (2.4) we obtain the coefficient of v

$$\sum_{\alpha_1 \in \mathbb{F}} \sum_{\alpha_2 \in \mathbb{F}} \cdots \sum_{\alpha_n \in \mathbb{F}} \alpha_1^{\deg_{\{1\}} v} \alpha_2^{\deg_{\{2\}} v} \cdots \alpha_n^{\deg_{\{n\}} v}.$$

Since it is not zero, $\deg_{\{j\}} v$ is a nonzero multiple of $(p-1)$ for all j. In particular, $\deg_{\{j\}} v \geq p-1$ and hence, $\deg_{\mathcal{J}_0} v \geq (p-1)(s-r)$ (recall that $\mathcal{J}_0$ has $n-2r = s-r$ elements).

Suppose without loss of generality that all u_k appearing in (2.9) are distinct. For each u_k, there exists at least one monomial v_k appearing in the polynomial f_0 which is divisible by u_k, otherwise f_k is zero and u_k does not actually appear in that decomposition. Writing $v_k = w_k u_k$, where the monomial w_k appears in f_k, we note that $\deg_{\mathcal{J}_0} v_k = \deg_{\mathcal{J}_0} w_k + \deg_{\mathcal{J}_0} u_k$. Since $f_k \in \mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \notin \mathcal{J}_0]^H$, we get $\deg_{\mathcal{J}_0} w_k = 0$, and hence

$$\deg u_k \geq \deg_{\mathcal{J}_0} u_k = \deg_{\mathcal{J}_0} v_k \geq (p-1)(s-r),$$

establishing the result. □

Finally, we will introduce a monomial order. 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 $\mathrm{LM}(f)$. The term ordering defined above is compatible with the action of g in the sense that $\mathrm{LM}(f) \succeq \mathrm{LM}(g(f))$. We direct the reader to [12] for a detailed discussion of monomial orders.

Chapter 3

Jordan Blocks of Maximum Size 2

In this chapter, we will consider a special case where the Jordan blocks have sizes at most 2. We have two important reasons to consider this case.

First, the generators of the invariant ring is known under the action of such an element (not the generators of the invariant ring of the whole group). This knowledge enables us to give sharp bounds.

Second, we are able to pass from a result for cyclic groups to a result for an arbitrary group. This is quite important since only little is known in modular invariant theory, and the known results mainly consider either the cyclic group $\mathbb{Z}/p$ or permutation groups.

We also restrict the ground field to be prime field since explicit generators of the invariant ring is known only in this case. Since Jordan blocks have sizes at most 2, we have the following decomposition for T: Let r be the number of 2×2 blocks, and s be the number of all blocks, so $s - r$ is the number of trivial blocks.

Then, we can write

$$g = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{bmatrix}$$

where J_i's are elementary Jordan matrices of order 2×2 or 1×1

$$J_i = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad J_i = [1]\,.$$

We can further assume, by reordering if necessary, that

$$n_1 = n_2 = \cdots = n_r = 2 \text{ and } n_{r+1} = \cdots = n_s = 1$$

where J_i is an $n_i \times n_i$ matrix.

Lemma 3.1 *Let f_0 be the invariant given in equation (2.4). Then*

$$\mathrm{LM}(f_0) = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,j}^{p-1} \cdots x_{m,n}^{p-1}.$$

Proof. First, we claim that the monomial

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

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

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}^n} \underbrace{\alpha_1^{p-1} \cdots \alpha_1^{p-1}}_{m-n+1 \text{ times}} \alpha_2^{p-1} \cdots \alpha_n^{p-1}$$

which is equal to $(-1)^m \neq 0$ by well-known identity given in the proof of Lemma 3.3. Hence the claim is true.

Next, we will show that any monomial v for which $v \succ u$ holds does not appear in the expansion of f_0. If $\deg_{\{i\}\times\mathcal{J}} v \neq p-1$ for some $1 \leq i \leq m$ then v clearly does not appear in f_0 by (2.4). So, we can assume that $\deg_{\{i\}\times\mathcal{J}} v = p-1$ for all i. Note that, as $v \succ u$ and $\deg_{\{(i,1)\}} u = p-1$ 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 $x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,j}^{p-1} | v$ but $x_{m-n+j+1,j+1}^{p-1} \nmid v$ and $x_{m-n+j+1,k} | v$ for some $k < j+1$. But then, $\deg_{\{j+1,\ldots,n\}} v < (p-1)(n-j)$ which implies that there exists $j+1 \leq \ell \leq n$ for which $\deg_{\{\ell\}} v < (p-1)$ holds. Hence, by the same argument used in the first paragraph of the proof of Lemma 2.2, the coefficient of v in the expansion of f_0 cannot be nonzero, and the lemma follows. □

Remark. As we will use the following in the proof of the main result, we note them here for the convenience of the reader:

$$\begin{aligned}\deg_{\mathcal{J}_0} \mathrm{LM}(f_0) &= (s-r)(p-1),\\ \deg_{\mathcal{J}_1} \mathrm{LM}(f_0) &= (m-n+r)(p-1),\\ \deg_{\mathcal{J}_2} \mathrm{LM}(f_0) &= r(p-1).\end{aligned}$$

3.1 Main Result

To prove Theorem 1.1 we need the following result from [7].

Theorem 3.2 (Conjecture of Richman) *With the notations of the previous section, there are 4 classes of generators for the invariant ring $\mathbb{F}[\oplus_m V]^H$ namely,*

1. $x_{i,j'}$; $\quad i \in \mathcal{I}$ *and* $j' \in \mathcal{J}_0 \cup \mathcal{J}_2$
2. $\mathrm{N}(x_{i,j}) = \prod_{\alpha\in\mathbb{F}} g^\alpha(x_{i,j}) = x_{i,j}^p - x_{i,j}x_{i,j+1}^{p-1}$; $\quad i \in \mathcal{I}$ *and* $j \in \mathcal{J}_1$
3. $u_{(i,j)(k,l)} = x_{i,j}x_{k,l+1} - x_{i,j+1}x_{k,l}$; $\quad (i,j) <_{lex} (k,l)$, $i,k \in \mathcal{I}$, $j,l \in \mathcal{J}_1$
4. $\mathrm{Tr}(z) = \sum_{\alpha\in\mathbb{F}} g^\alpha(z)$ $\quad$ *such that* z *divides* $\prod_{i\in\mathcal{I},\, j\in\mathcal{J}_1} x_{i,j}^{p-1}$

where $(i,j) <_{lex} (k,l)$ *means either* $i<k$ *or* $i=k$ *and* $j<l$.

