GENERALIZED INVARIANTS AND HILBERT IDEAL IN MODULAR INVARIANT THEORY

DENİZ ERDEMİRCİ ERKUŞ

AUGUST 2015

GENERALIZED INVARIANTS AND HILBERT IDEAL IN MODULAR INVARIANT THEORY

A DISSERTATION SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL
AND APPLIED SCIENCES OF
IZMIR UNIVERSITY OF ECONOMICS

BY

DENİZ ERDEMİRCİ ERKUŞ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY
IN THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

AUGUST 2015

Ph.D. DISSERTATION EXAMINATION RESULT FORM

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Murat Aşkar
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Ünal Ufuktepe
Head of Department

We have read the dissertation entitled **"Generalized Invariants and Hilbert Ideal in Modular Invariant Theory"** completed by **DENİZ ERDEMİRCİ ERKUŞ** under supervision of **Asst. Prof. Dr. Uğur Madran** and we certify that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Asst. Prof. Dr. Uğur Madran
Supervisor

Examining Committee Members **Date:**

Asst. Prof. Dr. Uğur Madran
Dept. of Mathematics, İUE

Asst. Prof. Dr. Murat Altunbulak
Dept. of Mathematics,
Dokuz Eylül University

Assoc. Prof. Dr. Olcay Coşkun
Dept. of Mathematics,
Boğaziçi University

Asst. Prof. Dr. Aslı Güldürdek
Dept. of Mathematics, İUE

Assoc. Prof. Dr. Engin Mermut
Dept. of Mathematics,
Dokuz Eylül University

ABSTRACT

GENERALIZED INVARIANTS AND HILBERT IDEAL IN MODULAR INVARIANT THEORY

DENİZ ERDEMİRCİ ERKUŞ
Ph.D. in Applied Mathematics and Statistics
Graduate School of Natural and Applied Sciences
Supervisor: Asst. Prof. Dr. Uğur Madran
August 2015

The Hilbert ideal is the ideal of the polynomial ring generated by positive-degree invariants. It has been conjectured that the Hilbert ideal is generated by polynomial invariants of degree at most the group order, which is known as the Hilbert ideal conjecture.

In this thesis, we mainly consider two problems. In the first problem, we prove that the conjecture holds for a modular indecomposable representation of a cyclic group in a restricted dimension giving two approaches for the open problem.

The other study of this thesis is about generalized invariants. We introduce the definition of generalized invariants to arbitrary finite group as a new view for modular invariant theory, in which the characteristic of ground field divides the group order. Further, we determine explicitly the structural properties of generalized invariants of a cyclic group for lower dimensional indecomposable representations. Moreover, we show an analogy of Hilbert ideal conjecture for generalized invariants of these representations. As one of the main results, we give a structural theorem for generalized invariant module of any finite group. Finally, we determine the condition under which generalized invariants coincide with usual invariants.

Keywords: Modular invariant theory, polynomial invariants, Noether number, Hilbert ideal, generalized invariants.

ÖZ

MODÜLER DEĞİŞMEZ TEORİSİNDE GENELLEŞTİRİLMİŞ DEĞİŞMEZLER VE HİLBERT İDEALİ

DENİZ ERDEMİRCİ ERKUŞ
Uygulamalı Matematik ve İstatistik, Doktora
Fen Bilimleri Enstitüsü
Tez Danışmanı: Yrd. Doç. Dr. Madran
Ağustos 2015

Hilbert ideali, pozitif dereceli değişmezler ile üretilen polinom halkasının bir idealidir. Hilbert idealinin derecesi en fazla grubun mertebesi olan değişmezler ile üretilebileceği iddia edilmiştir, ve bu varsayım Hilbert ideali sanısı olarak bilinmektedir.

Bu tezde başlıca iki problemden bahsedilecektir. Birinci problemde devirli bir grubun kısıtlanmış bir boyutta verilen modüler, parçalanamaz temsilleri için Hilbert ideali sanısını iki farklı yaklaşım kullanarak kanıtlayacağız.

Bu tezdeki diğer bir çalışma genelleştirilmiş değişmezler üzerinedir. Cismin karakteristiği grubun mertebesini böldüğü durumla tanımlanan modüler değişmez teorisine yeni bir bakış olarak herhangi bir sonlu grup için genelleştirilmiş değişmezleri tanıtacağız. Daha sonra, devirli grubun küçük boyutlu parçalanamaz temsilleri için genelleştirilmiş değişmezlerin yapısal özelliklerini açık bir şekilde göstereceğiz. Ayrıca Hilbert ideali sanısının bir analojisini devirli grubun genelleştirilmiş değişmezleri için kanıtlayacağız. Ana sonuçlardan biri olarak bir sonlu grubun genelleştirilmiş değişmez modülü için yapısal teoremini vereceğiz. Son olarak, genelleştirilmiş değişmezlerin hangi koşulda alışılmış değişmezlere karşılık geldiğini göstereceğiz.

Anahtar Kelimeler: Modüler değişmez teorisi, polinom değişmezleri, Noether sayısı, Hilbert ideali, genelleştirilmiş değişmezler.

ACKNOWLEDGEMENT

I would like to begin with expressing my deepest gratitude to my supervisor Uğur Madran for accepting me to work together, supporting me in every way, his guidance and instructive comments.

I would like to thank to Engin Mermut for endearing Abstract Algebra in my undergraduate years, making insistently an excellent effort for us and his helps whenever I need.

I want to express my special thanks to Fatma Altunbulak Aksu for encouraging me to make my dreams come true, for her endless support, optimism and friendship. I am so glad I meet you.

I would like to thank to Professors Altunbulak, Coşkun, Güldürdek, Madran, Mermut in my examining committee for their time and comments.

This research is made possible by support of TÜBİTAK with the scholarship "2211-Yurtiçi Doktara Burs Programı" and with TÜBİTAK project entitled *The Structural Properties of Generalized Invariant Module and the Relation with Invariant Ring* of number 114F059.

Finally, I would like to thank to my parents, my sister and my husband Soner for their supports unconditionally and love, and to my baby cheering and filling with hope my life.

To my baby...

TABLE OF CONTENTS

Chapter 1

Introduction

In order to classify mathematical objects with respect to some property, the construction of invariants is required. Invariant theory is concerned with a special situation of this classification problem. It primarily benefits from representation theory. Representation theory may be considered in two cases. Let V be an n-dimensional representation of a finite group G over a field $\mathbb{F}$. In the first case, the representation V is called *non-modular* if the characteristic of the field $\mathbb{F}$ does not divide the group order $|G|$ (or equivalently, $|G|$ is invertible in $\mathbb{F}$); otherwise, it is said to be a *modular representation* as the second case. It can be asserted that non-modular representations are more understandable than the others. Indeed, the representations in non-modular case can be classified by decomposing completely into irreducible pieces due to Maschke's theorem. However, this theorem fails in the modular case. Because of this, many unsolved and interesting problems occur in modular invariant theory. In this thesis, we will discuss modular representations. For a prime p dividing $|G|$, the ground field $\mathbb{F}$ will have the characteristic p.

Invariant theory is generally interested in the algebraic properties of the structure obtained from the action of G on the polynomial ring $\mathbb{F}[V]$ generated by $x_1, \ldots, x_n$ which are a basis of the dual space V^*. The action of G on $\mathbb{F}[V]$ is induced from the action on V defining as $(\sigma \cdot f)(v) = f(\sigma^{-1} \cdot v)$ for each $\sigma \in G$, $v \in V$ and $f \in \mathbb{F}[V]$. The set of polynomials in $\mathbb{F}[V]$ fixed under the group action

is a central object of invariant theory. This set is denoted by $\mathbb{F}[V]^G$ and it has a ring structure, so it is called the *invariant ring* or the *ring of invariants*. More explicitly,

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

Each element of $\mathbb{F}[V]^G$ is said to be an *invariant* (or a *G-invariant*) in $\mathbb{F}[V]$.

Although the polynomial ring $\mathbb{F}[V]$ is a finitely generated $\mathbb{F}$-algebra, its subalgebras may not be finitely generated. Therefore, the finiteness of the invariant ring became a big problem in the nineteenth century, which is known as Hilbert's finiteness theorem. Firstly, it was proved by Gordan [16] in 1868 for the special linear group SL_2 over the field of characteristic zero. Then Hilbert gave a non-constructive proof for reductive groups in 1890 ([18]) and a constructive one in 1893 ([19]). The abstract methods of both papers contain many important basics of commutative algebra such as Hilbert Nullstellensatz, Noether normalization lemma, Hilbert syzygy theorem. Hilbert's finiteness theorem was showed in characteristic zero by Noether [32] in 1915. Finally, she proved it in 1926 for all finite groups in arbitrary characteristic (see [33]).

After it is revealed that the invariant ring is finitely generated, the maximum degree of a polynomial in a minimal generating set of the invariant ring becomes the other interesting problem. Noether [32] in characteristic zero, Fogarty [14] and Fleischmann [12] in non-modular case proved that the invariant ring can be generated by polynomials of degree at most the group order. This degree bound is called *Noether bound* in the literature. However, Noether bound does not hold for modular representations. It was showed by Symonds in [49] that there is an invariant ring that required a generator of degree $n(|G| - 1)$ depending on the dimension n.

