INVARIANT RINGS OF MODULAR P-GROUPS

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS

AND THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

By

Ceren Coşkun Toper

January, 2013

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. Müfit Sezer(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.

Assist. Prof. Dr. Özgün Ünlü

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. Ayşe Çiğdem Özcan

Approved for the Graduate School of Engineering and Science:

Prof. Dr. Levent Onural
Director of the Graduate School

ABSTRACT

INVARIANT RINGS OF MODULAR P-GROUPS

Ceren Coşkun Toper
M.S. in Mathematics
Supervisor: Assoc. Prof. Dr. Müfit Sezer
January, 2013

We consider a finite group acting as linear substitutions on a polynomial ring and study the corresponding ring of invariants. Computing the invariant ring and finding its ring theoretical properties is a classical problem. We focus on the modular case where the characteristic of the field divides the order of the group. We review invariants of basic modular actions and give explicit descriptions of invariants of small dimensional actions. We also discuss a recent algorithm that computes the invariant ring of a modular p-group up to a localization and we apply this algorithm to invariants of indecomposable representations of a cyclic group of prime order.

Keywords: modular group actions, invariants, polarization, generating sets, localization.

ÖZET

MODÜLER P-GRUPLARIN İNVARYANT HALKALARI

Ceren Coşkun Toper
Matematik, Yüksek Lisans
Tez Yöneticisi: Doç. Dr. Müfit Sezer
Ocak, 2013

Sonlu bir grubun bir polinom halkasına lineer bir etkimesini ele alıp bu etkimeye karşılık gelen invaryant halkayı çalışıyoruz. İnvaryant halkasının hesaplanması ve cebirsel özelliklerinin bulunması klasik bir problemdir. Biz cismin karakteristiğinin gruptaki eleman sayısını böldüğü modüler duruma odaklanıyoruz. Temel modüler etkimelerin invaryantlarını gözden geçirip küçük boyutlu bazı etkimelerin invaryantlarının üreteçlerini açık bir şekilde veriyoruz. Modüler bir p-grubun invaryantlarını içeren bir cismi hesaplayan, yakın zamanda bulunmuş bir algoritmayı çalışıp bu algoritmayı asal mertebeli devirli grupların parçalanamaz temsillerine uyguluyoruz.

Anahtar sözcükler: modüler grup etkimeleri, invaryantlar, polarizasyon, üretici kümeler, lokalizasyon .

Acknowledgement

I would like to express my sincerest gratitude to my supervisor, Assoc. Prof. Dr. Müfit Sezer who has supported me throughout my thesis with his guideness, encouragement and valuable suggestions. One simply could not wish for a friendlier or better supervisor.

I would like to thank Assist. Prof. Dr. Özgün Ünlü and Prof. Dr. Ayşe Çiğdem Özcan for reading this thesis.

I am grateful to my family members for their love and their support in every stage of my life.

I would like to express my gratitude to my dear husband Türkay Toper for his never-ending patience, continual support and love.

I also thank all my friends who have supported me in many ways during the creation period of this thesis.

The work that form the content of the thesis is supported financially by TÜBİTAK through the graduate fellowship program, namely "TÜBİTAK-BİDEB 2210- Yurt İçi Yüksek Lisans Programı". I am grateful to the council for their kind support.

Contents

Chapter 1

Introduction

Invariant theory tries to determine whether a mathematical object can be obtained from some other object by the action of some group. One way to answer this question is to construct "invariant polynomials". These are polynomial functions from the class of objects to some field which take the same value on any two objects which are related by an element of the group. Thus if we can find any invariant which takes different values on two objects, then these two objects cannot be related by an element of the group. Ideally, one would like to find enough invariants to distinguish as many orbits as possible. This means we want to find a (finite) set of invariants $f_1, f_2, \ldots, f_r$ with the property that if two objects are not related by the group action then at least one of these r invariants takes different values on the two objects in question.

This fascinating field was brought to life at the beginning of the last century. One of the central results in this area is the theorem about the finiteness of the number of fundamental invariants which is proved by Hilbert at the end of the nineteenth century. The celebrated theorems of Hilbert, like the Basis Theorem, the Syzygy Theorem, and Nullstellensatz were all born as lemmas for proving important theorems in invariant theory. Generally speaking, the invariant theory has applications in commutative algebra, topology, geometry and homological algebra, and on the other direction, these fields are sources that provide powerful tools to attack problems in invariant theory.

A central problem in invariant theory is to determine the invariant ring by finding a generating set explicitly. Knowing the degrees of the generators is very critical for this purpose because it reduces the problem to a linear algebra problem in a finite dimensional vector space. In the first quarter of the twentieth century, Noether made a big contribution to these problems with obtaining a bound on degrees of the generators. Specifically, she proved that if G is finite and the characteristic of the field does not divide $|G|$ (i.e. in the non-modular case), then the ring of invariants for G is always generated by invariants of degree at most $|G|$. This bound is called the Noether bound. However, Noether originally proved this over fields of characteristic zero. To extend this bound to all characteristics not dividing the order of the group could be achieved almost a hundred years later, [1], [2].

Many questions which are well understood in the non-modular case are still open in the modular case(i.e. when the characteristic of field divides $|G|$). Modular invariant theory is a recent trend which has emerged as an active research area in the last decade or so. Many tools and techniques that working the non-modular case do not carry over to the modular situations and modular invariant rings tend to be more complicated. Generally speaking, the degrees of the generators grow large and the invariant ring moves away from being a regular ring which means we get more and more relations among the generators. For instance, Noether bound is not true in general in the modular case. In fact, we know that one can not get a bound that depends only on the group order. Due to this complications, finding an explicit generating set for the invariants of a modular group is a difficult task. Even in the simplest modular case of a cyclic group of prime order explicit generating sets are known for a handful of cases only and we are still a very long way from being able to write down algebra generators in the general case. We direct the reader to [3], [4], [5], [6], [7], [8], [9] for some major results on this matter.

In this thesis, we restrict to the modular case and start by describing the modular actions of a cyclic group of prime order. We review basic properties of its invariants and give explicit descriptions of invariants of any vector copies of

the two dimensional indecomposable representations. Then we study an algorithm due to Chuai and Campbell [10] that computes the invariants of a modular p-group up to a localization. This algorithm realize on computing invariant polynomials with minimal positive degree in certain variables and our background on invariants of cyclic groups of prime order allows us to apply this algorithm to these groups and we obtain a localized invariant subalgebra that contains the full invariant ring. This method has the potential to be very useful to study the invariants of non-cyclic abelian modular p-groups and this provides us a perspective for future research. Another tool in constructing these critical polynomials is the polarization. This is a classical tool in invariant theory that goes back to Weyl and we also have a section that provides a background on polarization.

Chapter 2

Modular Invariants of Cyclic Group of Prime Order

2.1 Preliminaries

We consider a finite dimensional representation ρ of a group G over a field $\mathbb{F}$, i.e., a group homomorphism

$$\rho : G \to GL(V)$$

where V is a finite dimensional vector space over a field $\mathbb{F}$.

The representation defines a left action of the group G on V. Given $\sigma \in G$ and $v \in V$ we write $\sigma(v)$ for the vector $\rho(\sigma)(v)$, the result of applying $\rho(\sigma)$ to v.

We denote the set of vectors fixed (pointwise) by the group G by

$$V^G = \{v \in V \mid \sigma(v) = V, \text{ for all } \sigma \in G\}.$$

Now consider V^*, the vector space dual to V. This dual space V^* consists of all linear functionals from V to $\mathbb{F}$ and is denoted by $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$. Recall that $x : V \to \mathbb{F}$ is said to be a linear functional if $x(av + bw) = ax(v) + bx(w)$ for all $v, w \in V$, and all $a, b \in \mathbb{F}$. Of course, we have $\dim_{\mathbb{F}}(V^*) = \dim_{\mathbb{F}}(V)$.

The action of G on V determined by the representation ρ naturally induces a left action of G on V^* as follows. Let $x \in V^*$ be any linear functional on V and let $\sigma \in G$. Then $\sigma(x)$ should be another linear functional on V. This new linear functional is defined by $(\sigma(x))(v) := x(\sigma^{-1}(v))$. In this definition we use σ^{-1} instead of σ in order to obtain a left action (and not a right action) of G on V^*. This new representation of G is often referred to as the dual representation.

We extend this action linearly to the entire vector space V^*. This gives a left linear action of G on V^*. We obtain a faithful action iff the representation of G is faithful.

Often we simultaneously consider actions on V and V^* and so we note down how to pass from one action to the other.

Lemma 2.1.1. *Suppose we have a fixed representation $\rho : G \to GL(V)$ and consider also $\rho^* : G \to GL(V^*)$. In general, for $\sigma \in G$ the matrix representing $\rho(\sigma) \in GL(V)$ with respect to a fixed basis is the transpose inverse of the matrix representing $\rho^*(\sigma)$ with respect to the dual basis.*

So far we have an action of G on the vector space V given by a linear representation $\rho : G \to GL(V)$ which induces an action of G on the dual space V^*. This action also naturally induces an action of G on all polynomial functions as we see next.

