ON LOWER DEGREE BOUNDS FOR VECTOR INVARIANTS OVER FINITE FIELDS

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS

AND THE INSTITUTE OF ENGINEERING AND SCIENCES

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

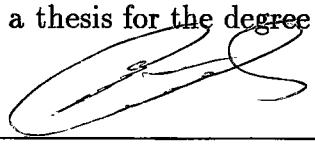
MASTER OF SCIENCE

By

Uğur Madran

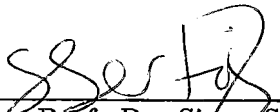
September, 2000

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



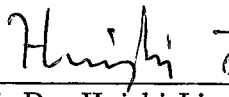
Prof. Dr. S.A. Stepanov(Principal Advisor)

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



Assoc. Prof. Dr. 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 thesis for the degree of Master of Science.



Asst. Prof. Dr. Huishi Li

Approved for the Institute of Engineering and Sciences:

Prof. Dr. Mehmet Baray
Director of Institute of Engineering and Sciences

ABSTRACT

ON LOWER DEGREE BOUNDS FOR VECTOR INVARIANTS OVER FINITE FIELDS

Uğur Madran
M. S. in Mathematics
Advisor: Prof. Dr. S.A. Stepanov
September, 2000

The purpose of this thesis is to obtain a lower degree bound in modular invariant theory for a special case. More precisely, let G be any group and k be a finite field of positive characteristic p such that p divides $|G|$. We prove that if an invariant which has degree at most $p-1$ with respect to each variable can be written as a polynomial in orbit sums of monomials, then the invariant ring $k[V^m]^G$ of m copies of the vector space V over k with $\dim V = n$ requires a generator of degree $\frac{m-t}{n-t} \cdot \frac{p-1}{n_1-1} \geq \frac{m}{n}$ provided that $m \geq n$ where t and n_1 depends on the representation of G such that $\lceil \frac{n}{p} \rceil \leq t \leq n+1$ and $2 \leq n_1 \leq p$.

Keywords and Phrases: Modular invariant theory, finite field, finite group.

ÖZET

SONLU CİSİMLER ÜZERİNDEKİ VEKTÖR DEĞİŞMEZLERİNİN DERECELERİNİN ALT SINIRLARI ÜZERİNE

Uğur Madran
Matematik Bölümü Yüksek Lisans
Danışman: Prof. Dr. S.A. Stepanov
Eylül, 2000

Bu tezin amacı özel bir durum için modüler değişmezlik teorisinde dereceler üzerine bir alt sınır bulmaktır. Karakteristiği p olan k sonlu cismi ve eleman sayısı p ile bölünen G grubu için aşağıdaki sonuç elde edilmiştir: Eğer her değişkene göre derecesi en fazla $p-1$ olan değişmez polinomların, yörünge toplamlarının polinomları şeklinde ifade edilebileceklerini varsayarsak, o zaman değişmezlik halkasını $k[V^m]^G$ oluşturan polinomların içinde derecesi en az $\frac{m-t}{n-t} \cdot \frac{p-1}{n_1-1} \geq \frac{m}{n}$ olan bir polinom vardır. Burada V, boyutu n olan k üzerine bir vektör uzayını; V^m, V'nin m kopyasını ifade etmektedir ve $m \geq n$ olmalıdır. Ayrıca t ile n_1 aşağıdaki eşitsizlikleri sağlayan ve G grubunun ifade edilişine bağlı tam sayılardır; $\lceil \frac{n}{p} \rceil \leq t \leq n+1$ ve $2 \leq n_1 \leq p$.

Anahtar Kelimeler ve İfadeler: Modüler değişmezlik teorisi, sonlu cisim, sonlu grup.

To my wife
Sezin

ACKNOWLEDGMENTS

I would like to thank my advisor Serguei A. Stepanov for sharing his ideas with me during my graduate studies and for his readiness to help at all times.

I am grateful to Bilsel Alisbah for establishing the **Orhan Alisbah Fellowship**. I also thank to committee members for naming me the recipient of the award. It was very difficult to continue studying mathematics without the award in the first days of my marriage.

I want to thank A. Klyachko for organizing algebra seminars which highly motivated me during my research. I thank to everyone joining our group seminars. Without listeners, it is very hard to do mathematics.

My special thanks goes to my family, in particular to my sister Hülya who visited and listened me during my hard days, and to my wife Sezin whose encouragement have motivated me most of the times.

This will never be completed without emphasizing the worth of friendship. I would like to thank to all my friends, especially to Emrah for sharing a lot with us.

In short, I thank everyone in Bilkent University whom I met.

Table of Contents

Chapter 1

Introduction

The fundamental problem in invariant theory is to describe all functions which are invariant under the action of a group. When the underlying field has a relatively prime characteristic to the order of the group, the situation is much simpler. But in the case of modular invariants, i.e. when the characteristic of the field divides the order of the group, almost nothing is known. My aim in this thesis is to give a lower bound on the degrees of generators of the invariant algebra.

Chapter 2 contains a short introduction to the problem in 0 characteristic and explains what is *Invariant Theory*. This chapter also describes the notation and the literature of the subject.

In chapter 3, I try to illustrate the difference of invariant theory in zero-characteristic and in positive characteristic. I mainly focus on the *Reynolds Operator*, which is the most powerful tool in zero-characteristic, and try to give such an operator for similar computations in positive characteristic. *Orbit Chern Classes* are introduced as a tool instead of Reynolds Operator and I hope that the use of this approach will yield a better understanding of modular invariant theory.

Chapter 4 is mainly on the cyclic groups of prime order. The importance of cyclic groups is that they may lead us to important bounds by means of elementary proofs instead of using highly detailed algebraic structures. The proofs may easily be understood by an undergraduate student who have been taken basic algebra courses. But the cost of elementary proof is too much for the theory, since the generalization is not so simple.

Chapter 5 illustrates the ideas explained in the previous chapter. The importance of this chapter is that it explains how some ideas work and the reasons why some do not.

I want to end this introduction with the following quotation from [9]:

> Like the Arabian phoenix rising out of its ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics. During its long eclipse, the language of modern algebra was developed, a sharp tool now at last being applied to the very purpose for which it was invented.

Chapter 2

Preliminaries

In this chapter, several of the basic ideas and problems of the subject are given. The easiest way to understand the invariant theory is to study the symmetric polynomials which should provide a key to begin the theory. From now on the underlying field is of characteristic 0, unless stated differently. For further details see [16] and [21], the later one being more elementary.