As a related structure with the invariant ring, the *Hilbert ideal* $\mathfrak{h}$ is the ideal of $\mathbb{F}[V]$ generated by invariants in positive degree:

$$\mathfrak{h} = \langle f \in \mathbb{F}[V]^G \mid \deg f > 0 \rangle.$$

It was observed that this ideal satisfies the Noether bound in the cases that it

fails for the invariant ring. Then, it was conjectured that the Hilbert ideal is generated by polynomials of degree at most the group order (see [8, Conjecture 3.8.6 (b)]).

The Hilbert ideal conjecture is a famous open problem of this century. Fleischmann and Fogarty also proved that the conjecture holds in non-modular case in [12], [14], respectively. Actually, they obtained this result in the proof of the Noether bound for the invariant ring. In Section 3.1, we give Fogarty's proof simplified by Benson since he used an elegant polynomial identity inspiring from an argument in [32]. This polynomial identity will become a useful tool to our targets in this thesis.

Moreover, the conjecture is proved for permutation representations by Fleischmann in 2004 [13]. In order to get this result, Fleischmann also defined an important polynomial identity as Benson's. The identity is a special tool to reach our results (see Section 3.3.2).

Campbell and Hughes in [3] gave the generators for the *ring of vector invariants* $\mathbb{F}[mV_2]^{C_p}$ of the cyclic group C_p of order p, where V_2 is an indecomposable two dimensional representation and mV_2 denotes the m-copy of V_2 with the diagonal action of G. Indeed, it is conjectured and showed by Richman in [35] that the invariant ring needs a generator of degree $m(p-1)$ which violates the Noether bound for sufficiently many copies of V_2. However, Shank and Wehlau in [42] are proved that the Hilbert ideal conjecture holds for the corresponding Hilbert ideal of $\mathbb{F}[mV_2]^{C_p}$.

Also, Sezer in [38] has studied on the Hilbert ideal of indecomposable representations for C_p and showed that the conjecture is true for these representations. The technique he used is similar to Benson's method. We frequently benefit from his results along this thesis. He recovered the statement of the conjecture as that the Hilbert ideal is generated by polynomials of degree at most the group order for indecomposable representations.

Besides, the calculations in all cases given in [39] satisfy the Hilbert ideal conjecture. In this thesis, we also show that the examples considered in [53]

confirm the conjecture.

Not only the degree bound of Hilbert ideal, but also its structure is studied in the literature. Kohls and Sezer in [24] considered the Gröbner basis of the Hilbert ideal for a class of Dihedral groups. The Hilbert ideals of vector invariants of the regular representation of the symmetric group S_n was examined by Sezer and Ünlü in [40].

The cyclic p-group C_{p^r} is a fundamental group for the open problems in modular invariant theory. Shank and Wehlau gave the relation of representations of C_p with their subrepresentations in [44]. The invariants of the cyclic group C_{p^2} were studied for its indecomposable representations and for its $p+1$ dimensional representations in [30] and [43], respectively.

In Section 3.3, we are interested in the Hilbert ideal conjecture for indecomposable representations of C_{p^2}. One of the main results of this thesis is that the conjecture holds for the representations with the dimension n satisfying $n \geq p^2 - 2p$ or $n \leq 4p$.

Beside a generating set of the invariant ring $\mathbb{F}[V]^G$, there are also studies on its structure. Shephard, Todd and Chevalley proved that in the non-modular case, $\mathbb{F}[V]^G$ is a polynomial algebra if and only if G is generated by *pseudo-reflections* which are linear automorphisms $s : V \to V$ of finite order fixing a hyperplane. The sufficient condition of the statement also holds for modular representations (see [37]). But, the necessary part is not satisfied if p divides the order of the group (for example, see [27]). Kac and Peterson recovered this part in [21] using the concept of the *ideal of generalized invariants*. Also, Neumann, Neusel and Smith studied this ideal in [28].

In Section 4.2, we define a new concept, *generalized invariants*, not only for pseudoreflection groups but for any group. Our definition is completely different from Kac-Peterson's definition although we inspire from it. Thus, it brings a new perspective in modular invariant theory. We call a polynomial $f \in \mathbb{F}[V]$ a *generalized invariant* if for each $1 \neq \sigma \in G$, there exists a positive integer ℓ such that $(\sigma - 1)^\ell \cdot f = 0$ provided that $(\sigma - 1)^\ell$ is non-zero. We denote the set consisting

of generalized invariants of $\mathbb{F}[V]$ by $\mathbb{F}[V]^G_\Delta$. Note that an element $f \in \mathbb{F}[V]$ is G-invariant if $(\sigma - 1) \cdot f = 0$ for all $\sigma \in G$. Thus, generalized invariants can be seen as a natural extension of the invariant ring $\mathbb{F}[V]^G$. However, the set $\mathbb{F}[V]^G_\Delta$ will provide a different structure from the invariant ring since it has an $\mathbb{F}[V]^G$-module structure by the *twisted derivation* property of $\sigma - 1$, see Section 4.3. Moreover, this module is finitely generated over the ring $\mathbb{F}[V]^G$. We expect that the concept of generalized invariants may give a solution to some problems in invariant theory because generalized invariants are more common and computable. During the thesis studies, we support our hypothesis and ideas by calculations in Magma ([2]) producing examples or counterexamples (see [26]).

Recently, Grosshans and Walcher publish their study [17] on *modules of higher order invariants* which arise as an algebraic result of the work [15] on a problem in ordinary differential equations. As well as the definition of these modules are similiar to generalized invariant modules, their concept is defined for linear algebraic groups and we have different results which are complement of their studies. Moreover, the paper [17] of Grosshans-Walcher is important as an application of generalized invariants in various areas of mathematics.

In order to understand the module structure of generalized invariants, we start with investigating the generalized invariants of the cyclic group C_p, as a basic step, in Chapter 5. We show that the necessary and sufficient condition to be C_p-generalized invariant is being in the kernel $\operatorname{Ker} \operatorname{Tr}^{C_p}$ of the transfer map of C_p, where the *transfer map* $\operatorname{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ is defined by $\operatorname{Tr}^G(f) = \sum_{\sigma \in G} \sigma \cdot f$ for $f \in \mathbb{F}[V]$ and it is a powerful tool to construct G-invariants, especially in the non-modular case. Moreover, the n-th cohomology group of C_p corresponds to the quotient $\mathbb{F}[V]^{C_p}/\operatorname{Im} \operatorname{Tr}^{C_p}$ if n is even, and to the quotient $\operatorname{Ker} \operatorname{Tr}^{C_p}/\operatorname{Im}(\sigma - 1) = \mathbb{F}[V]^{C_p}_\Delta/\operatorname{Im}(\sigma - 1)$ if n is odd, where σ is a generator of C_p. Thus, the generalized invariants of C_p provide an important structure in modular invariant theory. In Section 5.2, we describe the structure of generalized invariants of C_p for lower dimensional indecomposable representations, and show that for these representations, $\mathbb{F}[V]^{C_p}_\Delta$ is a free module over a polynomial ring generated by a *homogeneous system of parameters* while at the same time, the corresponding invariant ring is Cohen-Macaulay. Also, we prove an analogy of

the Hilbert ideal conjecture for the case of generalized invariants, see Section 5.3.

The structure of generalized invariants becomes more complicated for higher dimensional representations, even for indecomposable ones. Therefore, it is difficult to give an explicit description of generalized invariants as in Section 5.2. Instead of this, we find core structures of generalized invariant modules for any group G, and we give them in a general form in Chapter 6. To do this, we investigate some subgroup relations of generalized invariants for a finite group.

In Section 4.4, we prove that in the non-modular case, generalized invariants correspond to usual invariants. We demonstrate in Chapter 7 the condition in which these two structures coincide for modular representations. In order to show this, we benefit from the *ladder method* which is a powerful technique especially for representations in zero characteristic (see [25], [34], [52]).

The results about the indecomposable representations of the cyclic group of order p^2 have been published in [9], the first results about generalized invariants of cyclic groups have been published in [10] and some of the last results have been submitted for possible publication [11].

Chapter 2

Basic Notations and Constructions

In this chapter, we introduce basic definitions, tools and notations required for the thesis. These are split up into four main topics: group theory, module and ring theory, representation theory, and invariant theory.

2.1 Group Theory

Unless otherwise stated, we always consider finite groups. Generally, we denote a finite group by G, but now, we give the definition of some basic groups with their notations for our aim.

Reflection Groups: A linear automorphism $s : V \to V$ is called a *reflection* if

(i) $s \neq 1$,

(ii) $s^2 = 1$,

(iii) s fixes a codimension one subspace which is called the *hyperplane* of s.

A *reflection group* is a subgroup of the general linear group $\mathrm{GL}(V)$ generated by reflections.

Dihedral Groups: The *dihedral group* D_{2n} is the set of all symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon. The group D_{2n} has order $2n$ and the following *presentation*

$$\mathrm{D}_{2n} = \langle\, r, s \,|\, r^n = s^2 = (rs)^2 = 1 \,\rangle$$

where it is generated by the rotation r and the reflection s. Now, let $s_1 = s$, $s_2 = rs$. Then the presentation can be written with reflections as follows

$$\mathrm{D}_{2n} = \langle\, s_1, s_2 \,|\, s_1^2 = s_2^2 = (s_1 s_2)^n = 1 \,\rangle.$$

Coxeter Groups: A *Coxeter group* is a group given by the presentation

$$\langle\, s_1, \ldots, s_n \,|\, (s_i s_j)^{m_{ij}} = 1 \,\rangle$$

where $m_{ii} = 1$ and $m_{ij} \geq 2$ for all $i \neq j$. Coxeter in [7] proved that every reflection group is a Coxeter group.