Proof. The action of g is given explicitly by

$$g(x_{i,j}) = \begin{cases} x_{i,j} + x_{i,j+1} & \text{if } j \in \mathcal{J}_1 = \{1,3,\ldots,2r-1\},\\ x_{i,j} & \text{if } j \in \mathcal{J}_2 = \{2,4,\ldots,2r\}\end{cases}$$

and as noted earlier, $\mathbb{F}[x_{i,j}]^H = \mathbb{F}[x_{i,j} \mid j \notin \mathcal{J}_0]^H \otimes \mathbb{F}[x_{i,j} \mid j \in \mathcal{J}_0]$. The result then follows from [7]. □

We need the following technical lemma:

Lemma 3.3 *Let* $z = \prod_{i\in\mathcal{I},j\in\mathcal{J}_1} x_{i,j}^{e_{i,j}}$ *such that* $e_{i,j} \le p-1$ *for all* i,j. *If* $\mathrm{Tr}(z) \neq 0$ *then* $\deg_{\mathcal{J}_2} u \ge p-1$ *for any monomial* u *appearing in* $\mathrm{Tr}(z)$.

Proof. When we expand the $\mathrm{Tr}(z)$, we get the following formula:

$$\mathrm{Tr}(z) = \sum_{\alpha\in\mathbb{F}} g^{\alpha}(z) = \sum_{\alpha\in\mathbb{F}} \prod_{i\in\mathcal{I},j\in\mathcal{J}_1} \Big(x_{i,j} + \alpha\ x_{i,j+1}\Big)^{e_{i,j}}.$$

Since

$$\sum_{\alpha\in\mathbb{F}} \alpha^d = \begin{cases} 0, & \text{if } p-1 \nmid d \\ -1, & \text{if } p-1 \mid d, \end{cases}$$

the $\mathcal{J}_2$-degree of a monomial is a nonzero multiple of $p-1$, and in particular, at least $p-1$. □

Remark. Theorem 1.1 can be proved using a weaker lemma, where we only require that $\deg_{\mathcal{J}_2} \mathrm{LM}(\mathrm{Tr}(z)) \geq p-1$. In this case, however, we need to redefine the monomial order in a more complicated way which makes it difficult to follow each step in the proof of main theorem.

Proof of Theorem 1.1. Let

$$f_0 = \sum \alpha_{a_1,\ldots,a_k} h_1^{a_1} h_2^{a_2} \cdots h_k^{a_k}, \tag{3.1}$$

where the $h_i \in \mathbb{F}[\oplus_m V]^H$ belong to one of the four classes described in Theorem 3.2. Comparing the degrees of both sides with respect to $\{x_{i,1},\ldots,x_{i,n}\}$, we conclude that none of the h_i's on the right hand side belongs to the class $\mathrm{N}(x_{i,j})$ as the degree of $\mathrm{N}(x_{i,j})$ is p in this set of variables, whereas the degree of f_0 in the same variables $\{x_{i,1},\ldots x_{i,n}\}$ is at most $p-1$.

Next, observe that there must exist h_i's belonging to the class $\mathrm{Tr}(z)$. Otherwise, $f_0 \in \mathbb{F}[x_{i,j'}, u_{(i,j)(k,l)}]$ and hence the $\mathcal{J}_1$-degree of $\mathrm{LM}(f_0)$ is at most the $\mathcal{J}_2$-degree of $\mathrm{LM}(f_0)$. This contradicts the fact that

$$\deg_{\mathcal{J}_1} \mathrm{LM}(f_0) = (m-n+r)(p-1) > \deg_{\mathcal{J}_2} \mathrm{LM}(f_0) = r(p-1)$$

as $m > n$.

There exists an exponent sequence $\mathbf{a} = (a_1,\ldots,a_k)$ with $\alpha_{\mathbf{a}} \neq 0$ such that the monomial $\mathrm{LM}(f_0)$ appears in the expansion of $h_1^{a_1}\cdots h_k^{a_k}$. Let $\tau_{\mathbf{a}}$ be the number of h_i's, counted with multiplicities, which belong to the class $u_{(i,j)(k,l)}$, i.e., those

belonging to the third class as stated in Theorem 3.2, and $\nu_{\mathbf{a}}$ be the number of those belonging to the first class. Hence, $a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}$ of them belong to the fourth class.

Note that for any monomial w appearing in the expansion of $h_1^{a_1} \cdots h_k^{a_k}$ we have $\deg_{\mathcal{J}_0 \cup \mathcal{J}_2} w \geq (a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})(p-1) + \tau_{\mathbf{a}} + \nu_{\mathbf{a}}$ by using Lemma 3.3. Since $\mathrm{LM}(f_0)$ appears also as a monomial in that expansion, we find

$$(a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})(p-1) + \tau_{\mathbf{a}} + \nu_{\mathbf{a}} \leq \deg_{\mathcal{J}_0 \cup \mathcal{J}_2} \mathrm{LM}(f_0) = s(p-1).$$

Hence, we can approximate the number of factors in the given summand,

$$a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}} \leq \frac{s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{p-1}.$$

Since among h_i's, there are $\tau_{\mathbf{a}}$ invariants of degree 2 and $\nu_{\mathbf{a}}$ invariants of degree 1, the product of the remaining h_i's has degree $m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}$. Thus, among those h_i's belonging to the class $\mathrm{Tr}(z)$, there exists a generator of degree at least

$$\frac{m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{(s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})/(p-1)} = (p-1)\frac{m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}}. \tag{3.2}$$

Since, $x_{i,j}$ does not appear in any other class except the first one, for $j \in \mathcal{J}_0$, we have $\nu_{\mathbf{a}} \geq \deg_{\mathcal{J}_0} u$ for any monomial u appearing in $h_1^{a_1} \cdots h_k^{a_k}$, and hence by Lemma 2.2,

$$\nu_{\mathbf{a}} \geq (p-1)(s-r). \tag{3.3}$$

In particular,

$$\frac{m(p-1) - \nu_{\mathbf{a}}}{s(p-1) - \nu_{\mathbf{a}}} > 2, \tag{3.4}$$

since $m > n = s + r$.