2.1 Symmetric Polynomials

Let k be a field and $k[x_1, \cdots, x_n]$ be a polynomial algebra in n variables over the field k. We call a polynomial $f \in k[x_1, \cdots, x_n]$ **symmetric** if $f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = f(x_1, \cdots, x_n)$ for all $\sigma \in \Sigma_n$, where Σ_n denotes the symmetric group on n letters. The fundamental problem of the invariant theory is to classify all invariant polynomials, i.e. all the symmetric polynomials in our case. Note that the polynomials;

$$\begin{aligned} \sigma_1 &= x_1 + \cdots + x_n, \\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots x_{n-1}x_n, \\ &\vdots \\ \sigma_n &= x_1x_2 \cdots x_n, \end{aligned}$$

are all symmetric and called as *elementary symmetric polynomials.* In general they are defined as the coefficients of the polynomial in the new variable T;

$$\prod_{i=1}^{n}(1 + x_iT) = 1 + \sum_{i=1}^{n} \sigma_i T^i \tag{2.1}$$

These are fundamental since:

Theorem 2.1.1 *Every symmetric polynomial* $f(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ *can be written as a polynomial in the elementary symmetric polynomials.*

PROOF. The proof to be presented here follows the one in [16]. Lets define *lexicographic order* on monomials which is induced from the partial order $\prec$ in such a way that

$$x_1^{s_1} \cdots x_n^{s_n} \prec x_1^{t_1} \cdots x_n^{t_n}$$

if and only if the first nonzero difference $t_i - s_i$ is positive, e.g.

$$x_2 \prec x_1 \prec x_1 x_2 \prec x_1 x_2^2 \prec \cdots \prec x_1^2 \prec x_1^2 x_2.$$

Now proceed by induction on lexicographic order defined above. Let $f(x_1, \cdots, x_n)$ be symmetric. Since the action of the symmetric group on $k[x_1, \cdots, x_n]$ carries homogeneous polynomials into homogeneous polynomials of the same degree, without loss of generality, assume that f is homogeneous. Let $x_1^{t_1} \cdots x_n^{t_n}$ be the largest monomial appearing with a non-zero coefficient C in f. Note that $t_i \leq t_{i-1}$ for all i, since otherwise there should be a smallest i such that $t_i > t_{i-1}$. Then the transposition $\pi = (i-1, i)$ which interchanges $i-1$ and i belongs to S_n and since f is invariant, i.e. symmetric, $x_1^{t_1} \cdots x_{i-1}^{t_i} x_i^{t_{i-1}} \cdots x_n^{t_n}$ also appears in f with the same coefficient. But this is larger in the lexicographic order which contradicts our assumption that there exists an index i such that $t_i > t_{i-1}$. Now we will construct a symmetric polynomial with the same maximal monomial. To do this, first note that the polynomial $\sigma_1^{t_1 - t_2} \sigma_2^{t_2 - t_3} \cdots \sigma_{n-1}^{t_{n-1} - t_n} \sigma_n^{t_n}$ also contains the monomial $x_1^{t_1} \cdots x_n^{t_n}$ as maximal monomial in the lexicographic order. So $f - C\sigma_1^{t_1 - t_2} \sigma_2^{t_2 - t_3} \cdots \sigma_{n-1}^{t_{n-1} - t_n} \sigma_n^{t_n}$ is an invariant polynomial whose maximal monomial is less in lexicographic order than the maximal monomial of f. By induction hypothesis the theorem is proved. ∎

First of all note that the set of all invariants is an algebra. Lets fix the notation: If V is an n dimensional vector space over the field k and the dual space V^* has a basis $x_1, \ldots, x_n$ and the group $G \subset GL(n, k)$ acts on V then the polynomial algebra is denoted by $k[V] = k[x_1, \cdots, x_n]$, and the invariant algebra is denoted by $k[V]^G$ where we are interested in the invariants of the group $G \subset GL(n, k)$ acting on finite dimensional vector space V of dimension n. Now it is time to show the situation more deeply in zero-characteristic.

2.2 Noether's Bound

In zero-characteristic one of the powerful and important idea is to define an averaging function, the most famous is *Reynolds Operator "#"* which is defined as

$$\# : k[V] \to k[V]^G, \qquad f \mapsto f^{\#} := \frac{1}{|G|}\sum_{\sigma\in G}\sigma(f) \tag{2.2}$$

The Reynolds Operator has the following properties:

$$\begin{aligned} f^{\#} = f &\iff f \in k[V]^G \\ f^{\#\#} &= f^{\#} \\ (\sigma(f))^{\#} &= f^{\#} \qquad \forall\sigma \in G \end{aligned}$$

Hence $\#$ is a G-invariant projection of $k[V]$ on $k[V]^G$.

Theorem 2.2.1 (Noether) *The algebra of invariants $k[V]^G$ can be generated by invariants of degree $\leq |G|$.*

PROOF. This proof is from [8]. First, introduce the polarization identity

$$x_1 \cdots x_m = \frac{(-1)^m}{m!}\sum_{I\subseteq\{1,\ldots,m\}}(-1)^{|I|}\left(\sum_{i\in I}x_i\right)^m$$

So any homogeneous polynomial $f(x_1,\ldots,x_n)$ of degree m is of the form $f(\mathbf{x}) = \sum_1^N a_i L_i(\mathbf{x})^m$ where $L_i(\mathbf{x})$ denotes linear forms in $\mathbf{x} = (x_1,\ldots,x_n)$. Hence any G-invariant polynomial;

$$f(\mathbf{x}) = f^{\#}(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(f(\mathbf{x})) = \sum a_i \frac{1}{|G|}\sum_{\sigma\in G}\sigma(L_i(\mathbf{x}))^m$$

is a linear combination of $\sum_{\sigma\in G}\sigma(L_i(\mathbf{x}))^m$ which is in fact symmetric function in $\sigma(L_i(\mathbf{x}))$. It is known by Theorem 2.1.1 that any symmetric function is a polynomial of elementary symmetric functions in $\sigma(L_i(\mathbf{x}))$ which have degree $\leq |G|$ which proves the theorem. (Different proofs of the theorem can be found in any book on invariant theory. For example see [14],[16], and [21]) ∎

Even there is a bound in the degree of generators, it is hard to find the generator set. There are $\binom{n+|G|}{n}$ many invariant functions satisfying the condition. Hence the minimum number of generators is n whereas maximum is $\binom{n+|G|}{n}$.

The Noether's bound given above is optimal. However, for many special groups the bound is much smaller. To this end, it is worth saying that in modular case there is no bound on the degree of generators. In the next chapter, modular case is investigated in detail. But is remarkable to note that polarization identity given in the proof of Noether's bound cannot be used in modular case. The second remark is that, Reynolds operator also does not work as a projection in the modular case although it does in zero-characteristic.