Symmetric Groups: The group S_n of all permutations of the set $\{1, 2, \ldots, n\}$ is the *symmetric group* on n letters. The symmetric group S_n is a Coxeter group as follows

$$\langle\, s_1, \ldots, s_{n-1} \,|\, s_i^2 = (s_i s_{i+1})^3 = (s_i s_j)^2 = 1 \;\; \forall\, i \neq j \,\rangle$$

where s_i denotes the adjacent transposition $(i \;\, i+1)$. As a consequence, dihedral groups, symmetric groups and reflection groups are Coxeter groups.

Sylow Subgroups: If G is a group of order $p^r m$, where p is a prime and $p \nmid m$, then a subgroup P of order p^r is called a *Sylow p-subgroup* (or a *Sylow subgroup*) of G.

Example 2.1. For any prime p dividing the order $|G|$, the group G has a Sylow p-subgroup.

Characteristic Groups: A subgroup N of a group G is called *characteristic* in G if every automorphism of G maps N to itself.

Lemma 2.1 *A characteristic subgroup N of a group G is normal.*

Proof. Consider the automorphism $\varphi : \sigma \mapsto g\sigma g^{-1}$ of G for any $g \in G$. By the definition of a characteristic subgroup, N is invariant under φ:

$$\varphi(N) \subseteq N.$$

Therefore, we have $gNg^{-1} = N$ for each $g \in G$. □

Group Actions: A *left action* of a group G on a set A is a map from $G \times A$ to A, written $(g, a) \mapsto g \cdot a$ for all $g \in G$ and $a \in A$, satisfying the following properties

(i) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$,

(ii) $1 \cdot a = a$ for all $a \in A$.

The *kernel* of the action is the set of elements of G that act trivially on each element of A:

$$\{\, g \in G \,|\, g \cdot a = a \ \ \forall\, a \in A \,\}.$$

An action is *faithful* if its kernel is trivial.

A map between two sets commuting with the action of a group G is said to be G-*equivariant* or *equivariant map*. More precisely, if G acts on the sets A and B, and $f : A \to B$ is an equivariant map, then for all $g \in G$, $a \in A$,

$$f(g \cdot a) = g \cdot f(a).$$

2.2 Representation Theory

Definition. Let V be a finite dimensional vector space over a field $\mathbb{F}$. A *finite dimensional representation* ρ of a group G on V is a group homomorphism

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

defined by $\rho(\sigma)(v) = \sigma \cdot v$ for all $\sigma \in G$ and $v \in V$, where $GL(V)$ is the group of automorphisms of V. The vector space V may be assigned as a representation ρ in the text. The *dimension (or degree) of the representation* is the dimension of the vector space V. From now on, we denote $\rho(\sigma)(v)$ by $\sigma(v)$ when the representation is clear from the context.

If the group homomorphism ρ above is injective, then the representation is called a *faithful representation*. If a representation is not faithful, we can get an injective homomorphism by setting

$$\rho : G/\mathrm{Ker}(\rho) \hookrightarrow GL(V).$$

Thus, we can always consider faithful representations in this thesis.

Suppose that G acts on a finite set A. Let V be a vector space having a basis $(e_a)_{a\in A}$. For $\sigma \in G$, let $\rho(\sigma) : V \to V$ be the linear map which sends $e_a \mapsto e_{\sigma a}$. The resulting representation of G is called *permutation representation* of G associated with A. If we take itself of G instead of A, the obtained representation is called the *regular representation* of G.

Let V^G denote the set of vectors fixed by the action of the group G:

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

The *dual vector space* V^* of V is the set, $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$, of all linear functions from V to $\mathbb{F}$. The action of G on V given above induces a left action of G on the

dual space V^* defined by

$$\big(\sigma(x)\big)(v) = x\big(\sigma^{-1}(v)\big)$$

for all $\sigma \in G$, $x \in V^*$ and $v \in V$. Indeed, for all $\sigma, \tau \in G$,

$$\begin{aligned}\Big(\sigma\big(\tau(x)\big)\Big)(v) &= \big(\tau(x)\big)\big(\sigma^{-1}(v)\big)\\ &= x\Big(\tau^{-1}\big(\sigma^{-1}(v)\big)\Big)\\ &= x\big((\tau^{-1}\sigma^{-1})(v)\big)\\ &= x\big((\sigma\tau)^{-1}(v)\big)\\ &= \big((\sigma\tau)(x)\big)(v).\end{aligned}$$

A subspace W of the vector space V is called *G-invariant* (or simply *invariant*) if for all $\sigma \in G$,

$$\sigma(W) \subseteq W.$$

The restriction of ρ to a G-invariant subspace $W \subseteq V$ is called a *subrepresentation* of V. A representation ρ of V is said to be *irreducible* if it has only trivial subrepresentations V and $\{0\}$. An *indecomposable representation* V means that V cannot be decomposed into a direct sum of proper nontrivial subrepresentations. It follows that every irreducible representation is indecomposable.

The subgroup of the general linear group $\mathrm{GL}_n(V)$ given by a system of algebraic equations is called a *linear algebraic group*. For example,

$$\mathrm{SL}_n(V) = \{\sigma \in \mathrm{GL}_n(V) \,|\, \det(\sigma) = 1\}.$$

A linear algebraic group G is said to be *reductive* if each representation V of G is *completely reducible*, i.e. every G-invariant subspace $W \subseteq V$ has a G-invariant complement U:

$$V = W \oplus U.$$

The following is a famous and useful result in representation theory. However,

it holds only for a special case which is defined below.

Theorem 2.2 (Maschke's Theorem) *If G is a group and $\mathbb{F}$ is a field whose characteristic does not divide the group order $|G|$, then each representation of G over $\mathbb{F}$ is completely reducible.*

A representation of G over $\mathbb{F}$ satisfying the condition given in Maschke's theorem (or equivalently, when $|G|$ is invertible in $\mathbb{F}$) is called a *non-modular representation*. A representation of the group G is said to be a *modular representation* if the characteristic $\mathrm{char}(\mathbb{F})$ of $\mathbb{F}$ divides the group order $|G|$. In representation theory, there is a dichotomy as modular and non-modular cases. Many of the problems in invariant theory is better understood in non-modular case due to Maschke's theorem, while modular invariant theory of finite groups over finite fields presents many open problems.

The following well-known lemma is required for the results in this thesis.

Lemma 2.3 *If $q = p^r$ is a prime power and $k \in \mathbb{Z}^+$, then*

$$\sum_{\ell \in \mathbb{F}_q} \ell^k = \begin{cases} -1 & \text{if } q-1 \mid k, \\ 0 & \text{if } q-1 \nmid k. \end{cases}$$

Proof. Let a be a generator of $\mathbb{F}_q$. Then $\mathbb{F}_q \backslash \{0\} = \{1, a, a^2, \ldots, a^{q-2}\}$ and

$$\sum_{\ell \in \mathbb{F}_q} \ell^k = \sum_{i=0}^{q-2} (a^i)^k = \sum_{i=0}^{q-2} (a^k)^i.$$

Note that the element of $\mathbb{F}_q$, a^k is a root of the following polynomial

$$x^{q-1} - 1 = (x-1)(x^{q-2} + \cdots + x + 1).$$

If $q-1 \mid k$, then $a^k = 1$ and the sum is equal to $q-1 \equiv -1$. If $q-1 \nmid k$, then $a^k \neq 1$ and so a^k is a root of $x^{q-2} + \cdots + x + 1$. Thus, the sum is zero. □

2.3 Module and Ring Theory

Integral Extensions: Let B be a subring of a ring A. An element $a \in A$ is called *integral* over B if it is a root of a monic polynomial with coefficients in B, i.e.

$$a^n + b_1 a^{n-1} + \cdots + b_n = 0,$$

where $b_i \in B$. The ring A is called an *integral extension* of B if each element of A is integral over B.

$\mathbb{F}G$-Modules: Let V be a representation of a finite group G. Note that $\mathbb{F}G$ is a group ring and the G-action on the vector space V constructs an $\mathbb{F}G$-module structure on V. Therefore, a representation V of G can also be called an $\mathbb{F}G$-module.

Projective Modules: An A-module M is said to be a *projective module* if every epimorphism $\varphi : N \to M$ for any A-module N splits, i.e., there exists a homomorphism $\psi : M \to N$ such that $\varphi \circ \psi = 1_M$.

Noetherian Modules: A module M over a ring A is called *Noetherian* if every A-submodule of M is finitely generated.

Lemma 2.4 *An A-module M is Noetherian if and only if N and M/N are Noetherian A-modules for any submodule N of M.*

Proof. Suppose that M is a Noetherian A-module. Let $N \leq M$. Then N is Noetherian since every submodule of N is also submodule of M. Let $K/N \leq M/N$ for $N \leq K \leq M$. Since M is Noetherian, K is finitely generated. Also so is K/N. Hence, M/N is Noetherian.