Now, we consider the fraction in (3.2) as a function of $\tau_{\mathbf{a}}$. By differentiating it (with respect to $\tau_{\mathbf{a}}$) and by inequality (3.4), we see that it is an increasing function of $\tau_{\mathbf{a}}$, and hence takes its minimum when $\tau_{\mathbf{a}} = 0$. Thus, from equation (3.2) we get the inequality

$$(p-1)\frac{m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}} \geq (p-1)\frac{m(p-1) - \nu_{\mathbf{a}}}{s(p-1) - \nu_{\mathbf{a}}}. \tag{3.5}$$

Similarly, by considering the last fraction as a function of $\nu_{\mathbf{a}}$, we see that it is also an increasing function and thus takes its minimum value when $\nu_{\mathbf{a}}$ is minimum. The minimum of $\nu_{\mathbf{a}}$ is $(p-1)(s-r)$ by (3.3). Thus we obtain

$$(p-1)\frac{m(p-1)-\nu_{\mathbf{a}}}{s(p-1)-\nu_{\mathbf{a}}} \geq (p-1)\frac{(p-1)(m-(s-r))}{(p-1)(s-(s-r))} = (p-1)\frac{m-s+r}{r}. \quad (3.6)$$

Finally, using the relation $n = r + s$, we get the bound

$$\beta(H) \geq (p-1)\frac{m-n+2r}{r}$$

and by the argument used in the proof of Proposition 2.1, we can conclude that the same bound holds for G, i.e.,

$$\beta(G) \geq (p-1)\frac{m-n+2r}{r} \geq 2(p-1)\frac{m}{n}$$

where the last inequality is due to $r \leq n/2$. □

3.2 Remarks and Sharpness

The result and the proof of Theorem 1.1 can be read in two different directions. First, the maximum of degrees of generators depends on the Jordan block decomposition. Even if the representation $\rho(G)$ is irreducible, it is possible to get a reducible representation $\rho(H)$, and actually, this is always the case when $n > p$. Thus, considering the Jordan decomposition of an element of order p is a reasonable step.

Second, we made use of the generators of 2-dimensional vector invariants. Hence, finding generators of higher dimensional vector invariants would sharpen lower bounds in the general setting. Unfortunately, the generators are not known except for the 2-dimensional and the p-dimensional vector invariants, and a few other special cases.

The bound given in Theorem 1.1 is sharp in the sense that it is attained, as Theorem 3.2 shows, for

$$r = 1 \Rightarrow \beta(G) = (p-1)(m-n+2).$$

Moreover, it extends the bound of Richman, given here by (1.4), since the maximum of the numbers on the right hand side of (1.4) is, in general, at most

$$\frac{p}{p-1}\frac{m}{n} \leq 2(p-1)\frac{m}{n}.$$

Chapter 4

Arbitrary Jordan blocks

In this chapter, we will consider a more general case but we still restrict the ground field to be prime.

Recall that f_0 is a universal invariant and H is a cyclic subgroup generated by T which is given in Jordan canonical form

$$\mathsf{T} = \begin{bmatrix} \mathsf{J}_1 & & & \\ & \mathsf{J}_2 & & \\ & & \ddots & \\ & & & \mathsf{J}_s \end{bmatrix}$$

where J_i's are elementary Jordan matrices of order $n_i \times n_i$

$$\mathsf{J}_i = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

such that $p \geq n_1 \geq n_2 \geq \cdots \geq n_r > n_{r+1} = \cdots = n_s = 1$.

4.1 Observation

Recall that $\mathcal{J}_0 = \{\nu_r+1, \nu_r+2, \ldots, n=\nu_s\}$, $\mathcal{J}_1 = \{1, \nu_1+1, \nu_2+1, \ldots, \nu_{r-1}+1\}$, $\mathcal{J}_2 = \{\nu_1, \nu_2, \ldots, \nu_r\}$ and $\nu_j = \sum_{k\leq j} n_k$. Note that $\mathcal{I} \times (\mathcal{J}_0 \cup \mathcal{J}_2)$ lists all invariant variables.

Proposition 4.1 *Let $f \in \mathbb{F}[x_{1,1}, \ldots, x_{m,n}]^H$. If the degree of f with respect to each vector $(x_{i,1}, \ldots, x_{i,n})$ is at most $p-1$, and $f \notin \mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \in \mathcal{J}_0 \cup \mathcal{J}_2]$ then there exists (i_0, j_0) such that x_{i_0,j_0} divides $\mathrm{LM}(f)$ 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 $\mathrm{LM}(f)$. Let x_{i_1,j_1} be the smallest variable dividing $\mathrm{LM}(f)$ with respect to monomial order given. Consider the monomial

$$w = \frac{\mathrm{LM}(f)}{x_{i_1,j_1}} \cdot x_{i_1,j_1+1}. \tag{4.1}$$

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

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

The proof does not depend on the ground field. We will use this result also in the next chapter.

4.2 On Auxiliary Invariant

Recall by Lemma 3.1 that $\mathrm{LM}(f_0) = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} \cdots x_{m-n+j,j}^{p-1} \cdots x_{m,n}^{p-1}$. We will make use of the following result in the next section.