The following simple examples illustrate these facts in short:

Example 2.2.2 Consider the representation of the *Klein four-group* $G \subset GL(2,k)$ which is given by:

$$G = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}.$$

Note that any polynomial $f(x,y) \in k[x,y]$ is invariant under G if and only if

$$f(x,y) = f(-x,y) = f(x,-y)$$

since G is generated by the matrices;

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If $f = \Sigma_{i,j} a_{i,j} x^i y^j$, then $f \in k[x,y]^G$ iff $a_{ij} = 0$ for i,j odd. Hence it follows that

$$k[x,y]^G = k[x^2, y^2].$$

The importance of the last result is that $k[V]^G$ is in fact a polynomial algebra. Most of the groups do not admit such a property as the next example shows:

Example 2.2.3 This time consider the representation of the cyclic group of order 4 given by:

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Its invariants $f(x,y) \in k[x,y]^G$ have the following property; $f(x,y) = f(-y,x)$. Hence by means of simple computations and with the help of Noether's bound one can easily find the fundamental invariants;

$$f_1(x,y) = x^2 + y^2, \quad f_2(x,y) = x^2 y^2, \quad f_3(x,y) = x^3 y - x y^3.$$

But three polynomials are found in two variables. Hence they should be algebraically dependent and careful computations gives this relation: $f_3^2 = f_1^2 f_2 - 4f_2^2$. This simply means that $k[x,y]^G$ is not a unique factorization domain. If the invariant algebra is denoted by $k[f_1, f_2, f_3]$ then the homomorphism of algebras

$$\omega \ : \ k[f_1, f_2, f_3] \to k[x, y]$$

defined by

$$\omega(f_1) = x^2 + y^2, \quad \omega(f_2) = x^2 y^2, \quad \omega(f_3) = x^3 y - x y^3$$

is a surjection onto the algebra of invariants with kernel $(f_3^2 - f_1^2 f_2 + 4f_2^2)$. Therefore

$$k[x,y]^G \cong k[f_1, f_2, f_3]/(f_3^2 - f_1^2 f_2 + 4f_2^2)$$

as an algebra over k.

Moreover, $k[x,y]^G$ is a free module over the subalgebra $k[f_1, f_2]$ with generators $1, f_3$ and so there is a unique expression for every invariant polynomial of the form $f = g' + g'' \cdot f_3$, where $g', g'' \in k[f_1, f_2]$.

Remark 2.2.4 *Up to this point, it is assumed that $G \subset GL(n,k)$. In fact for any group G, there is a representation $\rho : G \to GL(n,k)$ which enables us to think G as being a subgroup of the general linear group. Thus the Noether's bound is independent of the representation of the group. It is solely given in terms of the group's properties, namely its size.*

Remark 2.2.5 *In the previous two examples the action of the matrix elements on the variables is defined explicitly as;*

$$\begin{bmatrix} \sigma(x_1) \\ \sigma(x_2) \\ \vdots \\ \sigma(x_n) \end{bmatrix} = \sigma \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sigma_{11}x_1 + \cdots + \sigma_{1n}x_n \\ \sigma_{21}x_1 + \cdots + \sigma_{2n}x_n \\ \vdots \\ \sigma_{n1}x_1 + \cdots + \sigma_{nn}x_n \end{bmatrix},$$

where $\sigma = [\sigma_{i,j}]_{n \times n} \in G$ is arbitrary.

2.3 The β-Number

It is time to define the beta number, β. For any group G let $\rho : G \to GL(n,k)$ be its representation; i.e. G acts on the n-dimensional vector space V over the

field k. Then it is defined as $\beta(G) = \max\{\beta(G,V) \mid G : V \text{ is a representation}\}$ where $\beta(G,V)$ denotes the smallest positive integer ℓ such that the homogeneous invariants of degree $\leq \ell$ generate the invariant algebra $k[V]^G$. For example, as explained in the previous section in zero-characteristic $\beta(G) \leq |G|$ for any G. For an algebraically closed field, k, of characteristic zero one has $\beta(G) = |G|$ for any cyclic group G. The following table illustrates the β-number for non-cyclic abelian groups of small order (For details see [14]):

$\lvert G\rvert$	4	8	9	12	16	18	20	24	25	27	28
$\beta(G)$	3	5	5	7	9	8	11	13	9	11	15

Although the Noether's bound is attained, as seen from the table, in general the β-number depends on the structure of the group and is much smaller than expected. However, in positive characteristic there is no bound in general. In particular, for the simplest group $\mathbb{Z}_2$ the β-number is infinity. The reason is that in positive characteristic, the β-number depends on the representation of the group, unlike zero-characteristic.

Chapter 3

Modular Case

This chapter briefly explains the situation in positive characteristic with some references to recent developments. The vector invariants are introduced, and an alternative way to Reynolds operator is discussed. From here to the end, there are no assumptions about the characteristic of the field. Mostly, positive characteristic will be used. First, the classification is given:

3.1 Classification of Invariants

In the survey, [17], L. Smith divide the invariant theory into the following cases:

(i) **The nonmodular case:** $|G| \in k^\times$ In the case when $|G|! \in k^\times$; i.e. $|G|$ is strictly less than the characteristic of k, it is known that $\beta(G) \leq |G|$ (See [13] for details). Recently, P. Fleischmann showed in [6] that when $|G|$ is coprime to the characteristic, then we have again $\beta(G) \leq |G|$.

(ii) **The modular case:** $|G| \equiv 0$ in k. In this case there are no bounds, i.e. $\beta_k(G) = \infty$. In this thesis, we are interested in how beta number depends on representation and how quickly tends to infinity. The known result that can be applied to this case is the one in [1], namely $\beta(G, V) \leq \max\{|G|, \text{rank}(V)\binom{|G|}{2}\}$ which works in arbitrary ring k.

3.2 Vector Invariants

In zero characteristic the representation of a group is a direct sum of irreducible ones and for any irreducible representation $G : V$ one has $\dim(V) \leq |G|$. For that reason, it is somehow cumbersome to deal with vector spaces of larger dimension. But this is not the case in modular invariant theory. However modular invariant theory has its own property since in that case $GL(n,k)$ is finite. The invariants of the general linear group is deeply investigated by Dickson and is called now the *Dickson algebra* (See for example [16, pp. 236-242] for details).

It should be remarkable to study the modular representation theory, but as explained above, the β-number depends fully on the representation in modular case. Hence a reasonable question at this point is how the representation should be in general to study with. One of the methods is to define the vector invariants which is investigated by Weyl in [22]. The usual way is to consider $k[V^m]^G$ instead of $k[V]^G$ where $V^m = \oplus_{i=1}^m V$ is a direct sum of m copies of V. From now on let $A_{mn} := k[V^m]$ where $\dim(V) = n$ and $A_{mn}^G = k[V^m]^G$ for simplicity. The vector invariants are studied in [1], [3], [5], [7], [10], [11], [20], [22].