For the converse, suppose that N is a submodule of M and both N and M/N are Noetherian. Let K be a submodule of M. Then the epimorphic image of K in M/N is finitely generated, say $m_1, \ldots, m_r \in K$ generate this image. Thus, for any $m \in K$, we have $m \equiv \sum_{i=1}^{r} a_i m_i \mod N$ for some $a_i \in A$. Then, $m - \sum_{i=1}^{r} a_i m_i \in K \cap N$. However, since $K \cap N \leq N$ and N is Noetherian, $K \cap N$ is generated by some elements $n_1, \ldots, n_s$. Therefore, we obtain

that $m = \sum_{i=1}^{r} a_i m_i + \sum_{j=1}^{s} b_j n_j$ where $b_j \in A$. Hence, K is generated by $m_1, \ldots, m_r, n_1, \ldots, n_s$ and M is Noetherian. □

Lemma 2.5 *A finite sum of Noetherian modules is Noetherian.*

Proof. Let $M = \sum_{i=1}^{n} N_i$ with N_i are Noetherian submodules of M. By induction on n, suppose that

$$K = \sum_{i=1}^{n-1} N_i$$

is Noetherian. Then we have $M/N_n = (K + N_n)/N_n \cong K/K \cap N_n$. Since K is Noetherian, so is $K/K \cap N_n$ and hence also M/N_n. The submodule N_n is Noetherian. Thus, the result follows from the previous lemma. □

Lemma 2.6 *A finitely generated module ${}_AM$ over a Noetherian ring A is Noetherian.*

Proof. For $m \in M$, we consider the A-module homomorphism

$$\varphi_m : A \to M$$

defined by $\varphi_m(a) = am$. Then $A/\mathrm{Ker}\varphi_m \cong \mathrm{Im}\varphi_m = Am$. Since A is Noetherian, so is Am. If $m_1, \ldots, m_n$ is a generating set of M, then the assertion follows from the previous lemma as

$$M = \sum_{i=1}^{n} Am_i.$$

□

2.4 Invariant Theory

2.4.1 Polynomial Ring

Let V be an n-dimensional representation of a finite group G over a field $\mathbb{F}$ and $\{x_1, x_2, \ldots, x_n\}$ a basis of the dual space V^*. Let $\mathbb{F}[V]$ denote the polynomial

ring $\mathbb{F}[x_1, \ldots, x_n]$ with n-indeterminates. Note that the polynomial ring $\mathbb{F}[V]$ has an $\mathbb{F}$-algebra structure and $x_1, \ldots, x_n$ generate $\mathbb{F}[V]$ as an $\mathbb{F}$-algebra. Define the monomial in $\mathbb{F}[V]$

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

for a sequence $I = \{i_1 \ldots, i_n\}$ of nonnegative integers. Then the total degree $i_1 + \ldots + i_n$ of the monomial x^I is called the *degree* of x^I and denoted by $\deg(x^I)$. Consider a polynomial

$$f = \sum_j a_j x^{I_j}$$

where $a_j \in \mathbb{F}$. The polynomial f is called *homogeneous of degree* d if each monomial x^I is of degree d. Let $\mathbb{F}[V]_d$ be the space of homogeneous polynomials of degree d. Then the polynomial ring $\mathbb{F}[V]$ is graded by nonnegative degree:

$$\mathbb{F}[V] = \bigoplus_{d \geq 0} \mathbb{F}[V]_d.$$

Therefore, $\mathbb{F}[V]$ has a *graded algebra* structure, i.e.,

(i) $\mathbb{F}[V]_d$ is a subspace of $\mathbb{F}[V]$ for each $d \geq 0$,

(ii) if $f \in \mathbb{F}[V]_d$ and $f' \in \mathbb{F}[V]_{d'}$, then $ff' \in \mathbb{F}[V]_{d+d'}$,

We use $\mathbb{F}[V]^+$ instead of $\bigoplus_{d>0} \mathbb{F}[V]_d$, the vector space generated by positive degree polynomials. A graded $\mathbb{F}$-algebra A is called *connected* if $A_0 = \mathbb{F}$. Therefore, the polynomial ring $\mathbb{F}[V]$ is a graded connected $\mathbb{F}$-algebra.

The action of G on the dual vector space V^* can be defined as

$$(\sigma(f))(v) = f(\sigma^{-1}(v))$$

for all $\sigma \in G$, $f \in V^*$, $v \in V$. This action can be naturally extended to the action of G on the polynomial ring $\mathbb{F}[V]$ additively and multiplicatively as follows

$$\sigma(f + f') = \sigma(f) + \sigma(f'),$$

$$\sigma(ff') = \sigma(f)\sigma(f')$$

for all $f, f' \in \mathbb{F}[V]$. An ideal I of $\mathbb{F}[V]$ is called a *G-stable ideal* if I is *invariant* under the action of G, i.e., for all $\sigma \in G$, $\sigma I \subseteq I$.

Let $\mathrm{LM}(f)$ and $\mathrm{LT}(f)$ denote the *leading monomial* and the *leading term*, respectively, of a polynomial $f \in \mathbb{F}[V]$ with respect to the given monomial order. Unless otherwise stated, we will use the graded reverse lex-order induced by $x_1 \prec \cdots \prec x_n$.

A generating set X for a module M is called *minimal* if any proper subset of X generates a proper submodule of M. In this thesis, we use the same term, *minimal generating set,* for a minimal generating set with an additional condition that the leading monomials of the polynomials in this generating set are minimal. The generators in a minimal generating set are not unique, but the leading monomials of the generators are unique for a fixed monomial order.

Although the polynomial ring $\mathbb{F}[V]$ is a finitely generated $\mathbb{F}$-algebra, not every subalgebra of $\mathbb{F}[V]$ need to be finitely generated as shown in the next example given in [46].

Example 2.2. Consider the subalgebra A of the polynomial ring $\mathbb{F}[x, y]$ generated by

$$1, xy, xy^2, \ldots, xy^n, \ldots$$

Observe that the generator xy^n can not be in the subalgebra generated by the remaining generators. Thus, A is an infinitely generated subalgebra of $\mathbb{F}[x, y]$.

2.4.2 Invariant Ring

The ring of all polynomials in $\mathbb{F}[V]$ fixed by the group action of G is called the *invariant ring* or *ring of invariants*, more precisely,

$$\mathbb{F}[V]^G = \{\, f \in \mathbb{F}[V] \mid \sigma(f) = f \ \ \forall\, g \in G \,\},$$

and is denoted by $\mathbb{F}[V]^G$. This construction clearly has a ring structure, and it is the main object in invariant theory. A polynomial in $\mathbb{F}[V]^G$ is called *G-invariant.*

Since the polynomial ring $\mathbb{F}[V]$ is a graded algebra, the subalgebra $\mathbb{F}[V]^G$ also has a graded structure. Therefore, without loss of generality, we assume that all polynomials are homogeneous polynomials unless stated otherwise. We denote the ideal of the positive degree invariants in $\mathbb{F}[V]^G$ by $\mathbb{F}[V]^{G,+}$. Notice that for a subgroup H of G,

$$\mathbb{F}[V]^G \subseteq \mathbb{F}[V]^H.$$

For $f \in \mathbb{F}[V]$ and $|G| = m$, consider the polynomial

$$\prod_{\sigma \in G}(X - \sigma(f)) = \sum_{i=1}^{m}(-1)^i s_i X^{m-i}. \tag{2.1}$$

The coefficients s_i of the polynomial are given by

$$\begin{aligned} s_1 &= \sigma_1(f) + \sigma_2(f) + \cdots + \sigma_m(f), \\ s_2 &= \sigma_1\sigma_2(f) + \sigma_1\sigma_3(f) + \cdots + \sigma_{m-1}\sigma_m(f), \\ &\vdots \\ s_m &= \sigma_1\sigma_2 \cdots \sigma_m(f). \end{aligned}$$

Hence, the coefficients s_i are in the invariant ring $\mathbb{F}[V]^G$. These coefficients are called *elementary symmetric polynomials*.

In the previous section, we demonstrated that a given subalgebra of $\mathbb{F}[V]$ is not necessarily finitely generated. However, now we show that the invariant ring $\mathbb{F}[V]^G$ is finitely generated an $\mathbb{F}$-algebra. In the literature, Gordan in 1868 proved this statement for the group SL_2 over the filed of characteristic zero. But, this method did not generalize to the other groups. Then, Hilbert gave a proof for linearly reductive groups in 1890 and a constructive proof in 1893. A constructive proof when the characteristic of the field is zero or greater than the group order was given by Noether in 1916. In 1926, she proved the result for all finite groups in arbitrary characteristic as follows.

Theorem 2.7 (Finiteness Theorem) *If G is a finite group acting as automorphisms of a finitely generated commutative algebra A over a field $\mathbb{F}$, then A^G is a finitely generated $\mathbb{F}$-algebra and A is finitely generated as a module over A^G.*

Proof. Let $f \in A$. Consider the monic polynomial (2.1)

$$P(X) = \prod_{\sigma \in G} (X - \sigma(f))$$

which lies in $A^G[X]$. Note that f is a root of this polynomial. So, A is an integral extension of A^G. Finitely many generators of A are roots of the monic polynomials $P(X)$. Let B be the subalgebra of A^G generated by the coefficients of the polynomials $P(X)$. Then B is a finitely generated $\mathbb{F}$-algebra. Since $\mathbb{F}$ is Noetherian, also so is B by Lemma 2.6. Note that A is a finitely generated module over B by the construction of B. Thus, A is a Noetherian B-module, so its B-submodule A^G is also finitely generated. Hence, A^G is a finitely generated $\mathbb{F}$-algebra. The last part is clear by the context of the proof. □

As a consequence of the finiteness theorem, we obtain the following result.