Let $\{x_1, x_2, \ldots, x_n\}$ be a fixed basis of V^*. Then we denote by $\mathbb{F}[V]$ the ring of polynomials in n indeterminants $x_1, x_2, \ldots, x_n$ with coefficients from a field $\mathbb{F}$, i.e., $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$.

For an exponent sequence $I = (i_1, \ldots, i_n)$ consisting of non-negative integers, we define the monomial

$$x^I = {x_1}^{i_1} \ldots {x_n}^{i_n}.$$

We say that x^I has degree $i_1 + \ldots + i_n$ and we denote the degree of x^I by $\deg(x^I)$ or $\deg(I)$. An arbitrary polynomial $f \in \mathbb{F}[V]$ can be written as a finite sum

$$f(x_1, \ldots, x_n) = \sum a_j x^{I_j} \text{ of terms } a_j x^{I_j}.$$

As usual, we say that a polynomial $f = \sum a_j x^{I_j}$ for $a_j \in \mathbb{F}$ is homogeneous of degree d if each of its monomials, x^{I_j}, is of degree d. We observe that $\mathbb{F}[V]$ is naturally graded by degree: we may write $\mathbb{F}[V] = \oplus_{d \geq 0} \mathbb{F}[V]_d$ where $\mathbb{F}[V]_d$ denotes the subspace of homogeneous polynomials of degree d (including the zero polynomial). We also observe that $\mathbb{F}[V]$ is a graded algebra. This just means that each $\mathbb{F}[V]_d$ is a subspace and that if $f \in \mathbb{F}[V]_d$ and $f' \in \mathbb{F}[V]'_d$ then $ff' \in \mathbb{F}[V]_{d+d'}$.

We define the G-action on a monomial as

$$\sigma({x_1}^{i_1} \dots {x_n}^{i_n}) = (\sigma(x_1))^{i_1} \dots (\sigma(x_n))^{i_n}$$

for $\sigma \in G$, i.e., we extend the action multiplicatively. To obtain an action of G on all polynomials, we also extend the action linearly:

$$\sigma f = \sigma(\sum a_j x^{I_j}) = \sum a_j \sigma(x^{I_j}).$$

Thus altogether we have

$$\sigma f(v) = f(\sigma^{-1}(v)), \text{ for all } \sigma \in G, \ v \in V \text{ and } f \in \mathbb{F}[V].$$

The main object of study in invariant theory is the collection of polynomial functions on V left fixed by all of G. We call a polynomial $f \in \mathbb{F}[V]$ invariant under the group action of G if

$$\sigma(f) = f, \text{ for all } \sigma \in G.$$

We denote by $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$ the subset of all invariant polynomials. That is

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid \sigma(f) = f \text{ for all } \sigma \in G\}.$$

Since the action is additive and multiplicative, sum of and product of invariant polynomials are also invariant. Thus the subset of all invariant polynomials is a subring. This ring is called the ring of invariants.

Since the group action preserves degree, if a polynomial is invariant under the group action of G then its homogeneous components are also invariant. This makes $\mathbb{F}[V]^G$ a graded subalgebra.

For a general reference for invariant theory we recommend [11], [12], [13], [14], [15], [16].

2.1.1 Some Basic Invariants

We have general methods to construct invariants of finite groups as follows.

Let $f \in \mathbb{F}[V]$. Then the *transfer* or *trace* of f is defined as

$$Tr(f) = Tr^G(f) = \sum_{g \in G} g(f).$$

Note that for all $h \in G$ we have

$$hTr^G(f) = \sum_{g \in G} h(gf) = \sum_{g \in G} (hg)f = \sum_{g' \in G} g'(f) = Tr^G(f),$$

because if $g \in G$ runs through all group elements, then hg (for a fixed h) does too. Therefore the image of the transfer is contained in the ring of invariants

$$Tr^G : \mathbb{F}[V] \to \mathbb{F}[V]^G.$$

Similarly, the *norm* of f is defined by

$$N(f) = N^G(f) = \prod_{g \in G} g(f).$$

2.1.2 Modular Actions of C_p

Let $G = C_p$ denote the cyclic group of order p. In this section, we study the representation of C_p over a field $\mathbb{F}$ of characteristic p.

We consider a finite dimensional indecomposable C_p-module V. In representation terminology, this means we have a finite dimensional indecomposable representation $\rho : G \to GL(V)$. We fix a generator σ of C_p. Now since $\sigma^p = 1$, every eigenvalue λ of σ must be a p^{th} root of unity. Thus $0 = \lambda^p - 1 = (\lambda - 1)^p$ and so $\lambda = 1$ is the only p^{th} root of unity in $\mathbb{F}$. Since the only eigenvalue of σ lies in $\mathbb{F}$, we may choose a basis $\{e_1, e_2, \ldots, e_n\}$ of V such that $\rho(\sigma)$ is in (lower) Jordan normal form with respect to this basis. If there are two or more Jordan blocks in this Jordan normal form these blocks yield a decomposition of V into a

direct sum of smaller C_p-modules contradicting the indecomposability of V. Thus

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 0 & \ddots & 0 & 0 \\ 0 & 1 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

Lemma 2.1.2. *The matrix above has order p^l if and only if $p^{l-1} < n \leq p^l$. In particular, this matrix has order p if and only if $1 < n \leq p$.*

Definition 2.1.3. For each n with $1 \leq n \leq p$ we denote the indecomposable C_p-module of dimension n by V_n.

We note that $\sigma(e_n) = e_n$ and $\sigma(e_i) = e_i + e_{i+1}$ for $1 \leq i \leq n-1$. We call such a basis a *triangular* basis of V_n and we say that e_1 is distinguished. Notice that the C_p-module generated by e_1 is all of V_n.

If the matrix $\rho(\sigma)$ has dimension greater than p^r then its order will be also greater than p^r and so greater than the order of the group which cannot be happen. Therefore, the matrix can have order at most p^r. Also note that every dimension in the Jordan block corresponds to a indecomposable C_p-module. Thus there can be at most p^r many indecomposable C_p-modules.

The preceding discussion , combined with Lemma 2.1.2, proves the following lemma.

Lemma 2.1.4. *Over any field of characteristic p, there are exactly p^r inequivalent indecomposable representation of C_{p^r}, one of dimension n for each n less than or equal to p^r. Furthermore, we have the following chain of inclusions:*

$$V_1 \subset V_2 \subset \ldots \subset V_{p^r}.$$

2.2 Invariants of V_2 and Its Vector Sums

2.2.1 Example: C_p Represented on a 2 Dimensional Vector Space in Characteristic p

As a simple example of a modular group action, consider the vector space V_2 of dimension 2 over a field $\mathbb{F}$ of characteristic $p > 0$ with basis $\{e_1, e_2\}$.

Let C_p denote the cyclic group of order p generated by σ. Consider the matrix

$$\tau = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

inside $GL(2, \mathbb{F})$ where $\mathbb{F}$ is a field of characteristic p. Using induction, it is easy to show that

$$\tau^i = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$$

Therefore, we obtain a representation $\rho : C_p \to GL(V_2)$ given by the rule $\rho(\sigma^i) = \tau^i$. We have $\sigma(e_1) = \tau(e_1) = e_1 + e_2$ and $\sigma(e_2) = \tau(e_2) = e_2$.

Let $\{x, y\}$ be the basis for V_2^* dual to $\{e_1, e_2\}$. Then the action on the dual basis is $\sigma(x) = x$ and $\sigma(y) = -x + y$ by Lemma 2.1.1.

We see immediately that the polynomial x is an invariant under this action. Moreover, since $(y + x)^p = y^p + x^p$,

$$\begin{aligned} \sigma(y^p - x^{p-1}y) &= \sigma(y)^p - \sigma(x)^{p-1}\sigma(y) \\ &= (y - x)^p - x^{p-1}(y - x) \\ &= y^p - x^p - x^{p-1}y + x^p \\ &= y^p - x^{p-1}y \end{aligned}$$

Therefore the polynomial $N = y^p - x^{p-1}y$ is another example of an invariant. Now, we will see that for this representation, these two invariants are the two most important invariants.

Lemma 2.2.1. $N^{C_p}(y) = y^p - x^{p-1}y$.

Our aim is to show that the ring of C_p-invariants is the algebra generated by the two invariants N and x.

Theorem 2.2.2. $\mathbb{F}[V_2]^{C_p} = \mathbb{F}[x, N]$.

Before proving this theorem, we need to prove some preliminary results.

Lemma 2.2.3. *Let $f \in \mathbb{F}[V_2]$. Then $deg_y(\sigma(f)) = deg_y(f)$.*

Proof. Let $\deg_y(f) = m$ and $f = a_m y^m + a_{m-1}y^{m-1} + \ldots + a_0$ where $a_i \in \mathbb{F}[x]$ and $a_m \neq 0$. Then

$$\begin{aligned}\sigma(f) &= \sigma(a_m)\sigma(y)^m + \sigma(a_{m-1})\sigma(y)^{m-1} + \ldots + \sigma(a_0) \\ &= a_m(y-x)^m + a_{m-1}(y-x)^{m-1} + \ldots + a_0 \\ &= a_m y^m + \text{terms of lower order in } y\end{aligned}$$

Thus $\deg_y(\sigma(f)) = m$. □

N is monic when considered as a polynomial in the variable y with coefficients from $\mathbb{F}[x]$, so we may divide any polynomial $f \in \mathbb{F}[x, y]$ by N to get $f = qN + r$ where $q, r \in \mathbb{F}[x, y]$ are unique with $\deg_y(r) < p = \deg_y(N)$.