The action of the group in this case is similar to Remark 2.2.5 and given explicitly as:

$$\begin{bmatrix} \sigma(x_{i1}) \\ \sigma(x_{i2}) \\ \vdots \\ \sigma(x_{in}) \end{bmatrix} = \sigma \begin{bmatrix} x_{i1} \\ x_{i2} \\ \vdots \\ x_{in} \end{bmatrix} = \begin{bmatrix} \sigma_{11}x_{i1} + \cdots + \sigma_{1n}x_{in} \\ \sigma_{21}x_{i1} + \cdots + \sigma_{2n}x_{in} \\ \vdots \\ \sigma_{n1}x_{i1} + \cdots + \sigma_{nn}x_{in} \end{bmatrix},$$

where $\sigma = [\sigma_{i,j}]_{n\times n} \in G$ is arbitrary and $A_{mn} = k[V^m]$ is identified by introducing the variables x_{ij} such that; $A_{mn} = k[x_{11}, \ldots, x_{1n}; \cdots ; x_{m1}, \ldots, x_{mn}]$.

To begin the theory, it is usual to begin with simplest cases. Since any group can be embedded in symmetric group Σ, it is natural to think $G = \Sigma_n$. Another simplest case is to consider cyclic group of prime order. The symmetric groups are widely investigated in [1], [5], [7], [16], [17], [20]. In this thesis the cyclic groups are investigated. The most important reason to study with cyclic group is to find a general result. The generalization follows from the following properties:

Let $G \subset GL(n,k)$ such that char $k = p$ and p divides $|G|$. Then there exist an element $\gamma \in G$ of order p, and define $H :=< \gamma >$, the subgroup generated by γ. Then $A_{mn}^{GL(n,k)} \subset A_{mn}^{G} \subset A_{mn}^{H}$.

There are many techniques to work and some of them are introduced in [2], [4], [15], [18]. The one that I should use here is the *orbit Chern classes* or more precisely the orbit polynomials. The next section contains some properties of orbit Chern classes.

3.3 Orbit Chern Classes

First of all, let's see why Reynolds operator does not work in modular case. In the proof of 2.2.1 the polarization identity requires that every integer should be invertible in k, since one can get an invariant of arbitrary degree (excluding some small ones in some cases). Instead of this polarization identity, other techniques are introduced in modular case. But even the new techniques work, the second and the most important difficulty arises: The Reynolds operator, which is a projection, cannot be applied directly since the order of the group, $|G|$ is no more invertible in modular case. New and simpler proofs of Noether's bound are given with new techniques and one of them is the orbit Chern classes.

For V being a finite-dimensional representation of a finite group G and an orbit $B \subset V^*$ let

$$\varphi_B(X) = \prod_{b \in B} (X + b) \tag{3.1}$$

which belongs to $k[V][X]$ with a new variable X. The polynomial $\varphi_B(X)$ is called the *orbit polynomial* of B. Since the decomposition of any G-set into orbits is an equivalence relation, it is easily seen that in fact $\varphi_B(X) \in k[V]^G[X]$. I.e. the coefficients of the orbit polynomial belongs to our invariant algebra.

When the product in 3.1 is expanded, one gets;

$$\varphi_B(X) = \sum_{i+j=|B|} c_i(B) X^j.$$

The new coefficients $c_i(B) \in k[V]^G$ are called the *orbit Chern classes.* The first orbit Chern class $c_1(B)$ is nothing but the sum of the orbit elements, whereas the last one $c_{|B|}(B)$ which is called *top Chern class* is the product of the orbit elements. Note that the first one is additive and the last one is multiplicative.

In this thesis I just need the first one but for the completeness of the subject some of the properties of all Chern classes are included here. If B_1, B_2 are two disjoint orbits then

$$\varphi_{B_1}(X) \cdot \varphi_{B_2}(X) = \varphi_{B_1 \cup B_2}(X) \quad \text{and} \quad c_t(B_1 \cup B_2) = \sum_{i+j=t} c_i(B_1) \cdot c_j(B_2)$$

We close the discussion of orbit Chern classes with the following theorem due to L. Smith and R.E. Strong.

Theorem 3.3.1 *Let $\rho : G \hookrightarrow GL(n,k)$ be a representation of a finite group G over a field k. Suppose either the field k is of characteristic zero or that the order of G is less than the characteristic of k. Then $k[V]^G$ is generated by orbit Chern classes. If b is the size of the largest orbit of G acting on V^*, then $k[V]^G$ is generated by homogeneous polynomials of degree at most b.*

PROOF. See for example [16, Theorem 3.1.10]. ∎

The importance of this result is that, any orbit has an order which is less than or equal to the size of the group, i.e. with the notations of the theorem, $b \leq |G|$.

Secondly, another useful property of orbit Chern classes is that, the generalized Chern classes of an orbit $B \in S^d(V^*)$ provides in a trivial way to express all invariant polynomials where S^d stands for the symmetric algebra. For a further discussion of orbit Chern classes see [16, pp. 41-52].

For simplicity we redefine the first orbit Chern class because the concept of orbit Chern classes is not necessary for the rest of this thesis. The purpose of introducing this subject is to give an alternative way in the theory of invariants.

For a polynomial $f \in A_{mn}$ we set

$$S_G(f) = \sum_{g \in Orb_G(f)} g \qquad \text{where} \qquad Orb_G(f) = \{\sigma(f) |\, \sigma \in G\}\,. \tag{3.2}$$

If the orbit of f is denoted as $[f]$ then the definition above is nothing but the first orbit Chern class, i.e. $S_G(f) = c_1([f])$.

Chapter 4

Cyclic Groups

Throughout this chapter, let k denotes the finite field with p elements $\mathbb{F}_p$, V be a finite dimensional vector space over $\mathbb{F}_p$ with $\dim V = n$ which we identify by $V = \mathbb{F}_p x_1 + \cdots + \mathbb{F}_p x_n$. By V^m we mean a direct sum of m copies of V, i.e. $V^m = \oplus_{i=1}^m V$. We suppose for the rest of this thesis that $m \geq n$. Let $G \subset GL(n, \mathbb{F}_p)$ be a finite group acting on V hence also acting on the commutative polynomial algebra $k[V^m]$, where p divides $|G|$.

4.1 Introduction

Let $\gamma \in G$ be an element of order p. In this section, we will mainly focus on the subgroup generated by γ, and the algebra of its invariants, $A_{mn}^{<\gamma>}$. Note that $A_{mn}^{GL(n,\mathbb{F}_p)} \subset A_{mn}^{G} \subset A_{mn}^{<\gamma>}$, which enables us to give some lower bounds on the degrees of generators by solely investigating the properties of cyclic group H of order p and its algebra of invariants, where H stands for the subgroup generated by γ.