Lemma 4.2 *If $\nu_1 \geq 3$, then we have among all monomials greater than $\mathrm{LM}(f_0)$ which have the same degree with respect to each block of variables*

$$\max\{\deg_{\mathcal{J}_2} u \mid u \succ \mathrm{LM}(f),\ \deg u = \deg f_0,\ \deg_{block} u = \deg_{block} f_0\} = (\nu_r - r)(p-1) - 1 \quad (4.2)$$

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

Proof. Note that, as $\deg_{\mathcal{I}\times\mathcal{J}_1} \mathrm{LM}(f_0) = (m-n+r)(p-1)$ and $\deg_{\mathrm{block}} u = \deg_{\mathrm{block}} f_0$, we should have $\deg_{\mathcal{I}\times\mathcal{J}_1} u \geq (m-n+r)(p-1)$ for any $u \succ f_0$. Hence, $\deg_{\mathcal{J}_2} u \leq m(p-1)-(m-n+r)(p-1)-(s-r)(p-1)$ with an equality only when there are no other variables except those $x_{i,j}$ such that $i \in \mathcal{I}$ and $j \in \mathcal{J}_0 \cup \mathcal{J}_1 \cup \mathcal{J}_2$. But this is not possible when $\nu \geq 3$.

Consider the monomial

$$u = x_{1,1}^{p-1} \cdots x_{m-n+1,1}^{p-1} x_{m-n+\nu_1+1,\nu_1+1}^{p-1} \cdots x_{m-n+\nu_{r-1}+1,\nu_{r-1}+1}^{p-1} x_{m-n+2,1} x_{m-n+2,\nu_1}^{p-2} x_{m-n+3,\nu_1}^{p-1} \cdots x_{m-n+j,\nu_k}^{p-1} \cdots x_{m,n}^{p-1} \quad (4.3)$$

which we obtain from $\mathrm{LM}(f_0)$ first by multiplying with $x_{m-n+2,1}x_{m-n+2,2}^{-1}$ (note that $x_{m-n+2,2}$ divides $\mathrm{LM}(f_0)$) and then pushing all variables which do not belong to class $\mathcal{J}_0 \cup \mathcal{J}_1 \cup \mathcal{J}_2$ to variables of class $\mathcal{J}_2$ contained in the same block.

Notice that $\deg_{\mathcal{J}_2} u = m(p-1) - (m-n+r)(p-1) - (s-r)(p-1) - 1 = (n-s)(p-1) - 1 = (\nu_r - r)(p-1) - 1$ that finishes the proof. □

We are now ready to prove the second result.

4.3 The Proof of Theorem 1.3

Let

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

be a decomposition of f_0 where h_i are among the generators of the invariant ring $\mathbb{F}[\oplus_m V]^H$. Note that as $\mathrm{LM}(f_0)$ 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 $\mathrm{LM}(f_0)$ appears as a monomial in the expansion of $h_1^{a_1} \cdots h_\ell^{a_\ell}$.

Moreover, as $\mathrm{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \succeq \mathrm{LM}(f_0)$ we can apply previous lemma to get a bound on $a_1 + \cdots + a_\ell$. By Lemma 4.2, $\deg_{\mathcal{J}_2} \mathrm{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \leq (\nu_r - r)(p-1) - 1$.

Now the observation gives the required bound: By Proposition 4.1, $\deg_{\mathcal{J}_2} h_i \geq 1$ 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 2.1 to finish the proof. Note that we get the bound

$$\begin{aligned}
\beta(G) &\geq \frac{(m-(s-r))(p-1)}{(\nu_r - r)(p-1) - 1} && \text{by splitting off } s-r \text{ variables} && (4.4)\\
&\geq \frac{(m-s+r)(p-1)}{(\nu_r - r)(p-1) - 1} \\
&= \frac{(m-s+r)(p-1)}{(n-s)(p-1) - 1} && \text{as } \nu_r - r = \nu_s - s = n - s \\
&> \frac{(m-s+r)(p-1)}{(n-s)(p-1)} \\
&= \frac{m-s+r}{n-s} && && (4.5)
\end{aligned}$$

□

Remark. Note that the bound given above extends Richman's bound as

$$\begin{aligned}
\beta(G) &> \frac{m-s+r}{n-s} \\
&\geq \frac{m}{n-r} && \text{since } m > n \text{ and } s - r \geq 0.
\end{aligned}$$

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

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

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

$$\beta(G) > \frac{m}{n-r} \geq \frac{m}{n - \frac{n}{p}} = \frac{m}{n(1-\frac{1}{p})} = \frac{p}{p-1}\frac{m}{n},$$

where we used the fact that when $s = r$ we have $r \geq n/p$. One 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 (1.4), we obtain here better and more dynamic results in general.

Chapter 5

Larger Fields

In this chapter, we will extend our last result to arbitrary fields. We will use the techniques of the previous chapter but first we need to modify some results.

5.1 Reduction to a Finite Field

It is important to get things on finite fields because of the construction of universal invariant f_0 which is the sum of polynomials where the sum runs over all vectors in $\mathbb{F}^n$, and for infinite fields, this sum is meaningless.

Before giving the reduction, let us mention another problem.

Example 5.1. Let $\mathbb{F}_p$ be the prime field with p elements and let t be a transcendental element. Define $\mathbb{F} = \mathbb{F}_p(t)$ a field over which we will define 2–dimensional representation.

Let $G = C_p \times C_p = \langle \mathsf{S} \rangle \times \langle \mathsf{T} \rangle$ the representation of the noncyclic group of order p^2, where

$$\mathsf{S} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \mathsf{T} = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

It is not possible to change the basis elements of $\mathbb{F}^2$ which may provide the

representation given above be written without a transcendental element.

Hence, we restrict ourselves to consider only representations defined over algebraic extensions of the prime fields.