Lemma 2.2.4. *If $f \in \mathbb{F}[V_2]^G$ and $f = qN + r$ with $deg_y(r) < p$, then $q, r \in \mathbb{F}[V_2]^G$.*

Proof. We note that it is enough to show that q and r are σ-invariant since σ generates C_p.We have $qN + r = f = \sigma(f) = \sigma(q)\sigma(N) + \sigma(r) = \sigma(q)N + \sigma(r)$ and since $\deg_y(\sigma(r)) = \deg_y(r) < p$ (by the previous lemma), by the uniqueness of remainders and quotients we must have $\sigma(r) = r$ and $\sigma(q) = q$. □

Now we need a result concerning the partial differential operator $\frac{\partial}{\partial y}$.

Lemma 2.2.5. *If $f \in \mathbb{F}[x, y]^G$, then $\frac{\partial}{\partial y}(f) \in \mathbb{F}[x, y]^G$.*

Proof. It is enough to show that $\sigma(\frac{\partial}{\partial y}(f)) = \frac{\partial}{\partial y}(f) = \frac{\partial}{\partial y}(\sigma(f))$ since $f \in \mathbb{F}[x,y]^G$. Therefore, we need to show that σ and $\frac{\partial}{\partial y}$ commute. Also, since both σ and $\frac{\partial}{\partial y}$ are $\mathbb{F}$-linear maps, we need only to show that they commute on monomials:

$$\sigma(\frac{\partial}{\partial y}(x^a y^b) = \sigma(bx^a y^{b-1}) = bx^a(y-x)^{b-1} \text{ and}$$

$$\frac{\partial}{\partial y}(\sigma(x^a y^b)) = \frac{\partial}{\partial y}(x^a(y-x)^b) = bx^a(y-x)^{b-1}$$

□

Now we can give the proof of the Theorem 2.2.2.

Proof. We know that $\mathbb{F}[x,N] \subseteq \mathbb{F}[V_2]^{C_p}$. Thus it remains to prove that each invariant is contained in $\mathbb{F}[x,N]$. To prove this we use induction on degree in y.

Let $f \in \mathbb{F}[V_2]^{C_p}$. If $\deg_y(f) = 0$, then $f \in \mathbb{F}[x] \subseteq \mathbb{F}[x,N]$.

Assume that every invariant whose degree in y is less than d lies in $\mathbb{F}[x,N]$, and now suppose that $\deg_y(f) = d$. Let us divide f by N and get $f = qN + r$ where $m := \deg_y(r) < p$. We will show that $m = 0$. By way of contradiction, assume that $m \geq 1$. By Lemma 2.2.4 and Lemma 2.2.5, $q, r \in \mathbb{F}[V_2]^{C_p}$ and if we apply the partial differential operator $\frac{\partial}{\partial y}$ to r, we get another invariant polynomial. Let h be defined by

$$h := \frac{\partial^{m-1}(r)}{\partial y^{m-1}}.$$

Then $h = ay + b$, where a is a non-zero scalar and $b \in \mathbb{F}[x]$. But on the other side, $h = \sigma(h) = \sigma(ay+b) = a(y-x) + b = ay + b - ax$, so this contradiction shows that we must have $m = 0$. Therefore, $f = qN + r$ where $r \in \mathbb{F}[x]$, $q \in \mathbb{F}[V_2]^{C_p}$ and $\deg_y(q) = d - p$. By the induction hypothesis, $q \in \mathbb{F}[x,N]$ and thus $f \in \mathbb{F}[x,N]$. □

2.2.2 Further Example: C_p Represented on $2V_2$ in Characteristic p

Here we compute the ring of invariants of the group C_p on $2V_2 = V_2 \oplus V_2$. But first we give the following useful lemma.

Lemma 2.2.6. *Suppose H is a normal subgroup of G with quotient group G/H. Let V be a representation of G. Then G/H acts naturally on V^H and $V^G = (V^H)^{G/H}$.*

We apply this lemma to a normal subgroup H of a group G acting on a coordinate ring $\mathbb{F}[V]$. Then we have $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$.

Remark 2.2.7. Let G be any p-group for p a prime and let H be any maximal proper subgroup. Then H is normal in G necessarily of index p. Hence if G is generated by H and σ, we have $G/H = C_p$ generated by $\bar{\sigma}$, the image of σ in G/H.

Now we are considering the action of C_p determined by

$$\sigma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

We introduce

$$\sigma_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\sigma_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Thus $\sigma = \sigma_2\sigma_1^{-1}$.

Let $\{x_1, y_1, x_2, y_2\}$ be the basis for the vector space $(2V_2)^*$ dual to the standard basis of $2V_2$. Thus $\sigma_i(x_j) = x_j$ for $1 \leq i, j \leq 2$, $\sigma_i(y_j) = y_j$ for $1 \leq j \neq i \leq 2$, $\sigma_1(y_1) = y_1 + x_1$ and $\sigma_2(y_2) = y_2 - x_2$. Define G to be the group generated by σ_1 and σ_2, so that $G = C_p \times C_p$ and H to be the group generated by $\sigma = \sigma_2\sigma_1^{-1}$ so that $H = C_p$. We want to compute $\mathbb{F}[2V_2]^H = \mathbb{F}[2V_2]^{C_p}$.

Given the example we computed in the section 2.2.1, it is easy to see that

$$\mathbb{F}[2V_2]^G = \mathbb{F}[V_2]^{C_p} \otimes \mathbb{F}[V_2]^{C_p} = \mathbb{F}[x_1, N(y_1), x_2, N(y_2)].$$

Now we consider the diagram

$$\begin{array}{ccccc} \mathbb{F}(2V_2)^G & \hookrightarrow & \mathbb{F}(2V_2)^H & \hookrightarrow & \mathbb{F}(2V_2) \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{F}[2V_2]^G & \hookrightarrow & \mathbb{F}[2V_2]^H & \hookrightarrow & \mathbb{F}[2V_2] \end{array}$$

where the vertical arrows are also inclusions. By Galois Theory, we have that the field $\mathbb{F}(2V_2)^H$ is an extension of the field $\mathbb{F}(2V_2)^G$ of degree p, that is, $\mathbb{F}(2V_2)^H$ as vector space over $\mathbb{F}(2V_2)^G$ has dimension p. In order to exploit this property, we need to find an element of $\mathbb{F}(2V_2)^H$ that lies outside of $\mathbb{F}(2V_2)^G$.

It is easy to see that the element $u = x_1y_2 - x_2y_1$ is an invariant of least degree in $\mathbb{F}[2V_2]^H$ outside $\mathbb{F}[2V_2]^H$, and therefore $\mathbb{F}(2V_2)^H$ has basis

$$\{1, u, u^2, \ldots, u^{p-1}\}.$$

We see that

$$u^p = x_1^p N(y_2) - x_2^p N(y_1) + x_1^{p-1}x_2^{p-1}u.$$

Theorem 2.2.8.

$$\mathbb{F}[2V_2]^{C_p} = \mathbb{F}[x_1, x_2, N(y_1), N(y_2), u].$$

In fact,

$$\mathbb{F}[2V_2]^{C_p} = \oplus_{i=0}^{p-1}\mathbb{F}[x_1, x_2, N(y_1), N(y_2)]u^i.$$

Proof. Since we noted above that $\mathbb{F}[2V_2]^G = \mathbb{F}[x_1, N(y_1), x_2, N(y_2)]$, our aim is to show that $\{1, u, u^2, \ldots, u^{p-1}\}$ is a basis for $\mathbb{F}[2V_2]^H$ as a module over $\mathbb{F}[2V_2]^G$.

Since G is abelian, we have that H is normal in G and hence by Lemma 2.2.6

$$\mathbb{F}[2V_2]^G = (\mathbb{F}[2V_2]^H)^{G/H}.$$

We note that the image of either σ_1 or σ_2 generates $G/H = C_p$.

We define

$$\begin{aligned} \Delta_1 &= \sigma_1 - \mathrm{Id} \\ \Delta_2 &= \sigma_2 - \mathrm{Id} \text{ and} \\ \Delta &= \sigma - \mathrm{Id} \end{aligned}$$

Consider $f \in \mathbb{F}[2V_2]^H$. Then we have $\sigma(f) = f$ and note that this implies $\sigma_1(f) = \sigma_2(f)$ and thus $\Delta_1(f) = \Delta_2(f)$. In particular, $f \in \mathbb{F}[2V_2]^G$ if and only if $\Delta_1(f) = 0$. Also, for $f \in \mathbb{F}[2V_2]^H$, we have

$$\sigma(\Delta_1(f)) = \sigma_2\sigma_1^{-1}(\sigma_1(f) - f) = \sigma_2(f) - \sigma(f) = \sigma_1(f) - f = \Delta_1(f).$$

Thus $\Delta_1 : \mathbb{F}[2V_2]^H \to \mathbb{F}[2V_2]^H$.