The reason of investigating cyclic group is that, as mentioned earlier, this is one of the easiest ways to give general results since every group has a cyclic subgroup of order p in the modular case. The cost of finding a general result is too much since it does not allow any assumption.

$$J_\rho = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

are $n_\rho \times n_\rho$ matrices with $n_\rho \leq p$ for all $\rho = 1, 2, \ldots, t$. By renumbering the basis elements, if necessary, we can without loss of generality assume that

$$n_1 \geq n_2 \geq \cdots \geq n_t \geq 1 \tag{4.1}$$

4.2 A Universal Invariant

In this section we will define a global invariant and explain our approach. In 1990, Richman proved in [11, Prop. 14] that if G contains a pseudo-reflection of order p then $\beta(G, V^m) \geq ([m/d] - n + 2)(p-1)$ provided that $m \geq (n+1)d$ where $d = (|k| - 1)/(p-1)$ and more generally he proved in [12, Prop. 9] for any group G in modular case, $\beta(G, V^m) \geq m(p-1)/(p^{|G|-1} - 1)$. Further, he proved in the same paper that the invariants over the integers, i.e. when $k = \mathbb{Z}$, the lower degree bound is $\beta(G, V^m) \geq \max\{n, m(n-1)\}$.

Later, Stepanov ([20]) and Kemper ([7]) proved independently using different arguments that if G is a permutation group then $\beta(G, V^m) \geq m(p-1)$ which improves the Richman's bound in the case of symmetric group. There are also upper bounds for the degree of generators of the invariant algebra. Campbell *et al.*[1] proved that for arbitrary commutative ring k, $\beta(\Sigma_n, V^m) \leq \max\{n, mn(n-1)/2\}$ and Fleischmann improved this bound to $\beta(\Sigma_n, V^m) \leq \max\{n, m(n-1)\}$ in [5]. However no upper bound is known in general case at the time of writing this thesis.

Stepanov's and Kemper's results suggest that it is worth to investigate the bound $m(p-1)$ in the general case, i.e. without assuming that G is a permutation group. The easiest way to do is to define an indecomposable invariant of degree $m(p-1)$. By the word *indecomposable*, we mean that it cannot be written as a polynomial in vector invariants of less degree. For this reason we introduce the invariant polynomial f_0;

$$f_0 = \sum_{\alpha_1,\cdots,\alpha_n \in \mathbb{F}_p} (\alpha_1 x_{11} + \cdots + \alpha_n x_{1n})^{p-1} \cdots (\alpha_1 x_{m1} + \cdots + \alpha_n x_{mn})^{p-1} \quad (4.2)$$

The virtue of defining f_0 in that manner is that for any $\sigma \in GL(n, \mathbb{F}_p)$ we have $\sigma(f_0) = f_0$, therefore $f_0 \in A_{mn}^G$ as well for any subgroup G, and in particular it also belongs to invariant algebra of our cyclic group H.

Proposition 4.2.1 *If σ is an arbitrary element of the group $GL(n,k)$ then $\sigma(f_0) = f_0$.*

PROOF. This proof follows the one in [19]. Since

$$\sigma((\alpha_1 x_{11} + \cdots + \alpha_n x_{1n})^{p-1} \cdots (\alpha_1 x_{m1} + \cdots + \alpha_n x_{mn})^{p-1})$$

$$= (\alpha_1 \sigma(x_{11}) + \cdots + \alpha_n \sigma(x_{1n}))^{p-1} \cdots (\alpha_1 \sigma(x_{m1}) + \cdots + \alpha_n \sigma(x_{mn}))^{p-1}$$

and the action of σ permutes the elements of $V_i = \mathbb{F}_p x_{i1} + \cdots \mathbb{F}_p x_{in}$, $1 \leq i \leq m$, in the same way, we deduce that

$$\sigma(f_0) = \sum_{\alpha_1,\ldots,\alpha_n \in \mathbb{F}_p} (\alpha_1 \sigma(x_{11}) + \cdots + \alpha_n \sigma(x_{1n}))^{p-1} \cdots (\alpha_1 \sigma(x_{m1}) + \cdots + \alpha_n \sigma(x_{mn}))^{p-1}$$

$$= \sum_{\alpha'_1,\ldots,\alpha'_n \in \mathbb{F}_p} (\alpha'_1 x_{11} + \cdots + \alpha'_n x_{1n}^{p-1} \cdots (\alpha'_1 x_{m1} + \cdots + \alpha'_n x_{mn})^{p-1} = f_0.$$

This proves the proposition. ∎

It should be necessary to check that if $f_0 \not\equiv 0$ in $\mathbb{F}_p$ but as we will see later in 4.3.1 that this is not the case. The definition of f_0 may seen to be obvious to one who studies enough the modular invariant theory.

4.3 The Projection π

The next question is how one can show that f_0 is indecomposable. As usual, the idea is assuming the converse to get a contradiction. As we promised in chapter 1, to get an elementary proof, we evaluate the polynomial f_0 and the generator set with lots of zeros to kill all but one monomial. Studying with a monomial is of course the easiest way to deal with polynomials. Most of the papers included in the references use this idea under different names. The most popular technique in that papers is introducing the *leading monomial* of a polynomial.

We define the projection π as follows (in fact it is an evaluation map and hence an $\mathbb{F}_p$-algebra homomorphism);

$$\pi(x_{ij}) = \begin{cases} x_{ii} & \text{if } i = j \text{ and } i \leq n, \\ x_{i1} & \text{if } i > n \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

Let $\pi(f)$ be the image of the polynomial f under the transformation π, i.e.

$$\pi(f(x_{11}, \ldots, x_{1n}; \cdots; x_{m1}, \ldots, x_{mn}))$$

$$= f(\pi(x_{11}), \ldots, \pi(x_{1n}); \cdots; \pi(x_{m1}), \ldots, \pi(x_{mn}))$$

The next proposition gives an exact form of the polynomial $\pi(f_0)$ when it is expressed as linear combinations of monomials. Also, it can serve as a proof of $f_0 \not\equiv 0$ in $\mathbb{F}_p$.