Lemma 5.1 *Any modular algebraic representation of a finite group can be realized over a finite field.*

Proof. Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation where $\mathbb{F}$ is an algebraic extension of $\mathbb{F}_p$. Since the representation is algebraic, matrix entries $\alpha_{i,j}(g) \in \mathbb{F}$ are algebraic over $\mathbb{F}_p$ and hence by adding all these elements, $\alpha_{i,j}(g)$ for $i \in \mathcal{I}, j \in \mathcal{J}$, and $g \in G$, to prime field, we get a finite field $\mathbb{F}_q$ such that ρ can be defined. □

Definition. From now on, let q be a power of p where the representation over $\mathbb{F}^n$ can be realized over $\mathbb{F}_q^n$.

5.2 Modified Auxiliary

For $m \geq n \cdot \frac{q-1}{p-1}$ define the following auxiliary polynomial:

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

where $m \geq m' = \frac{q-1}{p-1}[\frac{m}{(q-1)/(p-1)}] \geq n\frac{q-1}{p-1}$ and $[\ell]$ denotes the greatest integer not exceeding ℓ.

We have:

Lemma 5.2

$$0 \neq f_0 \in \mathbb{F}[x_{i,j} |\ 1 \leq i, j \leq n]^{\mathrm{GL}(n,\mathbb{F}_q)}.$$

Proof. The invariance of f_0 is straightforward and to show that f_0 is nonzero, we evaluate the coefficient of a special monomial which is going to be the leading

coefficient of f_0 when we make use of the graded lexicographical order. For the moment, introduce the following projection for simplicity of calculations:

$$\pi(x_{i,j}) = \begin{cases} 1, & \text{if } (j-1)\frac{q-1}{p-1}+1 \le i \le j\frac{q-1}{p-1}, \\ 1, & \text{if } i \ge n\frac{q-1}{p-1} \quad \text{and } j = n, \\ 0, & \text{otherwise.} \end{cases}$$

When applied to f_0 we get

$$\begin{aligned} \pi(f_0) &= \sum_{\alpha_1,\ldots,\alpha_n \in \mathbb{F}_q} \underbrace{\alpha_1^{p-1}\cdots\alpha_1^{p-1}}_{(q-1)/(p-1)} \cdots \underbrace{\alpha_n^{p-1}\cdots\alpha_n^{p-1}}_{(q-1)/(p-1)} \alpha_n^{(p-1)(m'-n\frac{q-1}{p-1})} \\ &= \sum_{\alpha_1,\ldots,\alpha_n \in \mathbb{F}_q} \alpha_1^{q-1}\cdots\alpha_n^{q-1}\alpha_n^{m''(q-1)-n(q-1)} \\ &= (-1)^n \end{aligned}$$

where $m'' = [\frac{m}{(q-1)/(p-1)}] \ge n$ and the sums are over all possible n-tuples $(\alpha_1,\ldots,\alpha_n) \in \mathbb{F}_q^n$, and in the last line we used a well-known identity, extended version of the one used in the proof of Lemma 3.3. □

5.3 General Degree Bound

The observation given in Proposition 4.1 is also valid over $\mathbb{F}_q$. But we need to modify Lemma 4.2 as follows.

Lemma 5.3

$$\mathrm{LM}(f_0) = \underbrace{x_{1,1}^{p-1}\cdots x_{*,1}^{p-1}}_{(m''-n+1)\frac{q-1}{p-1}} \underbrace{x_{*,2}^{p-1}\cdots x_{*,2}^{p-1}}_{(q-1)/(p-1)} \cdots \underbrace{x_{*,n}^{p-1}\cdots x_{m',n}^{p-1}}_{(q-1)/(p-1)}$$

where the first indices (some marked as $*$) are in increasing order from $1,\ldots,m'$.

Proof. It follows from direct computations. □

Lemma 5.4 *If $\nu_1 \ge 3$, then we have among all monomials greater than $\mathrm{LM}(f_0)$ which have the same degree with respect to each block of variables*

$$\begin{aligned} \max\{\deg_{\mathcal{J}_2} u \mid u \succ \mathrm{LM}(f),\ \deg u = \deg f_0,\ \deg_{block} u = \deg_{block} f_0\} \\ = (\nu_r - r)(q-1) - 1 \quad (5.1) \end{aligned}$$

where $\deg_{block}$ *stands for* $\deg_{\{i\}\times\{\nu_j+1,\nu_j+2,\ldots,\nu_{j+1}\}}$ *for each* $1 \le i \le n$ *and* $0 \le j \le s-1$.

Proof. Note that, as $\deg_{\mathcal{I}\times\mathcal{J}_1} \mathrm{LM}(f_0) = (m'-n+r)(q-1)$ and $\deg_{\mathrm{block}} u = \deg_{\mathrm{block}} f_0$, we should have $\deg_{\mathcal{I}\times\mathcal{J}_1} u \ge (m'-n+r)(q-1)$ for any $u \succ f_0$. Hence, $\deg_{\mathcal{J}_2} u \le m'(q-1)-(m'-n+r)(q-1)-(s-r)(q-1)$ with an equality only when there are no other variables except those $x_{i,j}$ such that $i \in \mathcal{I}$ and $j \in \mathcal{J}_0 \cup \mathcal{J}_1 \cup \mathcal{J}_2$. But this is not possible when $\nu \ge 3$.