Lemma 2.2.9. *If $f \in \mathbb{F}[2V_2]^H$, then $\Delta_1(f) = x_1x_2f'$ for some $f' \in \mathbb{F}[2V_2]^H$.*

Proof. For any $f \in \mathbb{F}[2V_2]$, we write $f = \sum_{l=0}^{d} f_l y_1^l$ with $f_l \in \mathbb{F}[x_1, x_2, y_2]$ for $0 \leq l \leq d$. Then by the action of σ_1, we see that $\Delta_1(f) = \sum_{l=0}^{d} f_l(y_1+x_1)^l - \sum_{l=0}^{d} f_l y_1^l$. Thus $\Delta_1(f) = x_1f'$. Similarly, $\Delta_2(f) = x_2f''$. If $f \in \mathbb{F}[2V_2]^H$, then $\sigma_1(f) = \sigma_2(f)$ as we noted above, and so $\Delta_1(f) = \Delta_2(f)$, that is, $x_1f' = x_2f''$. But x_1 and x_2 are co-prime in $\mathbb{F}[2V_2]$ and so $\Delta_1(f) = x_1x_2f'''$ for some $f''' \in \mathbb{F}[2V_2]$. Since both $\Delta_1(f)$ and x_1x_2 are H-invariant, we see that $f''' \in \mathbb{F}[2V_2]^H$. □

We now finish the proof of Theorem 2.2.8. Since $\Delta_1^p = (\sigma_1 - \mathrm{Id})^p = \sigma_1^p - \mathrm{Id} = 0$ we see that $\Delta_1^p(f) = 0$ for all $f \in \mathbb{F}[2V_2]$. Thus given $0 \neq f \in \mathbb{F}[2V_2]^H$ there must exist an l, $0 \leq l < p$ with the property that $0 \neq \Delta_1^l(f) \in \mathbb{F}[2V_2]^H$ and $\Delta_1^{l+1}(f) = 0$. We claim that then $f = \sum_{m=0}^{l} f_m u^m$ for $f_m \in \mathbb{F}[2V_2]^G$. We proceed by induction on l. If $l = 0$ then $\Delta_1(f) = 0$ which implies $f \in \mathbb{F}[2V_2]^G$ as we observed above.

For the general case, we write $\Delta_1(f) = x_1x_2f'$ with $f' \in \mathbb{F}[2V_2]^H$ and observe that $f' = \sum_{m=0}^{l-1} f'_m u^m$ with all $f'_m \in \mathbb{F}[2V_2]^G$ by induction. Now consider

$$\begin{aligned}
\Delta_1^l(f + uf'/l) &= \Delta_1^l(f + \frac{1}{l}\sum_{m=0}^{l-1} f'_m u^{m+1}) \\
&= \Delta_1^{l-1}(\Delta_1(f) + \frac{1}{l}\sum_{m=0}^{l-1} f'_m \Delta_1(u^{m+1})) \\
&= \Delta_1^{l-1}(x_1x_2f' + \frac{1}{l}f'_{l-1}\Delta_1(u^l) + \frac{1}{l}\sum_{m=0}^{l-2} f'_m \Delta_1(u^{m+1})) \\
&= \Delta_1^{l-1}(\sum_{m=0}^{l-1} x_1x_2f'_m u^m + \frac{1}{l}f'_{l-1}\sum_{i=0}^{l-1}\binom{l}{i}u^i(-x_1x_2)^{l-i} \\
&\qquad + \frac{1}{l}\sum_{m=0}^{l-2} f'_m \Delta_1(u^{m+1})) \\
&= \Delta_1^{l-1}(\sum_{m=0}^{l-2} x_1x_2f'_m u^m + \frac{1}{l}f'_{l-1}\sum_{i=0}^{l-2}\binom{l}{i}u^i(-x_1x_2)^{l-i} \\
&\qquad + \frac{1}{l}\sum_{m=0}^{l-2} f'_m \Delta_1(u^{m+1})) \\
&= \Delta_1^{l-1}(\sum_{m=0}^{l-2} h_m u^m)
\end{aligned}$$

where $h_m \in \mathbb{F}[2V_2]^G$ for $m = 1, 2, \ldots, l-2$ and this final expression is equal to zero since, as is easily verified, $\Delta_1^t(u^s) = 0$ whenever $t > s$. Therefore we have $\Delta_1^l(f + uf'/l) = 0$, and so $f + uf'/l \in \oplus_{m=0}^{l-1}\mathbb{F}[2V_2]^G u^m$ by the induction hypothesis. Thus $f \in \oplus_{m=0}^{l}\mathbb{F}[2V_2]^G u^m$ which proves Theorem 2.2.8. □

2.2.3 The Vector Invariants of V_2

Given a representation V of a group G and an integer $m \geq 2$, a ring of invariants $\mathbb{F}[mV]^G$ is called a ring of vector invariants. A theorem providing an explicit description of $\mathbb{F}[mV]^G$for all $m \geq 1$ is called a first fundamental (or main) theorem for V. The following first fundamental theorem for V_2 was conjectured by David

Richman and proved by Campbell and Hughes, see [17]. Their proof is technical and uses a deep result about the rank of zero-one matrices in characteristic p.

Theorem 2.2.10. *Let $G = C_p = \langle\sigma\rangle$ act on $V = mV_2$. Let $\{y_i, x_i\}$ denote a basis for the i^{th} copy of V_2^* in V^* where $\sigma(y_i) = y_i + x_i$ and $\sigma(x_i) = x_i$. Thus $\{x_1, y_1, x_2, y_2, \ldots, x_m, y_m\}$ is an upper triangular basis for V^*. Then the ring of invariants $\mathbb{F}[mV_2]^G$ is generated by the following invariants:*

1. *x_i for $i = 1, 2, \ldots, m$.*
2. *$N^{C_p}(y_i) = y_i^p - x_i^{p-1}y_i$ for $i = 1, 2, \ldots, m$.*
3. *$u_{ij} = x_j y_i - x_i y_j$ for $1 \leq i < j \leq m$.*
4. *$Tr^{C_p}(y_1^{a_1} y_2^{a_2} \ldots y_m^{a_m})$ where $0 \leq a_i < p$ for $i = 1, 2, \ldots, m$.*

Remark 2.2.11. Shank and Wehlau [18] showed that if $a_1 + a_2 + \ldots + a_m \leq 2(p-1)$, then $Tr^{C_p}(y_1^{a_1} y_2^{a_2} \ldots y_m^{a_m})$ lies in the subalgebra generated by $x_1, x_2, \ldots, x_m$ and u_{ij} with $1 \leq i < j \leq m$. Additionally, they also showed that if we exclude invariants of this form, the remaining invariants minimally generate $\mathbb{F}[mV_2]^{C_p}$.

The following example illustrates Theorem 2.2.10.

Example 2.2.12. If we take $m = 3$ and $\mathbb{F}$ a field of characteristic $p = 3$, then Theorem 2.2.10 tells us that $\mathbb{F}[3V_2]^{C_3}$ is generated by $x_1, x_2, x_3, N(y_1), N(y_2), N(y_3), u_{12}, u_{13}, u_{23}$ and some transfers.

It is straightforward to compute

$$\begin{aligned}
Tr^{C_3}(y_i) &= 0 && \text{for } i = 1, 2, 3;\\
Tr^{C_3}(y_i y_j) &= -x_i x_j && \text{for } 1 \leq i, j \leq 3;\\
Tr^{C_3}(y_i^2 y_j) &= x_i u_{ji} && \text{for } 1 \leq i \neq j \leq 3;\\
Tr^{C_3}(y_1 y_2 y_3) &= x_1 u_{23} - x_3 u_{12}; &&\\
Tr^{C_3}(y_i^2 y_j^2) &= -u_{ij} - x_i^2 x_j^2 && \text{for } 1 \leq i < j \leq 3;\\
Tr^{C_3}(y_i y_1 y_2 y_3) &= -u_{ij} u_{ik} - x_i^2 x_j x_k && \text{where } \{i, j, k\} = \{1, 2, 3\}.
\end{aligned}$$

Thus we see that $\mathbb{F}[3V_2]^{C_3}$ is minimally generated by

$x_1, x_2, x_3, N(y_1), N(y_2), N(y_3), u_{12}, u_{13}, u_{23}, Tr^{C_3}(y_1^2y_2^2y_3), Tr^{C_3}(y_1^2y_2y_3^2)$, $Tr^{C_3}(y_1y_2^2y_3^2)$ and $Tr^{C_3}(y_1^2y_2^2y_3^2)$.

2.3 Polarization

We call the ring $\mathbb{F}[mV]^G$ a ring of vector invariants of G where $mV = \oplus^m V$ the coordinate ring with the diagonal action of G.

Consider the map $\phi : mV \to V$ given by $\phi(v_1, v_2, \ldots, v_m) = v_1 + v_2 + \ldots + v_m$. This map is $GL(V)$-equivariant where $GL(V)$ acts diagonally on mV.

This map naturally induces ring map $\phi^* : \mathbb{F}[V] \to \mathbb{F}[mV]$ given by $(\phi^*(f))(v_1, v_2, \ldots, v_m) = f(\phi(v_1, v_2, \ldots, v_m)) = f(v_1 + v_2 + \ldots + v_m)$.

We define the polarization map in terms of the variables as follows.