Proposition 4.3.1 *If $m \geq n$ then the polynomial $\pi(f_0)$ is of the form:*

$$\pi(f_0) = (-1)^n x_{11}^{p-1} x_{22}^{p-1} \cdots x_{nn}^{p-1} x_{n+1,1}^{p-1} \cdots x_{m1}^{p-1}$$

PROOF. At first observe that

$$\pi(f_0) = \sum_{\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p} \prod_{i=1}^{n} (\alpha_i x_{ii})^{p-1} \times \prod_{i=n+1}^{m} (\alpha_1 x_{i1})^{p-1}$$

$$= x_{11}^{p-1} x_{22}^{p-1} \cdots x_{nn}^{p-1} x_{n+1,1}^{p-1} \cdots x_{m1}^{p-1} \times \sum_{\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p} \alpha_1^{(m-n+1)(p-1)} \alpha_2^{p-1} \cdots \alpha_n^{p-1}$$

and since

$$\sum_{\alpha \in \mathbb{F}_p} \alpha^s = \begin{cases} -1, & \text{if } s = \mu(p-1) \neq 0; \\ 0, & \text{otherwise} \end{cases}$$

for every integer $s \geq 0$, we get

$$\pi(f_0) = (-1)^n x_{11}^{p-1} x_{22}^{p-1} \cdots x_{nn}^{p-1} x_{n+1,1}^{p-1} \cdots x_{m1}^{p-1}$$

which ends the proof. ∎

4.4 Orbit Sums Revisited

For any monomial $f = x_{11}^{s_{11}} \cdots x_{1n}^{s_{1n}} \cdots x_{m1}^{s_{m1}} \cdots x_{mn}^{s_{mn}} \in A_{mn}$ we compute its orbit sum, $S_H(f)$. Note that if $\gamma(f) \neq f$ then we have;

$$S_H(f) = \sum_{\sigma \in H} \sigma(f) = \sum_{\alpha \in \mathbb{F}_p} \gamma^\alpha(f) = \sum_{\alpha \in \mathbb{F}_p} \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\gamma^\alpha(x_{ij}))^{s_{ij}}.$$

Letting $\nu_\rho = \sum_{k=0}^{\rho} n_k$ with the convention $n_0 = 0$ in the inequalities (4.1), we get

$$\gamma^\alpha(x_{ij}) = \sum_{k=j}^{\nu_\rho} \binom{\alpha}{k-j} x_{ik} \qquad \text{where} \qquad \nu_{\rho-1} + 1 \leq j \leq \nu_\rho.$$

Combining these two equations, the orbit sum of the monomial f becomes;

$$S_H(f) = \sum_{\alpha \in \mathbb{F}_p} \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \left(\sum_{k=j}^{\nu_\rho} \binom{\alpha}{k-j} x_{ik} \right)^{s_{ij}}$$

where the inner sum makes sense only if $\nu_{\rho-1} + 1 \leq j \leq \nu_\rho$, i.e.

$$S_H(f) = \sum_{\alpha \in \mathbb{F}_p} \prod_{i=1}^{m} \prod_{\rho=1}^{t} \prod_{j=\nu_\rho+1}^{\nu_\rho} \left\{ \sum_{k=j}^{\nu_\rho} \binom{\alpha}{k-j} x_{ik} \right\}^{s_{ij}}$$

Using the projection defined in (4.3) we obtain; $\pi(S_H(f)) = 0$ or

$$\begin{aligned} \pi(S_H(f)) &= \sum_{\alpha \in \mathbb{F}_p} \left(\prod_{\rho=1}^{t} \prod_{i=\nu_{\rho-1}+1}^{\nu_\rho} \prod_{j=\nu_{\rho-1}+1}^{i} \left\{ \binom{\alpha}{i-j} x_{ii} \right\}^{s_{ij}} \right) \left(x_{n+1,1}^{s_{n+1,1}} \cdots x_{m1}^{s_{m1}} \right) \\ &= x_{11}^{s_{11}} x_{22}^{\eta_2} \cdots x_{nn}^{\eta_n} x_{n+1,1}^{s_{n+1,1}} \cdots x_{m1}^{s_{m1}} \times C \end{aligned}$$

where

$$\eta_i = \sum_{j=\nu_{\rho-1}+1}^{i} s_{i,j} \qquad \text{provided that} \qquad \nu_{\rho-1}+1 \leq i \leq \nu_\rho,$$

and $C \in \mathbb{F}_p$ is a constant depending on f and given explicitly as;

$$C = \sum_{\alpha \in \mathbb{F}_p} \binom{\alpha}{0}^{\varepsilon_0} \binom{\alpha}{1}^{\varepsilon_1} \cdots \binom{\alpha}{n_1-1}^{\varepsilon_{n_1-1}}$$

with the convention $\varepsilon_0 = s_{11} + \cdots + s_{nn} + s_{n+1,1} + \cdots + s_{m1}$ and;

$$\varepsilon_i = \sum_{\rho=1}^{k} \sum_{j=\nu_{\rho-1}+i+1}^{\nu_\rho} s_{j,j-i}, \qquad n_1 \geq n_2 \geq \cdots \geq n_k > i \geq n_{k+1} \geq \cdots \geq n_t \geq 1.$$

For example;

$$\varepsilon_1 = s_{21} + s_{32} + \cdots + s_{n_1,n_1-1} + s_{n_1+2,n_1+1} + \cdots + s_{\nu_{t-1},\nu_{t-1}-1} + s_{\nu_{t-1}+2,\nu_{t-1}+1} + \cdots + s_{n,n-1}$$

and

$$\varepsilon_{n_t} = s_{n_t+1,1} + \cdots + s_{n_1,n_1-n_t} + s_{n_1+n_t+1,n_1+1} + \cdots + s_{\nu t-2,\nu_{t-2}-n_t} + \cdots + s_{\nu t-2+n_t+1,\nu_{t-2}+1} + \cdots + s_{\nu_{t-1},\nu_{t-1}-t_s}$$

We are mostly interested in the constant C given above since we are searching for monomials with a nonzero projection to be able to express our global invariant f_0 in terms of these ones. Further calculations of C becomes more and more complicated to generalize. For this reason we will just look for minimum conditions on the monomial f to provide a nonzero C. If we expand the sum of combinations by defining

$$d_i = \sum_{k=i}^{n_1-1} \varepsilon_k$$

we get

$$C = C_1 \sum_{\alpha \in \mathbb{F}_p} \alpha^{d_1} (\alpha-1)^{d_2} \cdots (\alpha - n_1 + 2)^{d_{n_1}-1} \tag{4.4}$$

where C_1 is a nonzero constant in $\mathbb{F}_p$. Since we want $\pi(S_H(f)) \neq 0$; we should have $d_1 + \cdots + d_{n_1-1} \geq p-1$ in equation (4.4) . But then we get

$$s_{21} + (s_{31} + s_{32}) + \cdots + (s_{n_1 1} + \cdots + s_{n_1,n_1-1}) + (s_{n_1+2,n_1+1}) + \cdots + (s_{n,\nu_{t-1}+1} + \cdots + s_{n,n-1}) \geq \frac{p-1}{n_1-1} \tag{4.5}$$

Remark 4.4.1 *Here we used an estimation which seems to be useful for partial results but not sharp enough. Further computations may yield better results. The estimation given above seems to carry us to our goal.*

4.5 A Strong Assumption

As we see in Section 3.3, every invariant polynomial can written in terms of orbit sums of monomials in the non-modular case. Now suppose that this is also the case in modular case. This assumption is however not always true. It should be investigated in detail that which groups may admit orbit Chern classes of monomials as generators of the invariant algebra. But nevertheless, the algebra generated by orbit Chern classes of monomials is a subalgebra of the invariant.