Consider the monomial

$$u = \left(\prod_{i=1}^{(m''-n+1)\frac{q-1}{p-1}} x_{i,1}^{p-1}\right)\left(\prod_{i=(m''-n+1)\frac{q-1}{p-1}+1}^{(m''-n+r)\frac{q-1}{p-1}} x_{i,\nu_k+1}^{p-1}\right) x_{(m''-n+r)\frac{q-1}{p-1}+1,1} x^{p-2}_{(m''-n+r)\frac{q-1}{p-1}+1,\nu_1}\left(\prod_{(m''-n+r)\frac{q-1}{p-1}+2}^{m'} x_{i,\nu_{k_i}}^{p-1}\right) \quad (5.2)$$

which we get from $\mathrm{LM}(f_0)$ by multiplying with $x_{(m''-n+r)\frac{q-1}{p-1}+1,1} x^{-1}_{(m''-n+r)\frac{q-1}{p-1}+1,2}$ (note that $x_{(m''-n+r)\frac{q-1}{p-1}+1,2}$ divides $\mathrm{LM}(f_0)$) and then pushing all variables which do not belong to class $\mathcal{J}_0 \cup \mathcal{J}_1 \cup \mathcal{J}_2$ to variables of class $\mathcal{J}_2$ contained in the same block.

Notice that $\deg_{\mathcal{J}_2} u = m'(q-1)-(m'-n+r)(q-1)-(s-r)(q-1)-1 = (n-s)(q-1)-1 = (\nu_r-r)(q-1)-1$. This finishes the proof. □

Proof of Theorem 1.4. We will repeat the proof of Theorem 1.3 on page 21 with adapting new notations.

Let

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

be a decomposition of f_0 where h_i are among the generators of the invariant ring $\mathbb{F}[\oplus_m V]^H$. Note that as $\mathrm{LM}(f_0)$ 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 $\mathrm{LM}(f_0)$ appears as a monomial in the expansion of $h_1^{a_1} \cdots h_\ell^{a_\ell}$.

Moreover, as $\mathrm{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \succeq \mathrm{LM}(f_0)$ we can apply previous lemma to get a bound on $a_1 + \cdots + a_\ell$. By Lemma 5.4, $\deg_{\mathcal{J}_2} \mathrm{LM}(h_1^{a_1} \cdots h_\ell^{a_\ell}) \leq (\nu_r - r)(q-1) - 1$.

Now the observation gives the required bound: By Proposition 4.1, $\deg_{\mathcal{J}_2} h_i \geq 1$ for all $1 \leq i \leq \ell$, and thus we should have $a_1 + \cdots + a_\ell \leq (\nu_r - r)(q-1) - 1$.

Recall that $\deg f_0 = m''(q-1)$. We will combine the above bound with the result of Proposition 2.1 to conclude. Hence we get the bound

$$\begin{aligned}
\beta(G) &\geq \frac{(m'' - (s-r))(q-1)}{(\nu_r - r)(q-1) - 1} && \text{by splitting off } s-r \text{ variables} && (5.3)\\
&= \frac{(m'' - s + r)(q-1)}{(n-s)(q-1) - 1} && \text{as } \nu_r - r = \nu_s - s = n - s \\
&> \frac{(m'' - s + r)(q-1)}{(n-s)(q-1)} \\
&= \frac{m'' - s + r}{n-s}, && && (5.4)
\end{aligned}$$

establishing the result. □

Remark. Recall that $m'' = [\frac{m}{(q-1)/(p-1)}]$ and $m' = m''\frac{q-1}{p-1}$ and hence bound given above can be written as

$$\begin{aligned}
\beta(G) &> \frac{m'' - s + r}{n-s} \\
&\geq \frac{m''}{n-r} = \frac{p-1}{q-1}\frac{m'}{n-r} \\
&\geq \frac{p-1}{q-1}\frac{p}{p-1}\frac{m'}{n} && \text{since } s = r \text{ implies } r \geq n/p \\
&= \frac{p}{q-1}\frac{m'}{n} && && (5.5)
\end{aligned}$$

establishing the last part of the statement. In this result, we keep the notation m' in these results because of simplicity. If we further estimate m' with the worse

case $m' > m - \frac{q-1}{p-1}$, we get

$$\begin{aligned} \beta(G) &> \frac{p}{q-1}\frac{m'}{n} \\ &> \frac{p}{q-1}\frac{m-(q-1)/(p-1)}{n} \\ &\geq \frac{p}{q-1}\frac{m}{n} - \frac{p}{p-1}\frac{1}{n}. \end{aligned} \tag{5.6}$$

Note that the last summand is always less than 1, which gives the most general result

$$\beta(G) > \frac{p}{q-1}\frac{m}{n} - 1.$$

Chapter 6

Appendix: Examples

We will give explicit examples to illustrate that Noether bound does not hold in the modular case.

6.1 Some Examples

Example 6.1. Let us consider 3–fold 2–dimensional representation of C_2 over $\mathbb{Q}$ and $\mathbb{F}_2$. The nonidentity element of C_2 acts on the variables $x_1, x_2, x_3, y_1, y_2, y_3$ by interchanging x_i and y_i's simultaneously.

The invariants are well known: $l_i := x_i + y_i$, $q_i := x_i y_i$ and the ones obtained from polarizations of q_i,'s namely $u_{i,j} := x_i y_j + y_i x_j$. These invariants suffice to generate all invariants on 0 characteristic, i.e., $\mathbb{Q}[x_1, \ldots, y_3]^{C_2} = \mathbb{Q}[l_1, l_2, l_3, q_1, q_2, q_3, u_{1,2}, u_{1,3}, u_{2,3}]$ and hence the invariant $f := x_1x_2x_3 + y_1y_2y_3$ can be written as a polynomial in terms of these generators. Explicitly, the expression can be given as

$$f = l_1 l_2 l_3 - \frac{1}{2}(u_{1,2}l_3 + u_{1,3}l_2 + u_{2,3}l_1)$$

Note that this last expression is not valid in $\mathbb{F}_2$ because of the quotient. Actually $f \notin \mathbb{F}_2[l_1, l_2, l_3, q_1, q_2, q_3, u_{1,2}, u_{1,3}, u_{2,3}]$. The degree of f is 3 and it is an indecomposable invariant, which shows that Noether bound fails in modular case.

When we check the Jordan form of the nonidentity element, we can express it over prime characteristic in two different ways, depending on the characteristic. If the characteristic is different than 2, it is

$$\mathsf{J} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

and if characteristic is 2, it is

$$\mathsf{J} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

There is one more thing special about the above example: the given representation is a permutation representation. Even Noether bound fails, there are still many connections between modular and nonmodular invariants, e.g., their Hilbert series are equal. In the next example, we will illustrate a completely different type of example.