Let V be an n-dimensional vector space over $\mathbb{F}$, with standard dual basis $\{x_1, \ldots, x_n\}$ and let $\{x_{11}, x_{12}, \ldots, x_{ij}, \ldots, x_{nm}\}$ be the dual basis for mV. We define the polarization map by

$$Pol : \mathbb{F}[V]_d \to \mathbb{F}[mV]_d,\ x_i \mapsto x_{i1} + \ldots + x_{im},$$

in other words we send the ith basis vector to the ith row sum of the matrix $[x_{ij}]_{ij}$. We extend this map additively and multiplicatively and thus obtain a homomorphism of $\mathbb{F}$-algebras.

Let $f \in \mathbb{F}[V]_d$. Using the $\mathbb{N}^m$-grading on $\mathbb{F}[mV]$ we have

$$\phi^*(f) = \sum_{i_1+i_2+\ldots i_m=d} f_{(i_1,i_2,\ldots,i_m)}$$

where each $f_{(i_1,i_2,\ldots,i_m)} \in \mathbb{F}[mV]_{(i_1,i_2,\ldots,i_m)}$. These polynomials $f_{(i_1,i_2,\ldots,i_m)}$ are called *partial polarizations* of f and we write

$$Pol^m(f) = \{f_{(i_1,i_2,\ldots,i_m)} \mid i_1 + i_2 + \ldots i_m = d\}$$

to denote the set of all such partial polarizations.

In order the compute individual polarizations, we take m indeterminates $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$, and consider $\mathbf{v} = (v_1, v_2, \ldots, v_m)$ where each v_i represents a generic element of V. We write $\lambda\mathbf{v} = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_m v_m$, and then we have

$$\begin{aligned} f(\lambda\mathbf{v}) &= f(\phi(\lambda_1 v_1, \lambda_2 v_2, \ldots, \lambda_m v_m)) \\ &= \phi^*(f)(\lambda_1 v_1, \lambda_2 v_2, \ldots, \lambda_m v_m) \\ &= \sum_{i_1+i_2+\ldots i_m=d} \lambda_1^{i_1}\lambda_2^{i_2}\ldots\lambda_m^{i_m} f_{(i_1,i_2,\ldots,i_m)}(v_1, v_2, \ldots, v_m) \\ &= \sum_I \lambda^I f_I(\mathbf{v}) \end{aligned}$$

with $|I| = i_1 + i_2 + \ldots + i_m = d$ where

$$f_I \in \mathbb{F}[mV]_I = \mathbb{F}[V]_{i_1} \otimes \mathbb{F}[V]_{i_2} \otimes \ldots \otimes \mathbb{F}[V]_{i_m} \subset \mathbb{F}[mV]_d.$$

As a special case, we may take $m = d = \deg(f)$ and $(i_1, i_2, \ldots, i_m) = (1, 1, \ldots, 1)$ to get the *full polarization* of f denoted by

$$P(f) = f_{(1,1,\ldots,1)} = f_{\text{multi-linear}} \in \mathbb{F}[dV].$$

Lemma 2.3.1. *The mapping $f \mapsto f_{(i_1,i_2,\ldots,i_m)}$ is GL(V)-equivariant. In particular, if G is any subgroup of $GL(V)$ and $f \in \mathbb{F}[V]^G$, then $Pol^m(f) \subset \mathbb{F}[mV]^G$.*

Proof. Let $\sigma \in GL(V)$. We need to show that $(\sigma f)_I = \sigma(f_I)$. The former is defined by the equation

$$(\sigma f)(\lambda\mathbf{v}) = \sum_I \lambda^I (\sigma f)_I(\mathbf{v}).$$

But

$$(\sigma f)(\lambda\mathbf{v}) = f(\lambda\sigma^{-1}(\mathbf{v})) = \sum_I \lambda^I f_I(\sigma^{-1}(\mathbf{v})).$$

Therefore,

$$(\sigma f)_I(\mathbf{v}) = f_I(\sigma^{-1}(\mathbf{v})) = (\sigma f_I)(\mathbf{v}).$$

In particular, if f is invariant then

$$(\sigma f)_I = f_I = \sigma(f_I)$$

. □

The following example illustrates polarization.

Example 2.3.2. Let $\mathbb{K}$ be a field of any characteristic. Consider the usual three dimensional permutation representation V of Σ_3, the symmetric group on three letters. Let $\{x, y, z\}$ be a permutation basis for V^*. It is well known that if $\mathbb{K}$ has characteristic zero, then $\mathbb{K}[V]^{\Sigma_3}$ is the polynomial ring $\mathbb{K}[s_1, s_2, s_3]$ where $s_1 = x + y + z$, $s_2 = xy + xz + yz$ and $s_3 = xyz$ are elementary symmetric polynomials. This result is also true when $\mathbb{K}$ has positive characteristic, even for characteristic 2 and 3.

Here we consider the ring of vector invariants $\mathbb{K}[2V]^{\Sigma_3}$. Weyl [19] proved that the polarizations of the elementary symmetric functions $f = s_1$, $g = s_2$, $h = s_3$ suffice to generate $\mathbb{K}[2V]^{\Sigma_3}$ if $6 = |\Sigma_3|$ is invertible in $\mathbb{K}$. In fact, he proved that if V is the usual permutation representation of Σ_n, then for any n and any m the polarizations of the elementary symmetric polynomials $s_1, s_2, \ldots, s_n$ generate the ring $\mathbb{K}[mV]^{\Sigma_n}$ provided only that $n!$ is invertible in $\mathbb{K}$. Here we have

$$\begin{aligned}\sum \lambda^I f_I &= f(\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2, \lambda_1 z_1 + \lambda_2 z_2) \\ &= \lambda_1(x_1 + y_1 + z_1) + \lambda_2(x_2 + y_2 + z_2).\end{aligned}$$

Thus $Pol^2(f) = \{f_{10}, f_{01}\}$ where

$$f_{10} = x_1 + y_1 + z_1,$$

$$f_{01} = x_2 + y_2 + z_2.$$

Similarly,

$$\begin{aligned}\sum \lambda^I g_I &= g(\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2, \lambda_1 z_1 + \lambda_2 z_2) \\ &= \lambda_1^2(x_1 y_1 + x_1 z_1 + y_1 z_1) \\ &\quad + \lambda_1\lambda_2(x_1 y_2 + x_1 z_2 + y_1 x_2 + y_1 z_2 + z_1 x_2 + z_1 y_2) \\ &\quad + \lambda_2^2(x_2 y_2 + x_2 z_2 + y_2 z_2).\end{aligned}$$

Thus $Pol^2(g) = \{g_{20}, g_{11}, g_{02}\}$ where

$$\begin{aligned}g_{20} &= x_1 y_1 + x_1 z_1 + y_1 z_1, \\ g_{11} &= x_1 y_2 + x_1 z_2 + y_1 x_2 + y_1 z_2 + z_1 x_2 + z_1 y_2, \\ g_{02} &= x_2 y_2 + x_2 z_2 + y_2 z_2.\end{aligned}$$

Here g_{11} is the full polarization $P(g)$. Finally,

$$\begin{aligned}\sum \lambda^I h_I &= h(\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2, \lambda_1 z_1 + \lambda_2 z_2) \\ &= \lambda_1^3(x_1 y_1 z_1) + \lambda_1^2\lambda_2(x_1 y_1 z_2 + x_1 y_2 z_1 + x_2 y_1 z_1) \\ &\quad + \lambda_1\lambda_2^2(x_1 y_2 z_2 + x_2 y_1 z_2 + x_2 y_2 z_1) + \lambda_2^3 x_2 y_2 z_2.\end{aligned}$$

Hence $Pol^2(h) = \{h_{30}, h_{21}, h_{12}, h_{03}\}$ where

$$\begin{aligned}h_{30} &= x_1 y_1 z_1, \\ h_{21} &= x_1 y_1 z_2 + x_1 y_2 z_1 + x_2 y_1 z_1, \\ h_{12} &= x_1 y_2 z_2 + x_2 y_1 z_2 + x_2 y_2 z_1, \\ h_{03} &= x_2 y_2 z_2.\end{aligned}$$

Weyl's result tells us that if the characteristic of $\mathbb{K}$ is neither 2 nor 3, then $\mathbb{K}[2V]^{\Sigma_3}$ is generated by the nine invariants

$$f_{10}, f_{01}, g_{20}, g_{11}, g_{02}, h_{30}, h_{21}, h_{12}, h_{03}.$$

It turns out that these nine invariants also generate $\mathbb{K}[2V]^{\Sigma_3}$ if $\mathbb{K}$ has characteristic 2. The identity

$$\begin{aligned}3(x_1 y_1 z_2^2 + y_1 z_1 x_2^2 + x_1 z_1 y_2^2) = f_{10}^2 g_{02} - f_{10} f_{01} g_{11} + f_{10} h_{12} + g_{11}^2 \\ - 2 f_{10} h_{12} + f_{01}^2 g_{11} - 4 g_{20} g_{02} + 2 f_{01} h_{21}\end{aligned}$$

shows how to express the invariant $k := x_1 y_1 z_2^2 + y_1 z_1 x_2^2 + x_1 z_1 y_2^2$ in terms of the polarized elementary symmetric functions when 3 is invertible. However, over a field of characteristic 3, this identity expresses an algebraic relation among the polarized elementary symmetric functions. In fact, over a field of characteristic 3, it is not possible to express k as a polynomial in the nine polarized elementary symmetric functions, and it turns out that the nine polarized elementary symmetric functions together with the invariant k form a minimal generating set for $\mathbb{K}[2V]^{\Sigma_3}$ when $\mathbb{K}$ has characteristic 3.