4.5.1 Main Result

Theorem 4.5.1 *If* $|G| \equiv 0$ *in* k, *then* $\beta(G, V^m) \geq \frac{m}{rank(V)}$ *provided that* $m \geq rank(V)$ *for any vector space* V *over the field* $\boldsymbol{k}$.

PROOF. Noting the total degree of variables

$$x_{22}, \cdots, x_{n_1 n_1}, x_{n_1+2, n_1+2}, \cdots, x_{n_{\nu_i} n_{\nu_i}}, x_{n_{\nu_i+2} n_{\nu_i+2}}, \cdots, x_{nn}$$

in (4.3.1) is $(n-t)(p-1)$ and using the degree inequality for monomials f given in (4.5); we can conclude that at most

$$\frac{(n-t)(p-1)}{(p-1)/(n_1-1)} = (n_1-1)(n-t)$$

of such monomials f, can be used to get f_0. Moreover the degree of $\pi(f_0)$ is $m(p-1)$, and only part of it which has degree at most $t(p-1)$ can be written by invariant monomials. So at least the part of it of degree at least $(m-t)(p-1)$ must be written by at most $(n_1-1)(p-1)$ monomial sums. Hence there should be an indecomposable monomial sum of degree at least $\frac{m-t}{n-t}\frac{p-1}{n_1-1}$ giving us;

$$\beta(G, V^m) \geq \frac{m-t}{n-t}\frac{p-1}{n_1-1} \geq \frac{m-t}{n-t} \geq \frac{m}{n} \qquad \text{where } n = \dim V. \tag{4.6}$$

which completes the proof. ∎

Remark 4.5.2 *As equation (4.6) shows, modular invariant theory is much more dependent with the representation of the given group. For example if G has a representation with $n_1 = 2$, then the bound given gets a factor of $p-1$ and results in $\beta(G, V^m) \geq m(p-1)/n$ which is much closer to the bound we started with. Moreover, assuming $n_1 = 2$, $n_2 = \cdots = n_t = 1$ we get a similar result to one in [11] since in that case, $t = n-1$ and hence $\beta(G, V^m) \geq (m-n+1)(p-1)$. Different representations yields different results and the general bound can not be improved so much by this reason.*

Chapter 5

Examples

We will provide here some examples to illustrate the idea and the cases when this idea does not work. The main point is to see that orbit sums of monomials do not always generate the invariant algebra.

5.1 A Short Example

Let $p = 3$ and consider the cyclic group H of order 3. Previous discussions shows that when $n = 2$ we have;

$$H = \left\{ \gamma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

Suppose further that $m = 2$. Hence we can identify the polynomial algebra by $A_{22} = \mathbb{F}_3[x_1, x_2; y_1, y_2]$ where the action is given by

$$\gamma(x_1) = x_1 + x_2, \quad \gamma(x_2) = x_2,$$

$$\gamma(y_1) = y_1 + y_2, \quad \gamma(y_2) = y_2.$$

Let's try to find A_{22}^H. This can be done most easily by considering the homogeneous polynomials of small degree. Let f be an invariant homogeneous polynomial of degree d. I.e.

$$f = \sum_{i+j+k+l=d} a_{ijkl} x_1^i x_2^j y_1^k y_2^l \in A_{22}^H \qquad \text{where} \quad a_{ijkl} \in \mathbb{F}_3.$$

For $d = 1$, we found that $f = ax_2 + by_2$, which are obviously invariant since x_2, y_2 belongs to fixed point set, i.e. to $(V^*)^H$.

For $d = 2$, considering the coefficients of all monomials in $\gamma(f) - f$, it is found that

$$f = ax_2^2 + bx_2y_2 + cy_2^2 + e(x_1y_2 + 2x_2y_1)$$

and note that the last summand is an indecomposable invariant. Up to now we have found 3 indecomposable invariants and thus we should continue for $d = 3$.

For $d = 3$ with the same technique, excluding the trivial ones, we found that

$$f = a(x_1^3 + 2x_1x_2^2) + b(y_1^3 + 2y_1y_2^2)$$

Hence now we have 5 indecomposable invariant, namely;

$$c_1(x_2),\ c_1(y_2),\ c_3(x_1),\ c_3(y_1),\ \text{and}\ \omega := x_1y_2 + 2x_2y_1.$$

Since we found more indecomposable invariants than the number of variables, it is reasonable to check whether they are sufficient to generate the whole invariant algebra.

Using a lexicographic order $x_1 \succ y_1 \succ x_2 \succ y_2$ and defining *leading monomial* of any polynomial to be the maximal one appearing with a nonzero coefficient in f with respect to the lexicographic order defined, it is easy by induction that any invariant polynomial f can be written as a polynomial in $x_2,\ y_2,\ c_3(x_1),\ c_3(y_1),$ and ω. Hence $A_{22}^H = \mathbb{F}_3[x_2, y_2, \omega, c_3(x_1), c_3(y_1)]$, but as in example (2.2.3) there should be an algebraic dependence on generators. Further calculations result in;

$$A_{22}^H \cong \mathbb{F}_3[x_2, y_2, \omega, c_3(x_1), c_3(y_1)]/(\omega^3 - c_3(x_1)y_2^3 + x_2^3c_3(y_1) + x_2^2y_2^2\omega)$$

and therefore, again A_{22}^H is found to be a free module over the subalgebra $\mathbb{F}_3[x_2, y_2, c_3(x_1), c_3(y_1)]$ with secondary generators $1, \omega$, and ω^2 (Note that $c_i()$ represents the orbit Chern class).

5.2 A Counter-example

Before explaining the counter-example, a short remark is necessary at that point. Among the generators found above, we make use of the top Chern class of orbits. But in the proof of my main result, I just consider the first orbit

Chern classes. The reason is that the so called universal invariant has a degree at most $p-1$ in each variable. So if one uses orbit Chern classes other than the first one, then the degree of the monomial to be considered should have a degree at least p, which is impossible.

Now it is time to explain the counter-example. Note that it is impossible to express ω as an orbit sum of any monomial. This is the reason why we insist on the assumption that *every invariant which has degree at most $p-1$ with respect to each variable can be written as a polynomial in orbit sums of monomials.* But if we compute further that, $\omega \in A_{22}^G$ iff $G \subset SL(2, \mathbb{F}_3)$, hence for any group G not contained in the special linear group such that $|G| \equiv 0$ in $\mathbb{F}_3$, our idea works fine. Therefore it is worth to find an answer to the following question which is currently not investigated or not known:

Problem 1 *For any group G not contained in $SL(n, \mathbb{F}_p)$ with $|G| \equiv 0$ in $\mathbb{F}_p$, is it possible to express all invariants, which have degrees at most $p-1$ with respect to each variable, in terms of orbit sums of monomials?*

5.3 Further Aspects of the Subject

We try to find an indecomposable invariant of cyclic groups of sufficiently large degree. This can be achieved only by examining the invariants in detail. But there is more than shown here. If we try to find an indecomposable invariant of cyclic group only, then the things become easier. For example, if m and n_1 are sufficiently large enough, then for any integer $d \geq 0$ there exists an indecomposable invariant of degree d. This can be proved directly from [7, Lemma 5, Corollary 4]. We will state these results without proofs.