Corollary 2.8 *The invariant ring $\mathbb{F}[V]^G$ is a finitely generated $\mathbb{F}$-algebra. In particular, it is a Noetherian ring and $\mathbb{F}[V]$ is a Noetherian $\mathbb{F}[V]^G$-module.*

2.4.3 Construction of Invariants

A powerful tool to construct an invariant for a finite group G is the *transfer map*

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

defined by

$$\mathrm{Tr}^G(f) = \sum_{\sigma \in G} \sigma(f)$$

where $f \in \mathbb{F}[V]$. Indeed, for all $\tau \in G$, we have

$$\tau \mathrm{Tr}^G(f) = \sum_{\sigma \in G} (\tau\sigma)(f)$$

which is the same as the sum defining $\mathrm{Tr}^G(f)$ except for the order of the summands. Thus, $\mathrm{Tr}^G(f) \in \mathbb{F}[V]^G$ for all $f \in \mathbb{F}[V]$. Sometimes, the transfer Tr^G is

called the *G-transfer*. Observe that the transfer Tr^G is an $\mathbb{F}[V]^G$-module homomorphism: for any $h \in \mathbb{F}[V]^G$, we have

$$\mathrm{Tr}^G(hf) = \sum_{\sigma \in G} h\sigma(f) = h\mathrm{Tr}^G(f),$$

and it is linear by the definition of the action on the polynomial ring $\mathbb{F}[V]$. It follows that for any $f \in \mathbb{F}[V]^G$,

$$\mathrm{Tr}^G(f) = \sum_{\sigma \in G} f\sigma(1) = |G|f.$$

Thus, in the non-modular case, Tr^G is surjective and

$$\mathcal{R}^G = \frac{1}{|G|}\mathrm{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$$

is a well-defined projection onto $\mathbb{F}[V]^G$. This map is called the *Reynolds operator*. It satisfies the following split equation

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V] \overset{\mathcal{R}}{\twoheadrightarrow} \mathbb{F}[V]^G.$$

So, we obtain the following decomposition:

$$\mathbb{F}[V] = \mathrm{Ker}\mathcal{R}^G \oplus \mathbb{F}[V]^G.$$

Similarly, we can define the relative versions of the transfer map and the Reynolds operator as follows. Let $H \leq G$ be a subgroup of G. Consider the map

$$\mathrm{Tr}^G_H : \mathbb{F}[V]^H \to \mathbb{F}[V]^G$$

defined by

$$\mathrm{Tr}^G_H(f) = \sum_{\sigma H \in G/H} \sigma(f)$$

where $f \in \mathbb{F}[V]^H$. It is well-defined since $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]^H$ and called the *relative transfer* from H to G. Sometimes we call the transfer Tr^G as the *full transfer* to

avoid confusion. It can immediately be seen that

$$\mathrm{Tr}^G = \mathrm{Tr}^G_H \circ \mathrm{Tr}^H$$

by the definition of the relative transfer. If the characteristic of the field does not divide the index $[G : H]$, then the relative transfer map Tr^G_H is surjective and the operator $\mathcal{R}^G_H = \frac{1}{[G:H]}\mathrm{Tr}^G_H$ is a projection from $\mathbb{F}[V]^H$ onto $\mathbb{F}[V]^G$. Also, we have the decomposition

$$\mathbb{F}[V]^H = \mathrm{Ker}\mathcal{R}^G_H \oplus \mathbb{F}[V]^G.$$

Moreover, the image ImTr^G of the transfer is an ideal of $\mathbb{F}[V]^G$ since the transfer map Tr^G is a module homomorphism. The following theorem states that this ideal is proper in the modular case which is proved in [41, Theorem 2.2].

Theorem 2.9 *If $p \,|\, |G|$, then the image ImTr^G of transfer is properly contained in $\mathbb{F}[V]^G$.*

The other tool to construct invariants of finite groups is *the norm* N^G defined as

$$\mathrm{N}^G(f) := \prod_{\sigma \in G} \sigma(f),$$

and the *relative norm* N^G_H for a subgroup $H \leq G$ is

$$\mathrm{N}^G_H(f) := \prod_{\sigma H \in G/H} \sigma(f).$$

The image ImTr^G of transfer is also a nonzero ideal as shown below.

Lemma 2.10 *[4, Corollary 9.0.17] For a representation V of G, the image of the transfer $\mathrm{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ is nonzero.*

Proof. We extend the action of the group G to the field of the fractions $\mathbb{F}(V)$. Since any set of field automorphisms is linearly independent, Tr^G is nonzero in $\mathbb{F}(V)$, i.e., there are polynomials $f, h \in \mathbb{F}[V]$ such that

$$\mathrm{Tr}^G(f/h) \neq 0.$$

However, notice that $\mathrm{N}^G(h)f/h \in \mathbb{F}[V]$. Therefore, for the $\mathbb{F}[V]^G$-module homomorphism Tr^G,

$$\mathrm{Tr}^G(\mathrm{N}^G(h)f/h) = \mathrm{N}^G(h)\mathrm{Tr}^G(f/h) \neq 0.$$

□

2.4.4 Cyclic p-Groups

Let G denote the cyclic group C_{p^r} of order p^r with generator σ, and let V be a finite dimensional indecomposable representation of G of dimension n over the field $\mathbb{F}$ of characteristic p. Let H be a subgroup of G of order p. Then we can give the transfers and the norms of C_{p^r} as follows: for all $f \in \mathbb{F}[V]$,

(i) the full transfer of f is $\mathrm{Tr}^G(f) = \sum_{\ell=0}^{p^r-1} \sigma^\ell(f)$,

(ii) the H-transfer of f is $\mathrm{Tr}^H(f) = \sum_{\ell=0}^{p-1} \sigma^{p^{r-1}\ell}(f)$,

(iii) the G-norm of f is $\mathrm{N}^G(f) = \prod_{\ell=0}^{p^r-1} \sigma^\ell(f)$,

(iv) the H-norm of f is $\mathrm{N}^H(f) = \prod_{\ell=0}^{p-1} \sigma^{p^{r-1}\ell}(f)$,

(v) if $f \in \mathbb{F}[V]^H$, the relative transfer of f is $\mathrm{Tr}_H^G(f) = \sum_{\ell=0}^{p^{r-1}-1} \sigma^{p\ell}(f)$

which are required for the rest of the thesis. The order of G implies that $\sigma^{p^r} = 1$. It follows that every eigenvalue λ of σ is a p^r-th root of unity in the ground field $\mathbb{F}$. Since $\mathrm{char}(\mathbb{F}) = p$, we have

$$(\lambda - 1)^{p^r} = \lambda^{p^r} - 1 = 0.$$

Thus, $\lambda = 1$ is the only p^r-th root of unity that lies in $\mathbb{F}$. Let $\{e_1, \ldots, e_n\}$ be a basis of V such that σ is in the Jordan canonical form. If σ has more than one Jordan blocks, then V has a direct sum decomposition corresponding to the blocks. It is a contradiction by the assumption on V. Hence, the representation

of σ has the form

$$\sigma = \begin{bmatrix} 1 & 0 & \dots 0 & 0 \\ 1 & 1 & \dots 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots 1 & 0 \\ 0 & 0 & \dots 1 & 1 \end{bmatrix}$$

and we obtain the following result.

Lemma 2.11 *With the above notations, if a representation V of G with degree n is indecomposable, then $p^{r-1} < n \leq p^r$.*

Proof. The above matrix has order p^r if and only if $p^{r-1} < n \leq p^r$. It completes the proof. □

Corollary 2.12 *There are exactly p^r-many inequivalent indecomposable representations $V_1, V_2, \dots, V_{p^r}$ of G. Moreover, we obtain the following inclusion:*

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

Since we generally use the cyclic group C_p in this thesis and for the simplicity of the notations, the following corollary is given in a special case although it is true for any cyclic p-group C_{p^r}.

Corollary 2.13 *If V is a finite dimensional representation of C_p, then it decomposes into indecomposable C_p-representations as follows*

$$V = \bigoplus_{i=1}^{p} m_i V_i$$

where m_i is the number of the copies of V_i in V.

Lemma 2.14 *The only projective indecomposable representation of C_p is V_p which is isomorphic to the regular module $\mathbb{F}C_p$.*

Proof. Let $\{e_1, \dots, e_p\}$ be a basis for V_p as defined by the above lower triangular matrix and let V_r be the subspace spanned by $\{e_{p-r+1}, e_{p-r+2}, \dots, e_p\}$ for $r < p$.

Suppose, for contradiction, that V_r is projective. Define a map $\varphi : V_p \to V_r$ by

$$\varphi(e_i) = \begin{cases} 0 & \text{if } i > r, \\ e_{p-r+i} & \text{if } i \leq r. \end{cases}$$

Then we obtain the following exact sequence of C_p-modules

$$0 \to \mathrm{Ker}\varphi \hookrightarrow V_p \xrightarrow{\varphi} V_r \to 0.$$

But V_r is projective. Then, the sequence splits and we get

$$V_p \cong \mathrm{Ker}\varphi \bigoplus V_r.$$

Since V_p is indecomposable, it is a contradiction. Hence, V_r is not projective. □

Lemma 2.15 *An invariant in a projective indecomposable C_p-module is either a norm or a transfer of a polynomial.*

Proof. The assertion follows from Lemma 2.14. □

The following division about C_p-invariants is useful for the reduction of the degrees of invariants.