Chapter 3

Localized Invariant Rings of p-Groups

In this chapter, we study an algorithm due to Chuai and Campbell [10] that computes the invariants of a modular p-group up to a localization.

Let $\mathbb{F}(V)^G$ denote the quotient field of $\mathbb{F}[V]^G$. It is easy to see that $\mathbb{F}(V)^G$ is also the G-invariant subfield of the quotient field $\mathbb{F}(V)$. It is a famous question of Noether's whether or not $\mathbb{F}(V)^G$ is purely transcendental. The answer to this question is negative in general. However, if $p > 0$ and G is a p-group, then $\mathbb{F}(V)^G$ is purely transcendental [20].

If R denotes a commutative ring and $b \in R$, we denote by $R_{(b)}$ the localization of R at the multiplicative set $\{1, b, b^2, \ldots\}$. In this chapter, we show that, for G a p-group, a minimal generating set for $\mathbb{F}(V)^G$ can be taken as homogeneous invariants from the invariant ring. If $\{a_1, \ldots, a_n\}$ is such a set,we show that there exists an element $b \in \mathbb{F}[a_1, \ldots, a_n]$, such that $\mathbb{F}[V]^G_{(b)} = \mathbb{F}[a_1, \ldots, a_n]_{(b)}$. This generalizes the result of [21], which examines the case $G = C_p$, the cyclic group of order p, and V is an arbitrary representation of C_p.

3.1 General Algorithm

Consider a representation V of a p-group G over a field $\mathbb{F}$ of characteristic $p > 0$. We may assume that G is a subgroup of the upper triangular group $U(V) = U_n(\mathbb{F})$: any p-subgroup of $GL(V)$ is triangularizable.

Consequently, we can choose a basis $\{x_1, \ldots, x_n\}$ for V^* such that $(\sigma - 1)x_i$ is in the span of $\{x_1, \ldots, x_{i-1}\}$ for all $\sigma \in G$ and for all $i = 1, \ldots, n$. In particular, we note that x_1 is invariant. We set $R[m] = \mathbb{F}[x_1, \ldots, x_m]$ for $0 \leq m \leq n$ subject to the convention that $R[0] = \mathbb{F}$. Then G acts on $R[m]$. For any non-zero $f \in R[m]$, we may express f as a polynomial in x_m and write

$$f = f_0 + f_1 x_m + \ldots + f_d {x_m}^d$$

with $f_i \in R[m-1]$ for all $i = 0, 1, \ldots, d$ where $f_d \neq 0$ and we set $\deg_{x_m}(f) = \deg_m(f) = d$. We denote the leading coefficient $f_d \in R[m-1]$ of f by $c(f)$. Writing $\sigma(x_m) = x_m + \alpha_{m-1}x_{m-1} + \ldots + \alpha_1 x_1$, we have $\alpha(f) = \sum_{i=0}^{d} \sigma(f_i)(x_m + \alpha_{m-1}x_{m-1} + \ldots + \alpha_1 x_1)^i$. Therefore, $\sigma(c(f)) = c(\sigma f)$ for all $\sigma \in G$. In particular, if f is invariant, so is $c(f)$ since $\sigma(c(f)) = c(\sigma f) = c(f)$.

For each m with $1 \leq m \leq n$, let $\phi_m \in R[m]^G$ denote a fixed homogeneous invariant with the smallest positive degree in x_m among all invariants in $R[m]^G$. The existence of ϕ_m follows from the fact that the set $R[m]^G \backslash R[m-1]$ is non-empty since $N(x_m) := \prod_{\sigma \in G} \sigma(x_m) = x_m^{|G|} + \{\text{terms of lower degree in } x_m\}$ lies in it. We take $\phi_1 = x_1$. The invariants $c_m = c(\phi_m) \in R[m-1]$ will play a special role.

Finally, note that we can make no claim as to the total degree of ϕ_m, in particular, we cannot claim that the total degree of ϕ_m is less than or equal to $|G|$ for all m.

We first prove two lemmas.

Lemma 3.1.1. *For any $f \in R[m]^G$, there exists an integer $k \geq 0$ such that $c_m^k f \in R[m-1]^G[\phi_m]$.*

Proof. We use induction on $\deg_{x_m}(f)$. When $\deg_{x_m}(f) = 0$, there is nothing to prove. So we may assume $\deg_{x_m}(f) = d > 0$.

In the ring $R[m]_{(c_m)}$, the localization of $R[m]$ at the multiplicative set $\{1, c_m, c_m^2, \ldots\}$, the element ϕ_m/c_m is monic as a polynomial in x_m. Hence we may divide f by ϕ_m/c_m in order to obtain $f = q'(\phi_m/c_m) + r'$ where $q', r' \in R[m]_{(c_m)}$ with $\deg_{x_m}(r') < \deg_{x_m}(\phi_m)$. Thus

$$f = \sigma(f) = \sigma(q')(\phi_m/c_m) + \sigma(r') = q'(\phi_m/c_m) + r'$$

for all $\sigma \in G$. Since

$$\deg_{x_m}(\sigma(r')) = \deg_{x_m}(r') < \deg_{x_m}(\phi_m),$$

we see by the uniqueness of remainders that $r' = \sigma(r')$ and hence $q' = \sigma(q')$ for all $\sigma \in G$. Therefore $q', r' \in R[m]^G_{(c_m)}$. Multiplying by a suitable power of c_m, we see that there exists an integer $s \geq 0$ and polynomials $q = c_m^{s-1}q', r = c_m^s r' \in R[m]^G$ such that $c_m^s f = q\phi_m + r$ where $\deg_{x_m}(r) = \deg_{x_m}(r') < \deg_{x_m}(\phi_m)$. Therefore, $r \in R[m-1]^G$ because ϕ_m has the least positive degree in x_m inside $R[m]^G$. Since $\deg_{x_m}(q) = \deg_{x_m}(f) - \deg_{x_m}(\phi_m)$, by the induction hypothesis, $c_m^t q \in R[m-1]^G[\phi_m]$ for some $t \geq 0$. Therefore, for $k = s + t$ we have $c_m^k f \in R[m-1]^G[\phi_m]$, as required. □

We note that it follows immediately from Lemma 3.1.1 that if $c_m = 1$ for all m, then any $f \in R[m]^G$ lies in $\mathbb{F}[\phi_1, \ldots, \phi_m]$ as easily seen by induction on m. So we have the following.

Corollary 3.1.2. *If $c_m = 1$ for all $m = 1, 2, \ldots, n$, then*

$$\mathbb{F}[V]^G = \mathbb{F}[\phi_1, \ldots, \phi_m]$$

is a polynomial ring.

Lemma 3.1.3. *For any finite number of invariants $h_1, \ldots, h_t \in R[m]^G$, there exists a monomial $c = c_1^{k_1} \ldots c_m^{k_m}$ in $c_1, \ldots, c_m$, such that $ch_i \in \mathbb{F}[\phi_1, \ldots, \phi_m]$ for all $i = 1, 2, \ldots, t$.*

Proof. We use induction on m. First let $m = 1$. Since $\phi_1 = x_1$ and $c_1 = 1$, the lemma follows from the previous corollary. Now assume $m > 1$. By Lemma 3.1.1, there exists an integer $s \geq 0$ such that $c_m^s h_i \in R[m-1]^G[\phi_m]$ for all i. Let $c_m^s h_i = \sum_j a_{ji}\phi_m^j$, where $a_{ji} \in R[m-1]^G$. Now, since the finite set $\{a_{ji}\} \subset R[m-1]^G$, by the induction hypothesis, there exist $k_1, \ldots, k_{m-1} \geq 0$ such that $c_1^{k_1} \ldots c_{m-1}^{k_{m-1}} a_{ji} \in \mathbb{F}[\phi_1, \ldots, \phi_{m-1}]$ for all i and j. Hence, for $c = c_1^{k_1} \ldots c_{m-1}^{k_{m-1}} c_m^s$, we have that $ch_i \in \mathbb{F}[\phi_1, \ldots, \phi_m]$ for all $i = 1, 2, \ldots, t$, as required. □

The following theorem shows that for a p-group, the invariant field is purely transcendental.