Example 6.2. We will consider C_3 on $3V_2$ over $\mathbb{F}_3$ and list all invariants up to degree 6 and show by means of simple arguments that $\beta(C_3) \geq 6$. Let T be a generator which is given in Jordan form, i.e.,

$$\mathsf{T} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

and the action is $\mathsf{T}(x_i) = x_i + y_i$, and $\mathsf{T}(y_i) = y_i$ for $1 \leq i \leq 3$.

There are 3 obvious invariants of degree 1, and none else: y_1, y_2, y_3.

In degree 2, there are 9 invariants, 3 are new, 6 are coming from those of first degree: $u_{i,j} := x_i y_j - x_j y_i$ for $1 \leq i < j \leq 3$ are three new ones.

In degree 3, we have again 3 new invariants: $N_i := x_i^3 - x_i y_i^2$ for each $i = 1, 2, 3$. Also, here comes an interesting relation which breaks Cohen-Macaulayness of the invariant ring: $(x_1y_2 - y_1x_2)y_3 - (x_1y_3 - y_1x_3)y_2 = (x_3y_2 - y_3x_2)y_1$.

In degree 4, there is not any new (indecomposable) invariant.

In degree 5, we have again 3 new invariants:
$p_1 := x_1^2x_2y_2y_3 - x_1^2y_2^2x_3 + x_1y_1y_2^2y_3 - x_1y_1x_2y_2x_3 + x_1y_1x_2^2y_3 - y_1^2x_2^2x_3 + y_1^2x_2y_2y_3 - y_1^2y_2^2x_3$ and similiarly p_2, p_3. Note that it is rather easy to show that p_i are indecomposable. $\mathrm{LM}(p_1) = x_1^2x_2y_2y_3$ and the ratio of 1st and 2nd components is higher than the previous ones, except the N_i's but they cannot appear in a decomposition of p_1 as their degree with respect to vectors are all 3, whereas p_1 has degree at most 2. We choose to consider the ratio of degrees of vector components because T respects it.

Finally, in degree 6, we have only one new invariant, namely: $x_1^2x_2^2y_3^2 + x_1^2x_2y_2x_3y_3 + x_1^2y_2^2y_3^2 + x_1y_1x_2y_2y_3^2 + y_1^2x_2^2y_3^2 + x_1y_1y_2^2x_3y_3 + y_1^2x_2y_2x_3y_3 + x_1y_1x_2^2x_3y_3 + y_1^2y_2^2x_3^2 + x_1^2y_2^2x_3^2 + x_1y_1x_2y_2x_3^2 + y_1^2x_2^2x_3^2 + y_1^2y_2^2y_3^2$. The indecomposability of this new invariant can be shown similarly as the indecomposability of the ones of degree 5 above.

It is guaranteed by Theorem 3.2 that these 13 invariants generate the whole invariant ring.

Bibliography

[1] D. J. Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series, vol. 190, Cambridge University Press, Cambridge, 1993. MR1249931

[2] H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank, and D. L. Wehlau, *Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants*, Canad. Math. Bull. **42** (1999), no. 2, 155–161. MR1692004

[3] H. E. A. Campbell, J. C. Harris, and D. L. Wehlau, *On rings of invariants of non-modular abelian groups*, Bull. Austral. Math. Soc. **60** (1999), no. 3, 509–520. MR1727484

[4] H. E. A. Campbell, I. Hughes, and R. D. Pollack, *Vector invariants of symmetric groups*, Canad. Math. Bull. **33** (1990), no. 4, 391–397. MR1091341

[5] ———, *Rings of invariants and p-Sylow subgroups*, Canad. Math. Bull. **34** (1991), no. 1, 42–47. MR1108927

[6] H. E. A. Campbell and I. P. Hughes, 2*-dimensional vector invariants of parabolic subgroups of* $\mathrm{Gl}_2(\mathbf{F}_p)$ *over the field* $\mathbf{F}_p$, J. Pure Appl. Algebra **112** (1996), no. 1, 1–12. MR1402392

[7] ———, *Vector invariants of* $U_2(\mathbf{F}_p)$*: a proof of a conjecture of Richman*, Adv. Math. **126** (1997), no. 1, 1–20. MR1440251

[8] ———, *Rings of invariants of certain p-groups over the field* $\mathbf{F}_p$, J. Algebra **211** (1999), no. 2, 549–561. MR1666658

[9] H. E. A. Campbell and D. L. Wehlau (eds.), *Invariant theory in all characteristics*, CRM Proceedings & Lecture Notes, vol. 35, Providence, RI, American Mathematical Society, 2004. MR2066574

[10] H.E.A. Campbell, B. Fodden, and David L. Wehlau, *Invariants of the diagonal C_p-action on V_3*, J. Algebra **302** (2006), no. 2, 501–513.

[11] Jianjun Chuai, *A new degree bound for invariant rings*, Proc. Amer. Math. Soc. **133** (2005), no. 5, 1325–1333 (electronic). MR2111938

[12] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1189133

[13] Harm Derksen, *Polynomial bounds for rings of invariants*, Proc. Amer. Math. Soc. **129** (2001), no. 4, 955–963 (electronic). MR1814136

[14] ———, *Degree bounds for syzygies of invariants*, Adv. Math. **185** (2004), no. 2, 207–214. MR2060467

[15] Harm Derksen and Gregor Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002. MR1918599

[16] P. Fleischmann, M. Sezer, R.J. Shank, and C.F. Woodcock, *The Noether numbers for cyclic groups of prime order*, UKC/IMS/05/10, arXiv:math.AC/0508075.