Lemma 2.16 *If $f \in \mathbb{F}[V]^{C_p}$ and $f = qN^{C_p}(x_n) + r$, where the degree $\deg_{x_n} r$ of r in x_n is less than p, then $q, r \in \mathbb{F}[V]^{C_p}$.*

Proof. Applying a generator σ in C_p to both sides of the above equation, we obtain

$$f = \sigma(q)\mathrm{N}^{C_p}(x_n) + \sigma(r).$$

Since $\deg_{x_n}(\sigma(r)) = \deg_{x_n} r < p$ and $\deg_{x_n}(\sigma(q)) = \deg_{x_n} q$, the uniqueness of the remainder implies that $\sigma(r) = r$ and so $\sigma(q) = q$. □

For a representation V of a finite group G, let $\bigoplus_{i=1}^{m} V$ be denoted by mV. Then the invariant ring $\mathbb{F}[mV]^G$ is called the ring of *vector invariants*. The

following result was conjectured by Richman in [35] and proved by Campbell and Hughes in [3].

Theorem 2.17 *Let mV_2 be a representation of C_p with a basis $\{x_i, y_i\}$ for each copy of V_2^* and for $i = 1, \ldots, m$. Then the invariant ring $\mathbb{F}[mV_2]^{C_p}$ is generated by:*

(i) $x_1, x_2, \ldots, x_m$,

(ii) *the C_p-norms* $N^{C_p}(y_i) = y_i^p - x_i^{p-1}y_i$ *for* $i = 1, \ldots, m$,

(iii) $u_{ij} = x_j y_i - x_i y_j$ *for* $1 \leq i < j \leq m$,

(iv) *the C_p-transfers* $\mathrm{Tr}^{C_p}(y_1^{k_1} \cdots y_m^{k_m})$ *with* $0 \leq k_i < p$.

Remark. It is proved in [42] that if $k_1 + \cdots + k_m \leq 2(p-1)$, then $\mathrm{Tr}^{C_p}(y_1^{k_1} \cdots y_m^{k_m})$ is in the subalgebra generated by the remaining generators above, and if we omit the invariants satisfying above condition, $\mathbb{F}[mV_2]^{C_p}$ can be generated by the remaining elements.

By the above theorem and the remark, we immediately obtain the following results.

Corollary 2.18 *The invariant ring $\mathbb{F}[V_2]^{C_p}$ is equal to $\mathbb{F}[x, N^{C_p}(y)]$.*

Corollary 2.19 *The invariant ring $\mathbb{F}[2V_2]^{C_p}$ is equal to $\mathbb{F}[x_1, x_2, N^{C_p}(y_1), N^{C_p}(y_2), u_{12}]$ with the notations introduced above.*

2.4.5 Homogeneous Systems of Parameters

For a commutative ring A, a chain of its prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \mathfrak{p}_m$$

has length m. The supremum of the lengths over all chains of prime ideals in A is called the *Krull dimension* of A.

Proposition 2.20 *[29, Proposition 10.17] The Krull dimension of the polynomial ring $\mathbb{F}[V]$ is equal to the dimension of V.*

Definition. Let A be a finitely generated $\mathbb{F}$-algebra. A set of homogeneous elements $\{f_1, \ldots, f_n\}$ is called a *homogeneous system of parameters (h.s.o.p.)* of positive degree for A if

(i) the Krull-dimension of A is n, and

(ii) A is finitely generated as a module over the ring $\mathbb{F}[f_1, \ldots, f_n]$.

The following fundamental theorem, Noether Normalization Lemma ([33]) states that h.s.o.p. always exists.

Theorem 2.21 *If A is a finitely generated graded connected $\mathbb{F}$-algebra, then A has an h.s.o.p.*

Definition. Let A be a finitely generated $\mathbb{F}$-algebra. A sequence $\{r_1, \ldots, r_m\}$ in A is called a *regular sequence* if

(i) $(r_1, \ldots, r_m)A \neq A$,

(ii) r_1 is not a zero divisor in A,

(iii) r_i is not a zero divisor in $A/(r_1, \ldots, r_{i-1})A$ for all $i = 2, \ldots, m$.

2.4.6 Noether Number

In Section 2.4.2, we showed that the invariant ring $\mathbb{F}[V]^G$ can be minimally generated as an algebra with a finite collection of homogeneous invariants. The maximum degree of these polynomials is said to be the *Noether number*. We will consider in more detail on this number in Chapter 3. The following result asserts that the Noether number is independent of the choice of the generating set of the group.

Lemma 2.22 (Graded Nakayama Lemma) *The $\mathbb{F}[V]^G$-module $\mathbb{F}[V]^{G,+}$ is (minimally) generated by $f_1, \ldots, f_m$ if and only if the quotient space $\mathbb{F}[V]^{G,+}/(\mathbb{F}[V]^{G,+})^2$ is spanned by their (linearly independent) images $\bar{f_1}, \ldots, \bar{f_m}$.*

Proof. Suppose that $\bar{f_1}, \ldots, \bar{f_m}$ span the $\mathbb{F}$-vector space $\mathbb{F}[V]^{G,+}/(\mathbb{F}[V]^{G,+})^2$. Let $M = \sum_{i=1}^{m} \mathbb{F}[V]^G f_i$ be the submodule of $\mathbb{F}[V]^{G,+}$. Since f_i are homogeneous, M has a graded structure. For contradiction, assume that $M \neq \mathbb{F}[V]^{G,+}$ and let d be the smallest degree satisfying $M_d \subsetneq \mathbb{F}[V]_d^{G,+}$. Let h be in $\mathbb{F}[V]_d^{G,+}$ and not in M_d and its image

$$\overline{h} = \sum_{i=1}^{m} k_i \bar{f}_i$$

where $k_i \in \mathbb{F}$. Then

$$h = \sum_{i=1}^{m} k_i f_i + \sum_{j=1}^{t} g_j h'_j$$

where $g_j, h'_j \in \mathbb{F}[V]^{G,+}$. We may suppose that $\deg(g_j h'_j) = d$ for each $i = 1, \ldots, t$. Therefore, the degree of h'_j is less than d since $\deg g_j \geq 1$, so $h'_j \in M$ for all $j = 1, \ldots, t$. It follows that $h \in \mathbb{F}[V]^{G,+}$. It is a contradiction. The converse statement is obviously true. □

Corollary 2.23 *The lifting of a basis for $\mathbb{F}[V]^{G,+}/(\mathbb{F}[V]^{G,+})^2$ minimally generates the $\mathbb{F}$-algebra $\mathbb{F}[V]^G$.*

By the previous corollary, we can say that a minimal generating set for $\mathbb{F}[V]^G$ is not unique; however, the number of generators in a given degree remains stable. Then, we obtain that the Noether number is independent of the choice of the generators.

Chapter 3

Hilbert Ideal Conjecture

In Section 2.4.2, we proved that the invariant ring for a representation of a finite group is finitely generated. The natural question after this result is what the maximum degree of a polynomial in a minimal generating set of the invariant ring is. In this chapter, we consider such upper degree bounds and give some examples. Then we define an alternative structure to the invariant ring, the Hilbert ideal. We mention a famous conjecture, Hilbert ideal conjecture, with a review of some recent results on this conjecture. Further, we prove that this conjecture holds for a restricted dimension of an indecomposable representation of the cyclic group C_{p^2} which is the main result of this chapter.

3.1 Hilbert Ideal

Consider a representation V of a finite group G over the field $\mathbb{F}$. With respect to this representation, we define $\beta(G)$ as the maximum degree of a generator in a minimal generating set for the invariant ring $\mathbb{F}[V]^G$. By the graded Nakayama lemma in Section 2.4.6, this number does not depend on the choice of the minimal generators. The number $\beta(G)$ is called the *Noether number* for G.

We show that the Noether number for the invariant ring $\mathbb{F}[V]^G$ of a non-modular representation is the order $|G|$ of group G. Originally, Noether proved this in characteristic zero (see [32]). We give the statement of the theorem in the general case where $|G|$ is invertible in $\mathbb{F}$. It was shown independently by Fogarty in [14] and Fleischmann in [12]. Then, Benson simplified the proof of Fogarty using the following elegant lemma (see [8, Section 3.8.]).

Lemma 3.1 *Let A be a commutative ring with unity, and G be a finite group of automorphisms of A. If $|G|$ is invertible in A, and I is a G-stable ideal in A, then*

$$I^{|G|} \subseteq I^G A,$$

where I^G denote the subset of G-invariants in I.

Proof. Consider the set $\{f_g \,|\, g \in G\}$ consisting of $|G|$-many elements of I indexed by the group elements. For every $h \in G$, we have the following identity

$$\prod_{g\in G}(hg(f_g) - f_g) = 0.$$

Expanding each component of this product and summing over all $h \in G$, we obtain that

$$\sum_{S\subseteq G}(-1)^{|G\setminus S|}\left[\left(\sum_{h\in G}\prod_{g\in S} h(gf_g)\right)\left(\prod_{g\in G\setminus S} f_g\right)\right] = 0$$

where S corresponds to a subset of G in each case of the sum. Note that when $S = \emptyset$, the term is

$$\pm|G|\prod_{g\in G} f_g$$

and all other terms lie in $I^G A$ because $\sum_{h\in G}\prod_{g\in S} h(gf_g)$ is in the image of the transfer Tr^G and I is a G-stable ideal. Thus,

$$\pm|G|\prod_{g\in G} f_g \in I^G A.$$

Since $|G|$ is invertible in $\mathbb{F}$, it follows that $\prod_{g\in G} f_g \in I^G A$. □

The following is an important object in invariant theory. Benson used this concept in the proof of the Theorem 3.2 below.