Theorem 3.1.4. *Let $G \subseteq U(V) \subset GL(V)$ be a p-group. Choose any set of homogeneous invariants $\phi_1, \ldots, \phi_n$ with the property that $\phi_m \in R[m]^G$ is of smallest positive degree in x_m for $1 \leq m \leq n$. Then $\mathbb{F}(V)^G = \mathbb{F}(\phi_1, \ldots, \phi_n)$. Furthermore, there exists a non-zero $f \in \mathbb{F}[\phi_1, \ldots, \phi_n]$ such that $\mathbb{F}[V]^G_{(f)} = \mathbb{F}[\phi_1, \ldots, \phi_n]_{(f)}$.*

Proof. We use the above notation. For the first part of the theorem, we need only to show that any $h \in \mathbb{F}[V]^G$ lies in $\mathbb{F}(\phi_1, \ldots, \phi_n)$. (Since $\mathbb{F}(V)^G = \{\frac{f_i}{g_i} \mid f_i, g_i \in \mathbb{F}[V]^G\}$, if f_i and g_i lies in $\mathbb{F}(\phi_1, \ldots, \phi_n)$ then $\frac{f_i}{g_i}$ does too). Assume $h \in R[m]^G \backslash R[m-1]$. By Lemma 3.1.1, there exists an integer $s \geq 0$ such that $c_m^s h \in R[m-1]^G[\phi_m]$. We write $c_m^s h = \sum_k a_k \phi_m^k$, where $a_k \in R[m-1]^G$. By Lemma 3.1.3, there exists some monomial $c^K = c_1^{k_1} \ldots c_{m-1}^{k_{m-1}}$ with $c^K \cdot c_m^s \in \mathbb{F}[\phi_1, \ldots, \phi_{m-1}]$ ($c_m \in R[m-1]^G$) and $c^K \cdot a_k \in \mathbb{F}[\phi_1, \ldots, \phi_{m-1}]$ for all k. Thus, $h \in \mathbb{F}(\phi_1, \ldots, \phi_m) \subseteq \mathbb{F}(\phi_1, \ldots, \phi_n)$.

For the proof of the second part, let $\mathbb{F}[V]^G = \mathbb{F}[a_1, \ldots, a_l]$. Since $\mathbb{F}[V]^G \subseteq \mathbb{F}(\phi_1, \ldots, \phi_n)$ ($\mathbb{F}[V]^G \hookrightarrow \mathbb{F}(V)^G = \mathbb{F}(\phi_1, \ldots, \phi_n)$), we can write every a_i as h_i/k_i where $h_i, k_i \in \mathbb{F}[\phi_1, \ldots, \phi_n]$. Multiplying with suitable polynomials in $\mathbb{F}[\phi_1, \ldots, \phi_n]$ we can write common denominator instead of k_i's. Thus we can write $a_i = h_i/f$, where $h_i, f \in \mathbb{F}[\phi_1, \ldots, \phi_n]$. Then

$$\mathbb{F}[V]^G = \mathbb{F}[\frac{h_1}{f}, \ldots, \frac{h_l}{f}] \subseteq \mathbb{F}[\phi_1, \ldots, \phi_n]_{(f)}.$$

Therefore, we have $\mathbb{F}[V]^G \subseteq \mathbb{F}[\phi_1, \ldots, \phi_n]_{(f)}$ and so $\mathbb{F}[V]^G_{(f)} \subseteq \mathbb{F}[\phi_1, \ldots, \phi_n]_{(f)}$ as required.

The inverse is clear. Since $\mathbb{F}[\phi_1, \ldots, \phi_n] \subseteq \mathbb{F}[V]^G$ we also have $\mathbb{F}[\phi_1, \ldots, \phi_n]_{(f)} \subseteq \mathbb{F}[V]^G_{(f)}$. □

3.2 Cyclic Group of Order p

We denote by C_p the cyclic group of order p with generator σ. There are p non-isomorphic indecomposable representations of C_p in characteristic p; one indecomposable representation, V_r, of dimension r for $1 \leq r \leq p$. And for the dual space $V_r^* = \hom_{\mathbb{F}}(V_r, \mathbb{F})$, there is a basis $\{x_1, \ldots, x_r\}$ with the property that $\sigma(x_i) = x_i + x_{i-1}$, setting $x_0 = 0$. Therefore, the matrix of σ with respect to this basis is

$$\sigma = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & \ddots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

Of course, any representation of V can be written as $k_1V_1 \oplus \ldots \oplus k_pV_p$, and if we choose a basis for V^*

$$\{x_{i,j,r} \mid 1 \leq i \leq r,\ 1 \leq j \leq k_r,\ 1 \leq r \leq p\}$$

with the property that $\sigma(x_{i,j,r}) = x_{i,j,r} + x_{i-1,j,r}$, subject to the convention that $x_{0,j,r} = 0$, then we can identify $\mathbb{F}[V]$ with the polynomial algebra

$$\mathbb{F}[x_{i,j,r} \mid 1 \leq i \leq r,\ 1 \leq j \leq k_r,\ 1 \leq r \leq p].$$

Let us denote by $\mathbb{F}[V]_d$ the vector space spanned by the homogeneous polynomials of degree$d$ and note $\mathbb{F}[V] = \oplus_{d=0}\mathbb{F}[V]_d$. We have $\mathbb{F}[V]_0 = \mathbb{F}$ and $\mathbb{F}[V]_1 = V^*$, and each element σ^i of C_p acts as a degree-preserving algebra automorphism of $\mathbb{F}[V]$.

We note that

$$\mathbb{F}[V]^{C_p} = \mathbb{F}[V_1] \otimes \mathbb{F}[V']^{C_p},$$

where

$$V' = (k_1 - 1)V_1 \oplus k_2V_2 \ldots \oplus k_pV_p,$$

and so we may as well assume $k_1 = 0$, that is, the representation V is reduced.

3.2.1 Construction of Invariants

Given any element $f \in \mathbb{F}[V]$, we know that the trace of f, $Tr(f) = \sum_{i=0}^{p-1} \sigma^i(f)$, and the norm of f, $N(f) = \prod_{i=0}^{p-1} \sigma^i(f)$, are invariant. For example, in $\mathbb{F}[V_2]$, straightforward calculations show that $N(x_2) = x_2^p - x_1^{p-1}x_2$ and $Tr(x_2^i) = 0$ if $1 \leq i < p-1$ with $Tr(x_2^{p-1}) = -x_1^{p-1}$. We note that $N(x_2)$ has degree p in x_2 and since $\mathbb{F}[V_2]^{C_p} = \mathbb{F}[x_1, N(x_2)]$, we may choose $N(x_2)$ as ϕ_2 in the notation of section 3.1.

Invariants in $\mathbb{F}[V]^{C_p}$ such as

$$s_2 = x_2^2 - x_1x_2 - 2x_1x_3$$

are invariant for all primes p. Invariants with this property are called rational invariants.

Shank [3] proposed an algorithm which constructs rational invariants with given (allowable) lead terms, for example, x_2^{m-1}:

$$s_2 = x_2^2 - x_1x_2 + x_1(-2x_3),$$
$$s_3 = x_2^2(x_2) + x_1x_2(-3x_3) + x_1^2(-x_2 + 3x_4),$$
$$s_4 = x_2^3(x_2) + x_1x_2^2(-4x_3) + x_1^2x_2(2x_3 - 6x_4) + x_1^3(-x_2 - 2x_3 - 6x_4 - 8x_5).$$

In general [21, 3], using the graded reverse lexicographic monomial order with $x_m < x_{m+1}$, there is a rational invariant s_{m-1} with lead term x_2^{m-1} and with a term $(-1)^m(m-1)(m-3)!x_1^{m-2}x_m$, and no terms involving x_i for $i > m$. We note that $(m-1)(m-3)!$ is non-zero and hence invertible in $\mathbb{F}$. Then in terms of the analysis of section 3.1, we may choose $\phi_m = s_{m-1}$.

In the event, V has more than one non-trivial summand, say

$$V_i \oplus V_j \subset V$$

with $i, j > 1$, we need a particular kind of rational invariant, the two-dimensional determinant invariants. Denote the basis for V_i^* by $\{x_1, x_2, \ldots, x_i\}$ and for V_j^* by $\{y_1, y_2, \ldots, y_j\}$. Then $u = u_{V_i,V_j} = x_1y_2 - x_2y_1$ is invariant, and there is such an invariant for every pair of non-trivial summands in the indecomposable decomposition of V. We note that u has degree 1 in y_2.

There is one more family of invariants that are needed, again associated to a representation with more than one non-trivial summand, say $V_i \oplus V_j \subset V$, with bases as above and $i \leq j$. Suppose $f = f(x_1, \ldots, x_i) \in \mathbb{F}[V_i]^{C_p}$ and consider the ring $\mathbb{F}[V][t]$ with C_p action given as usual on $\mathbb{F}[V]$ and $\sigma(t) = t$. Now note that

$$f(x_1 + ty_1, \ldots, x_i + ty_i) \in \mathbb{F}[V][t]^{C_p}$$

is invariant, since $\sigma(x_k + ty_k) = (x_k + ty_k) + (x_{k-1} + ty_{k-1})$. But

$$f(x_1 + ty_1, \ldots, x_i + ty_i) = \sum_{k \geq 0} f_k(x_1, \ldots, x_i, y_1, \ldots, y_i)t^k,$$

from which it follows that $f_k = f_k(x_1, \ldots, x_i, y_1, \ldots, y_i)$ is invariant. This process of constructing new invariants with 'mixed' variables from existing invariants is called polarization, as we see in 2.3. We are interested only in applying this construction to the Shank invariants, and we want only the coefficient of t. This is the function f_1 which has degree 1 in the y's. In the three examples above, these are

$$\begin{aligned}
(s_{2,i,j})_1 &= x_2y_1 + 2x_2y_2 - 2x_3y_1 + x_1(-y_2 - 2y_3),\\
(s_{3,i,j})_1 &= 6x_4x_1y_1 - 3x_3x_2y_1 - 3x_3x_1y_2 + 3x_2^2y_2 - 3x_2x_1y_3 - 2x_2x_1y_1 + x_1^2(-y_2 + 3y_4),\\
(s_{4,i,j})_1 &= -24x_5x_1^2y_1 + 16x_4x_2x_1y_1 + 8x_4x_1^2y_2 - 18x_4x_1^2y_1 - 4x_3x_2^2y_1 - 8x_3x_2x_1y_2\\
&\quad + 4x_3x_2x_1y_1 + 2x_3x_1^2y_2 - 6x_3x_1^2y_1 + 4x_2^3y_2 - 4x_2^2x_1y_3\\
&\quad + 8x_2x_1^2y_4 + 2x_2x_1^2y_3 - 3x_2x_1^2y_1 - x_1^3(-y_2 - 2y_3 - 6y_4 + 8y_5).
\end{aligned}$$

Note that $s_{k,i,j}$ is defined for $k \leq \min(i, j)$. Again, we note that the coefficient of $x_1^{m-2}y_m$ in $(s_{m-1,i,j})_1$ is invertible in $\mathbb{F}$.