Lemma 5.3.1 (G. Kemper) *Let σ be the automorphism of $k[x_{i,j} \mid 1 \leq i \leq m, 0 \leq j \leq n]$ given by*

$$\begin{aligned} \sigma: \quad & x_{i,j} \mapsto x_{i,j} + x_{i,j+1} \quad (1 \leq i \leq m,\ 0 \leq j \leq n-1), \\ & x_{i,n} \mapsto x_{i,n} \quad (1 \leq i \leq m). \end{aligned}$$

Define for a monomial $t = \prod_{i=1}^{m} \prod_{j=0}^{n} x_{i,j}^{e_{i,j}}$

$$w(t) = \sum_{i=1}^{m} \sum_{j=0}^{n} j \cdot e_{i,j} + p\text{-gcd}(e_{i,j} \mid 1 \leq i \leq m,\ 0 \leq j \leq n).$$

Then any monomial t occurring in an invariant must have $w(t) > n$.

Corollary 5.3.2 (G. Kemper) *With the notations of the above lemma, let t be a monomial occurring in a homogeneous invariant $f \in k[x_{i,j}]^\sigma$ of degree d, and suppose that each nonconstant strict divisor t' of t with $w(t') > n$ satisfies $w(t/t') \leq n$. Then f is irreducible.*

Hence for our goal it is not sufficient to think the cyclic groups alone. To get a general result, we should try to find a global invariant which cannot be expressed as a polynomial in invariants of cyclic subgroup of less degree.

Another interest of the modular invariant theory is to consider the groups generated by pseudo-reflections. The reason is that in positive characteristic, a pseudo-reflection need not be diagonalizable. For this purpose, transvections are introduced.

Definition 5.3.3 *An element $T \in GL(n,k)$ is called a* **transvection** *with hyperplane H_T, transvector $0 \neq x \in H_T$, and a direction $\mathrm{Span}_k\{x\}$, if there is a linear functional $\phi_T : V \to k$ such that $H_T = \ker(\phi_T)$ and $T(v) = v + \phi_T(v) \cdot x$ for all $v \in V$.*

If a transvection has finite order then it is a non-diagonalizable pseudo-reflection. If k has characteristic zero then transvections have infinite order. If the field k has characteristic p then every transvection has order p, and so is a pseudo-reflection. To sum up, in positive characteristic the transvections are exactly the non-diagonalizable pseudo-reflections and in zero characteristic they are never pseudo-reflections. Known results about both pseudo-reflections and transvections can be found in [16, pp. 242-256].

As stated in the quotation given in the Introduction, using new techniques provides some partial answers to this old problem. Finiteness problems continue to be one of the most interesting aspects of invariant theory. Both the upper and the lower bounds on the degrees of a set of generating polynomials for the algebra of invariants, lead to a number of basic open problems in the theory of finite groups in any characteristic.

References

[1] H.E.A. Campbell, I. Hughes, R.D. Pollack, *Vector Invariants of Symmetric Group*, Canad. Math. Bull. **33** (1990) 391-397.

[2] H.E.A. Campbell, I. Hughes, R.D. Pollack, *Rings of Invariants and p-Sylow Subgroups*, Canad. Math. Bull. **34**, (1991) 42-47.

[3] H.E.A. Campbell, A.V. Geramita, I.P. Hughes, R.J. Shank, D.L. Wehlau, *Non-Cohen-Macaulay Vector Invariants and a Noether Bound for a Gorenstein Ring of Invariants*, Canad. Math. Bull. **42** (1999) 155-161.

[4] H.E.A. Campbell, I.P. Hughes, *Rings of Invariants of Certain p-Groups over the Field* $\mathbb{F}_p$, J. Algebra, **211** (1999) 549-561.

[5] P. Fleischmann, *A New Degree Bound for Vector Invariants of Symmetric Groups*, Trans. Amer. Math. Soc. **350** (1998) 1703-1712.

[6] P. Fleischmann, *The Noether Bound in Invariant Theory of Finite Groups*, to appear.

[7] Gregor Kemper, *Lower Degree Bounds for Modular Invariants and a Question of I. Hughes*, Trans. Groups, **2** (1998) 135-144.

[8] A.A. Klyachko, *Lecture Notes of "Invariant Theory"*, taught by A.A. Klyachko in 1999-2000 Spring semester at Bilkent University

[9] J.P.S. Kung, G.-C. Rota, *The Invariant Theory of Binary Forms*, Bull. Amer. Math. Soc. (N.S.) **10** (1984) 27-85.

[10] David R. Richman, *The Fundamental Theorems of Vector Invariants*, Adv. in Math. **73** (1989) 43-78.

[11] David R. Richman, *On Vector Invariants over Finite Fields*, Adv. in Math. **81** (1990) 30-65.

[12] David R. Richman, *Invariants of Finite Groups over Fields of Characteristic p*, Adv. in Math. **124** (1996) 25-48.

[13] David R. Richman, *Explicit Generators of the Invariants of Finite Groups*, Adv. in Math. **124** (1996) 49-76.

[14] B.J. Schmid, *Finite Groups and Invariant Theory*, Séminar d'Algébre P. Dubriel et M.-P. Malliavin 1989-1990, Lecture Notes in Math. 1478, 1991.

[15] R.James Shank, David L. Wehlau, *The Transfer in Modular Invariant Theory*, J. Pure Appl. Algebra, **412** (1999) 63-77.

[16] Larry Smith, *Polynomail Invariants of Finite Groups*, A. K. Peters, 1995.

[17] Larry Smith, *Polynomial Invariants of Finite Groups a Survey of Recent Developments*, Bull. Amer. Math. Soc. (N.S.), **34** (1997) 211-250.

[18] Larry Smith, *Invariant Theory and the Koszul Complex Representations of $\mathbb{Z}/p$ in Characteristic p Applications*, to appear.

[19] Serguei A. Stepanov, *Modular Invariant of Finite Groups*, Preprint, 2000.

[20] Serguei A. Stepanov, *Vector Invariants of Symmetric Groups in Prime Characteristic*, Preprint, September 1999.

[21] Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, 1993.

[22] H. Weyl, *The Classical Groups*, Princeton Univ. Press, Princeton, 1942.