Definition. The ideal of $\mathbb{F}[V]$ generated by the positive degree polynomials in $\mathbb{F}[V]^G$ is called the *Hilbert ideal* and denoted by $\mathfrak{h}$, i.e.,

$$\mathfrak{h} = \langle\, f \in \mathbb{F}[V]^{G,+} \,\rangle \leq \mathbb{F}[V].$$

Theorem 3.2 *For a representation V of a finite group G, if $|G|$ is invertible in $\mathbb{F}$, then $\mathbb{F}[V]^G$ is generated by polynomials of degree at most $|G|$. In particular,*

$$\beta(G) \leq |G|.$$

Proof. Put $A = \mathbb{F}[V]$ and $I = \mathbb{F}[V]^+$ in Lemma 3.1. Thus, $(\mathbb{F}[V]^+)^{|G|} \subseteq \mathfrak{h}$. We claim that the Hilbert ideal $\mathfrak{h}$ is generated by polynomials of degree at most $|G|$. Since $\mathbb{F}[V]$ is a Noetherian ring, there are finitely many invariants $f_1, \ldots, f_r$ which generate $\mathfrak{h}$. Suppose that $f_1, \ldots, f_r$ is a minimal generating set for $\mathfrak{h}$. If the degree of f_i is greater than $|G|$ for some i, then

$$f_i = \sum_{j=1}^{n} f_{ij} x_j$$

for some $f_{ij} \in \mathbb{F}[V]$. So, $\deg(f_{ij}) \geq |G|$ and $f_{ij} \in \mathfrak{h}$ by Lemma 3.1. Since $\deg(f_{ij}) < \deg(f_i)$, for each j, f_{ij} is in the ideal of $\mathbb{F}[V]$ generated by the set $\{f_1, \ldots, \hat{f}_i, \ldots, f_r\}$ obtained by omitting f_i. It contradicts with the minimality of the generating set. Thus, the Noether number of the Hilbert ideal, $\beta(\mathfrak{h}) = |G|$.

Now, consider an invariant f of degree $> |G|$. Then $f \in \mathfrak{h}$ by Lemma 3.1. Thus,

$$f = \sum_{i=1}^{r} k_i f_i,$$

where k_i is a polynomial in $\mathbb{F}[V]^+$ and $f_i \in \mathbb{F}[V]^G$. Since $|G|$ is invertible, by the

Reynolds operator, we have

$$\begin{aligned} f &= \frac{1}{|G|}\sum_{j=1}^{|G|} g_j(f) \\ &= \frac{1}{|G|}\sum_{j=1}^{|G|}\sum_{i=1}^{r} g_j(k_i f_i) \\ &= \frac{1}{|G|}\sum_{j=1}^{|G|}\sum_{i=1}^{r} g_j(k_i) f_i \\ &= \frac{1}{|G|}\sum_{i=1}^{r} f_i\big(\sum_{j=1}^{|G|} g_j(k_i)\big) \end{aligned}$$

Since $\sum_{j=1}^{|G|} g_j(k_i) \in \mathbb{F}[V]^{G,+}$ for each i, f cannot be in a minimal generating set of $\mathbb{F}[V]^G$. □

Definition. The upper bound given in Theorem 3.2 is called the *Noether's bound*.

In the modular case, Noether's bound does not hold. By Richman in [36], the vector invariant ring $\mathbb{F}[mV_2]^G$ of the cyclic group of order p needs a generator of degree $m(p-1)$. Thus, it shows that the Noether bound does not satisfied for decomposable representations mV_2 of dimension large enough. As a more explicit example:

Example 3.1. Consider the representation $C_2 \hookrightarrow GL_6(V)$ given by the permutation matrix

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

If the characteristic is different from 2, then the invariant ring $\mathbb{F}[x_1, y_1, x_2, y_2, x_3, y_3]^{C_2}$

is generated by

$$\begin{aligned} f_i &= x_i + y_i \text{ for } i \in \{1,2,3\}, \\ h_i &= x_i y_i \text{ for } i \in \{1,2,3\}, \\ u_i &= x_j x_k + y_j y_k \text{ for distinct } i,j,k \in \{1,2,3\}. \end{aligned}$$

But in our case, when $\text{char}(\mathbb{F}) = 2$, since

$$x_1x_2x_3 + y_1y_2y_3 = \frac{1}{2}(f_1f_2f_3 - u_1f_1 - u_2f_2 - u_3f_3)$$

is not defined, the following cubic polynomial is required for the generating set

$$v = x_1x_2x_3 + y_1y_2y_3.$$

Now, we will consider a new structure defined above and which is similar to the invariant ring, Hilbert ideal. In the proof of Theorem 3.2, we also showed the following result.

Corollary 3.3 *For non-modular representations, the Hilbert ideal $\mathfrak{h}$ is generated by polynomials of degree at most the group order.*

Even though the vector invariants $\mathbb{F}[mV_2]^G$ have generators of arbitrary large degrees, the corresponding Hilbert ideal needs only the generators of degree at most the group order (proved in [43]) as shown in the following example.

Example 3.2. We consider the representation given in Example 3.1. In this example, it is required a generator v for $\mathbb{F}[V]^G$ when $\text{char}(\mathbb{F}) = 2$. We can write v as follows:

$$\begin{aligned} v &= x_1x_2x_3 + y_1y_2y_3 \\ &= f_1f_2f_3 + x_2y_3f_1 + x_3u_3 + y_2u_2 \end{aligned}$$

Hence, it is in the Hilbert ideal $\mathfrak{h} = \langle f_1, f_2, f_3, h_1, h_2, h_3, u_1, u_2, u_3 \rangle$. Therefore, $\mathfrak{h}$ satisfies Noether bound.

As a generalization of the Noether bound for the invariant ring, it is conjectured that the Noether bound holds for the Hilbert ideal (see [8, Conjecture 3.8.6 (b)]).

Conjecture 3.4 (Hilbert Ideal Conjecture) *Let V be a representation of a finite group G. Then the corresponding Hilbert ideal is generated by polynomials of degree at most $|G|$.*

3.2 Recent Studies on the Hilbert Ideal

The Hilbert ideal conjecture is an interesting problem in the invariant theory. There are many studies about this conjecture. However, the conjecture is proved only for special cases in these studies. Until now, it has been not achieved to show it for all representations. In this section, we will list the studies about the Hilbert ideal supporting the conjecture.

1. Due to Noether, Fleischmann and Fogarty, the conjecture holds for non-modular representations (Corollary 3.3).
2. Due to Fleischmann, the conjecture holds for permutation representations ([12, Theorem 4.1]).
3. Due to Shank and Wehlau, the conjecture holds for vector invariants $\mathbb{F}[mV_2]^{C_p}$ of the cyclic group C_p ([43]).
4. Due to Sezer, the conjecture holds for the indecomposable representations of C_p ([38]).
5. Due to Sezer and Shank, the conjecture holds for some given examples of decomposable representations of C_p ([39]).
6. Due to a result of Wehlau, the conjecture holds for given examples of decomposable representations of C_p ([53]).

7. Due to Erdemirci Erkuş and Madran, the conjecture holds for indecomposable representations of C_{p^2} having dimension ≤ 4 or $\geq p^2 - 2p$ (see Section 3.3).

3.3 Hilbert Ideal of the Cyclic Group C_{p^2}

Beside the cyclic group C_p, the cyclic group C_{p^2} of order p^2 and its invariants were studied especially for indecomposable representations and for $p+1$-dimensional representations (see [30], [43]). Now, we examine the Hilbert ideal of the group C_{p^2} for indecomposable representations in two different approaches. In Section 3.3.1, we give the first approach by considering the representations in dimension $p+1$. Here, we obtain invariants in an inductive way, increasing the degree of a representation and identifying the invariants of the extended representation, $V_{n+1} \supset V_n$. Then, Section 3.3.2 include the other approach given for a more general case. Although the result of the second one covers the result of the first one, we provide this direct approach to initiate an inductive argument which we expect to provide a more general and complete result.

In the rest of this section, let $G = C_{p^2}$ be the cyclic group of order p^2 and H be its subgroup of order p. Let V_n denote the n-dimensional indecomposable faithful representation of G. If the dimension is clear in the context, we will denote it by V for simplicity of notations. For a faithful indecomposable representation, n must be in the interval $p < n \leq p^2$ (see Lemma 2.11). Because of this constraint, our first step starts with the representations in $p+1$-dimension.