3.2.2 Localized Invariants of Indecomposable Representations of C_p

We can compute generators for certain localized rings of C_p-invariants as follows. First, let us consider the case $V = V_n$, and identify $\mathbb{F}[V_n]$ with $\mathbb{F}[x_1, x_2, \ldots, x_n]$ such that $\sigma(x_i) = x_i + x_{i-1}$, with $x_0 = 0$. We use Shank polynomials

$$s_{m-1} = x_2^{m-1} + \ldots + \alpha x_1^{m-2} x_m,$$

for α non-zero in $\mathbb{F}$. Recall that $\alpha = (-1)^m(m-1)(m-3)!$. As discussed in section 3.1, we note that we may choose $\phi_1 = x_1$, $\phi_2 = N(x_2)$ and $\phi_m = s_{m-1}$ for $m \geq 3$ because each of these polynomials ϕ_m has degree 1 in x_m. Further, we note that for all m, c_m is a power of x_1.

Theorem 3.2.1. *Let V_n denote an indecomposable representation of C_p, and let ϕ_m be chosen as above and write $x_1 = x$. Then*

$$\mathbb{F}(V_n)^{C_p} = \mathbb{F}(\phi_1, \ldots, \phi_n).$$

Furthermore,

$$\mathbb{F}[V_n]_{(x)}^{C_p} = \mathbb{F}[\phi_1, \ldots, \phi_n]_{(x)}.$$

3.2.3 Localized C_p-invariants in general

We have that any representation of V can be written as $k_1V_1 \oplus \ldots \oplus k_pV_p$ and that we may assume $k_1 = 0$ as we see in 3.2.

We choose the largest m for which $k_m > 0$ and fix a particular copy $V_{l,m}$ of V_m. Let $\{x_1, x_2, \ldots, x_m\}$ denote the usual basis for $V_{l,m}^*$. Set $x = x_{1,l,m}$ and $x_2 = x_{2,l,m}$. Note that $\sigma(x) = x$ and $\sigma(x_2) = x_2 + x$.

For each other distinct non-trivial summand, say the jth copy of V_r, we have $r \leq m$, and we choose the usual basis $\{x_{1,j,r}, \ldots, x_{r,j,r}\}$ for $V_{j,r}^*$, that is, we have $\sigma(x_{i,j,r}) = x_{i,j,r} + x_{i-1,j,r}$ with $x_0 = 0$.

We consider the polarized Shank invariants $(s_{i-1,r,m})_1$ for $3 \leq i \leq r$, each of which has a term $x^{i-2}x_{i,j,r}$, which occurs with non-zero coefficient in $\mathbb{F}$. That is, each of these invariants has degree 1 in $x_{i,j,r}$ for $3 \leq i \leq r$.

We also consider the determinant invariant

$$u_{r,m,j} = xx_{2,j,r} - x_2x_{1,j,r}$$

of degree 1 in $x_{2,j,r}$.

Therefore, we may choose $\phi_{1,j,r} = x_{1,j,r}$, $\phi_{2,j,r} = u_{r,m,j}$ and $\phi_{i,j,r} = (s_{i-1,r,m})_1$ for $3 \leq i \leq r$ and we obtain Theorem 3.2.2.

Theorem 3.2.2. *Let $V = k_2V_2 \oplus \ldots \oplus k_mV_m$ be any reduced representation of C_p, where $m \leq p$ and $k_m > 0$. Choose a basis $\{x_{i,j,r}\}$ for the jth copy of V_r, and identify $\mathbb{F}[V]$ with $\mathbb{F}[x_{i,j,r} \mid 1 \leq i \leq r, 1 \leq j \leq k_r, 2 \leq r \leq m]$. Fix a choice $x = x_{1,l,m}$ and $x_2 = x_{2,l,m}$ for some l and choose $\phi_{i,j,r}$ as above. Then*

$$\mathbb{F}(V)^{C_p} = \mathbb{F}(\phi_{i,j,r} \mid 1 \leq i \leq r, 1 \leq j \leq k_r, 2 \leq r \leq m),$$

and

$$\mathbb{F}[V]^{C_p}_{(x)} = \mathbb{F}[\phi_{i,j,r} \mid 1 \leq i \leq r, 1 \leq j \leq k_r, 2 \leq r \leq m]_{(x)}.$$

Bibliography

[1] P. Fleischmann, "The Noether bound in invariant theory of finite groups," *Adv. Math.*, vol. 156, no. 1, pp. 23–32, 2000.

[2] J. Fogarty, "On Noether's bound for polynomial invariants of a finite group," *Electron. Res. Announc. Amer. Math. Soc.*, vol. 7, pp. 5–7, 2001.

[3] R. J. Shank, "S.A.G.B.I. bases for rings of formal modular semiinvariants [semi-invariants]," *Comment. Math. Helv.*, vol. 73, pp. 548–565, 1998.

[4] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau, "Vector invariants for the two-dimensional modular representation of a cyclic group of prime order," *Adv. Math.*, vol. 225, no. 2, pp. 1069–1094, 2010.

[5] M. D. Neusel, "Degree bounds-an invitation to postmodern invariant theory," *Topology Appl.*, vol. 154, no. 4, pp. 792–814, 2007.

[6] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock, "The Noether numbers for cyclic groups of prime order," *Adv. Math.*, vol. 207, no. 1, pp. 149–155, 2006.

[7] H. E. A. Campbell, B. Fodden, and D. L. Wehlau, "Invariants of the diagonal C_p action on V_3," *J. Algebra*, vol. 303, no. 2, pp. 501–513, 2006.

[8] R. J. Shank and D. L. Wehlau, "Computing modular invariants of p-groups," *J.Symbolic Comput.*, vol. 34, no. 5, pp. 307–327, 2002.

[9] R. J. Shank and D. L. Wehlau, "Noether numbers for subrepresentations of cyclic groups of prime order," *Bull. London Math. Soc.*, vol. 34, no. 4, pp. 438–450, 2002.

[10] H. E. A. Campbell and J. Chuai, "Invariant fields and localized invariant rings of p-groups," *Quart. J. Math.*, vol. 34, pp. 151–157, 2007.

[11] H. E. A. Campbell and D. L. Wehlau, *Modular Invariant Theory*. Encyclopaedia of Mathematical Sciences, 139. Springer-Verlag, Berlin., 2011.

[12] D. J. Benson, *Modular Invariant Theory*. London Mathematical Society Lecture Note Series, 190. Cambridge University Press, Cambridge, 1993.

[13] H. Derksen and G. Kemper, *Computational invariant theory*. Encyclopaedia of Mathematical Sciences, 130. Springer-Verlag, Berlin., 2002.

[14] M. D. Neusel, *Invariant theory*. Student Mathematical Library, 36. American Mathematical Society, Providence, RI., 2007.

[15] M. D. Neusel and L. Smith, *Invariant theory of finite groups*. Mathematical Surveys and Monographs, 94. American Mathematical Society, Providence, RI., 2002.

[16] L. Smith, "Polynomial invariants of finite groups. a survey of recent developments," *Bull. Amer. Math. Soc. (N.S.)*, vol. 34, no. 3, pp. 211–250, 1997.

[17] H. E. A. Campbell and I. P. Hughes, "Vector invariants of $u_2(\mathbb{F}_p)$: a proof of a conjecture of Richman," *Adv. Math.*, vol. 126, no. 1, pp. 1–20, 1997.

[18] R. J. Shank and D. L. Wehlau, "Computing modular invariants of p-groups," *J. Symbolic Comput.*, vol. 34, no. 5, pp. 307–327, 2002.

[19] H. Weyl, *The Classical Groups*. Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1997.

[20] T. Miyata, "Invariants of certain groups," *Nagoya Math. J.*, vol. 41, pp. 69–73, 1971.

[21] H. E. A. Campbell, "Rings of invariants of representations of c_p in characteristic p," *Verahmihir J. Math. Sci.*, vol. 6, no. 2, pp. 181–198, 2006.