[17] Peter Fleischmann, *A new degree bound for vector invariants of symmetric groups*, Trans. Amer. Math. Soc. **350** (1998), no. 4, 1703–1712. MR1451600

[18] ———, *The Noether bound in invariant theory of finite groups*, Adv. Math. **156** (2000), no. 1, 23–32. MR1800251

[19] ———, *On invariant theory of finite groups*, in Campbell and Wehlau [9], pp. 43–69.

[20] John Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7 (electronic). MR1826990

[21] Frank D. Grosshans, *Vector invariants in arbitrary characteristic*, arXiv:math.AC/0605690.

[22] Frank D. Grosshans, *The work of Gian-Carlo Rota on invariant theory*, Algebra Universalis **49** (2003), no. 3, 213–258, Dedicated to the memory of Gian-Carlo Rota. MR2021386

[23] G. Kemper, *Lower degree bounds for modular invariants and a question of I. Hughes*, Transform. Groups **3** (1998), no. 2, 135–144. MR1628445

[24] Joseph P. S. Kung and Gian-Carlo Rota, *The invariant theory of binary forms*, Bull. Amer. Math. Soc. (N.S.) **10** (1984), no. 1, 27–85. MR0722856

[25] Uğur Madran, *Lower degree bounds for modular vector invariants*, Proc. Amer. Math. Soc. (to appear).

[26] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Codes and invariant theory*, Math. Nachr. **274/275** (2004), 104–116. MR2092326

[27] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Self-dual codes and invariant theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR2209183

[28] Mara D. Neusel, *Degree bounds. an invitation to postmodern invariant theory*, Topology and its Applications (to appear).

[29] Mara D. Neusel and Larry Smith, *Invariant theory of finite groups*, Mathematical Surveys and Monographs, vol. 94, American Mathematical Society, Providence, RI, 2002. MR1869812

[30] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1915), no. 1, 89–92 (German). MR1511848

[31] ———, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p.*, Nachrichten Göttingen (1926), 28–35 (German).

[32] V. L. Popov, *Groups, generators, syzygies, and orbits in invariant theory*, Translations of Mathematical Monographs, vol. 100, American Mathematical Society, Providence, RI, 1992. MR1171012

[33] David R. Richman, *The fundamental theorems of vector invariants*, Adv. in Math. **73** (1989), no. 1, 43–78. MR0979587

[34] ———, *On vector invariants over finite fields*, Adv. Math. **81** (1990), no. 1, 30–65. MR1051222

[35] ———, *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1996), no. 1, 49–76. MR1423198

[36] ———, *Invariants of finite groups over fields of characteristic p*, Adv. Math. **124** (1996), no. 1, 25–48. MR1423197

[37] Gian-Carlo Rota, *Combinatorics, representation theory and invariant theory: the story of a ménage à trois*, Discrete Math. **193** (1998), no. 1-3, 5–16. MR1661358

[38] Barbara J. Schmid, *Finite groups and invariant theory*, Topics in invariant theory (Paris, 1989/1990), Lecture Notes in Math., vol. 1478, Springer, Berlin, 1991, pp. 35–66. MR1180987

[39] R. James Shank and David L. Wehlau, *The transfer in modular invariant theory*, J. Pure Appl. Algebra **142** (1999), no. 1, 63–77. MR1716047

[40] ———, *Computing modular invariants of p-groups*, J. Symbolic Comput. **34** (2002), no. 5, 307–327. MR1937464

[41] ———, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002), no. 4, 438–450. MR1897423

[42] N. J. A. Sloane, *Error-correcting codes and invariant theory: new applications of a nineteenth-century technique*, Amer. Math. Monthly **84** (1977), no. 2, 82–107. MR0424398

[43] Larry Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995. MR1328644

[44] ———, *Polynomial invariants of finite groups. A survey of recent developments*, Bull. Amer. Math. Soc. (N.S.) **34** (1997), no. 3, 211–250. MR1433171

[45] ———, *Homological codimension of modular rings of invariants and the Koszul complex*, J. Math. Kyoto Univ. **38** (1998), no. 4, 727–747. MR1670003

[46] ———, *Putting the squeeze on the Noether gap—the case of the alternating groups A_n*, Math. Ann. **315** (1999), no. 3, 503–510. MR1725992

[47] ———, *On alternating invariants and Hilbert ideals*, J. Algebra **280** (2004), no. 2, 488–499. MR2089248

[48] ———, *Invariant theory and the Koszul complex: Representations of F/p in characteristic p applications*, J. Math. Kyoto Univ. (to appear).

[49] Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), no. 3, 475–511. MR0526968

[50] S. A. Stepanov, *Vector invariants of symmetric groups in the case of a field of prime characteristic*, Diskret. Mat. **12** (2000), no. 4, 25–38. MR1826176

[51] Bernd Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993. MR1255980

[52] David L. Wehlau, *The Noether number in invariant theory*, Compte Rendus Math. Rep. Acad. Sci. (to appear).

[53] Hermann Weyl, *The Classical Groups. Their Invariants and Representations. reprint of the second edition (1946) of the 1939 original.*, Princeton University Press, Princeton, N.J., 1997.

VITA

Uğur Madran was born in Bozdoğan, Aydın, Turkey, on January 15, 1974, the son of Bekir and Mahmure Madran. In 1999, he married to Sezin (Soylu) Madran of Pınarbaşı, Kayseri, Turkey.

After receiving his B.S. degree in 1998 from the Department of Mathematics, in Bilkent University, he continued his academic studies with S. A. Stepanov in the same department. In 1999, he was named Orhan Alisbah Fellow. He wrote the thesis *On lower degree bounds for vector invariants over finite fields* in September 2000 and got M.S. degree.

During his Ph.D. studies he visited Mathematisches Institut der Universität, Göttingen, Germany as TÜBİTAK-BDP fellow and continued his studies under the supervision of Larry Smith between September 2003 and August 2004.

He completed the requirements for the doctor of philosophy degree at Bilkent University. His research interests include algebraic and computational invariant theory, coding theory and cryptography.

He is currently a member of TMD, AMS, and SIAM.