For the representation V of G, we consider the corresponding polynomial ring $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ with indeterminates $x_1, \ldots, x_n$. If ρ is the faithful representation of G with $\rho(\sigma) = [\alpha_{i,j}(\sigma)] \in \mathrm{GL}(n, \mathbb{F})$ for all $\sigma \in G$, then the

action of G on $\mathbb{F}[V]$ is given by

$$\begin{bmatrix} \sigma \cdot x_1 \\ \sigma \cdot x_2 \\ \vdots \\ \sigma \cdot x_n \end{bmatrix} = \begin{bmatrix} \alpha_{1,1}(\sigma) & \alpha_{1,2}(\sigma) & \dots & \alpha_{1,n}(\sigma) \\ \alpha_{2,1}(\sigma) & \alpha_{2,2}(\sigma) & \dots & \alpha_{2,n}(\sigma) \\ \vdots & \vdots & & \vdots \\ \alpha_{n,1}(\sigma) & \alpha_{n,2}(\sigma) & \dots & \alpha_{n,n}(\sigma) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Along this section, the monomial ordering is the graded reverse lex order with $x_{i+1} \succ x_i$ for $i = 1, 2, \dots, n-1$. Let σ be a generator for the group G. It is showed in Section 2.4.4 that σ has the following Jordan canonical form

$$\sigma = \begin{bmatrix} 1 & 0 & \dots 0 & 0 \\ 1 & 1 & \dots 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots 1 & 0 \\ 0 & 0 & \dots 1 & 1 \end{bmatrix}$$

and hence

$$\sigma(x_i) = \begin{cases} x_1 & \text{if } i = 1, \\ x_i + x_{i-1} & \text{if } 2 \le i \le n. \end{cases}$$

Setting $\Delta := \sigma - 1$, we obtain

$$\Delta(x_i) = \begin{cases} 0 & \text{if } i = 1, \\ x_{i-1} & \text{if } 2 \le i \le n. \end{cases}$$

The main aim of the section is to prove the Hilbert ideal conjecture for indecomposable representations of the cyclic group G. For this, it is essential to know about the generators of the invariant ring $\mathbb{F}[V]^G$. Therefore, the following theorem of Symonds given in [48] is a necessary tool in the section. We restate the theorem in our notations as follows:

Theorem 3.5 *The invariant ring $\mathbb{F}[V]^G$ is generated by the G-norm $\mathrm{N}^G(x_n)$ and invariants of degree less than p^2 modulo modules which are projective relative to the proper subgroups of G.*

Corollary 3.6 *The invariant ring $\mathbb{F}[V]^G$ is generated by the norm $\mathrm{N}^G(x_n)$, invariants of degree less than p^2, and the image of the relative transfer Tr_H^G.*

Proof. Since the only nontrivial proper subgroup of G is H and $\mathrm{Im}\,\mathrm{Tr}^G \subseteq \mathrm{Im}\,\mathrm{Tr}_H^G$, we obtain that the fixed points of the projective modules not in the ideal generated by G-norms are in the image of the relative transfer Tr_H^G by Lemma 2.15. Then $\mathbb{F}[V]^G$ is generated by the G-norm $\mathrm{N}^G(x_n)$, invariants of degree less than p^2, and the image of the relative transfer Tr_H^G. □

By the previous result, in order to prove the Hilbert ideal conjecture, the only obstacle may be the image of relative transfer. Thus, in two approaches, we try to show that the image of the relative transfer can be written with elements of Hilbert ideal of degree at most the group order, p^2. For the rest of the section, the Hilbert ideal $\mathfrak{h}$ denotes the ideal in $\mathbb{F}[V]$ generated by the G-invariants in positive degree.

3.3.1 Hilbert Ideal in $\mathbb{F}[V_{p+1}]$

Suppose that the dimension of the representation V is $p+1$. Let A denote the proper subalgebra $\mathbb{F}[x_1, x_2, \ldots, x_p]$ of $\mathbb{F}[V]$. Note that by the canonical form of σ, the generator σ^p of the group H has the following form in $p+1$ dimension

$$\sigma^p = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & 1 \end{bmatrix}.$$

Then, it can immediately be seen that every element of A is H-invariant since $x_1, x_2, \ldots, x_p \in \mathbb{F}[V]^H$.

Now, we construct an auxiliary polynomial in $\mathbb{F}[V]$ as a polynomial generated by H-transfers given in [38].

Construction of the Polynomial: Consider a monomial $m = w_1 w_2 \cdots w_{p-1}$ in A of degree $p-1$. For any subset S of $\{1, 2, \ldots, p-1\}$, let

$$m_S := \prod_{j \in S} w_j$$

and let S' denote the complement of S in $\{1, 2, \ldots, p-1\}$. For such a monomial m and a polynomial f in $\mathbb{F}[V]^H$, we define

$$F_{m,f} = \sum_{S \subseteq \{1,2,\ldots,p-1\}} (-1)^{|S|} m_{S'} \mathrm{Tr}_H^G(f m_S). \tag{3.1}$$

Note that the polynomial $F_{m,f}$ is in the Hilbert ideal $\mathfrak{h}$ since $m_S \in \mathbb{F}[V]^H$ for each $S \subseteq \{1, 2, \ldots, p-1\}$ and the image of the relative transfer Tr_H^G lies in $\mathbb{F}[V]^G$.

Other Constructions: For the monomial $m = w_1 w_2 \cdots w_{p-1}$, define the following monomial

$$\Delta_m := \Delta(w_1)\Delta(w_2)\cdots\Delta(w_{p-1})$$

of degree $p-1$ or zero. Let B be the subalgebra $\mathbb{F}[x_1, x_2, \ldots, x_{p-1}]$ of $\mathbb{F}[V]$, and B_i denote the vector subspace of B consisting of homogeneous polynomials of degree i. Thus, we obtain that Δ_m is either 0 or a monomial in B_{p-1}.

Recall that we denote the leading term of a polynomial f with $\mathrm{LT}(f)$, leading monomial of f with $\mathrm{LM}(f)$, and leading coefficient of f with $\mathrm{LC}(f)$.

Some technical properties of the polynomial constructed above is given in the following two deductions. Indeed, these two results can be derived from [38, Lemma 2, Lemma 3] considering the action on the algebra A instead of $\mathbb{F}[V]$.

Lemma 3.7 *With the above notations, the polynomial $F_{m,f}$ given in (3.1) has the following properties:*

(i) $F_{m,f} = 0$ *if* $\Delta_m = 0$,

(ii) $\mathrm{LT}(F_{m,f}) = -\Delta_m \mathrm{LT}(f)$ *if* $\Delta_m \neq 0$,

(iii) $F_{m,f} \in B_{p-1} \cdot \mathbb{F}[V]$.

Proof. Expand the product $\prod_{i=1}^{p-1}\big(w_i - \sigma^\ell(w_i)\big)$ and apply σ^ℓ. Then, we obtain

$$\sigma^\ell(f)\Big(\prod_{i=1}^{p-1}\big(w_i - \sigma^\ell(w_i)\big)\Big) = \sum_{S\subseteq\{1,2,\dots,p-1\}} (-1)^{|S|} m_{S'}\sigma^\ell(fm_S)$$

for each $0 \le \ell \le p-1$. Since the relative transfer is $\mathrm{Tr}_H^G = \sum_{\ell=0}^{p-1}\sigma^\ell$, summing over ℓ yields

$$\sum_{\ell=0}^{p-1}\sigma^\ell(f)\Big(\prod_{i=1}^{p-1}\big(w_i - \sigma^\ell(w_i)\big)\Big) = F_{m,f}. \tag{3.2}$$

If $\Delta_m = 0$, then $\Delta(w_i) = 0$ for some $1 \le i \le p-1$. Therefore, by the definition of Δ, $w_i - \sigma^\ell(w_i) = 0$ for all $\ell = 0, 1, \dots, p-1$. Thus, the summands in the polynomial $F_{m,f}$ become zero. So the property (i) is satisfied.

Now assume that $\Delta_m \neq 0$. From the identity

$$1 - \sigma^\ell = (1 + \sigma + \sigma^2 + \cdots + \sigma^{\ell-1})\cdot(1-\sigma),$$

we obtain

$$w_i - \sigma^\ell(w_i) = (1 + \sigma + \sigma^2 + \cdots + \sigma^{\ell-1})(-\Delta(w_i)). \tag{3.3}$$

Since the action of σ respects the monomial order, in the sense that $\mathrm{LT}(\sigma(f)) = \mathrm{LT}(f)$, we get

$$\mathrm{LT}\big(w_i - \sigma^\ell(w_i)\big) = -\ell\Delta(w_i).$$

Hence, the leading term of $\sigma^\ell(f)\Big(\prod_{i=1}^{p-1}\big(w_i - \sigma^\ell(w_i)\big)\Big)$ is computed as

$$\mathrm{LT}(f)(-\ell)^{p-1}\prod_{i=1}^{p-1}\Delta(w_i) = \mathrm{LT}(f)\ell^{p-1}\Delta_m.$$

Summing over ℓ proves the part (ii) since $\sum_{\ell=0}^{p-1}\ell^{p-1} = -1$ (Lemma 2.3).

By the equation (3.3), we can say that the variables that appear in $w_i - \sigma^\ell(w_i)$ are in the algebra B. Then, if $\Delta_m \neq 0$, the product $\prod_{i=1}^{p-1}\big(w_i - \sigma^\ell(w_i)\big)$ is of degree $p-1$. Thus, the product is in B_{p-1}. Hence, $F_{m,f} \in B_{p-1}\cdot\mathbb{F}[V]$, completing the proof. □

Lemma 3.8 *The subspace B_{p-1} is in the Hilbert ideal $\mathfrak{h}$.*

Proof. Suppose, for contradiction that $B_{p-1} \setminus \mathfrak{h}$ is nonempty. Let f be a polynomial in $B_{p-1} \setminus \mathfrak{h}$ with minimal leading monomial u. Then u is not in $\mathfrak{h}$. Indeed, if u were in $\mathfrak{h}$, the polynomial $f - \mathrm{LC}(f)u$ would be in $B_{p-1} \setminus \mathfrak{h}$, and this would contradict with the minimality of f. Moreover, since $u \in B_{p-1}$, there exists a monomial $m \in A$ such that $\Delta_m = u$. Now, consider the polynomial $F_{m,1}$. By Lemma 3.7, $\mathrm{LT}(F_{m,1}) = -\Delta_m = -u$. Therefore, the leading monomial of $u + F_{m,1}$ is strictly smaller than u. Since $F_{m,1} \in \mathfrak{h}$, we have $u + F_{m,1} \in B_{p-1} \setminus \mathfrak{h}$. But again this contradicts to the minimality of f. Therefore $B_{p-1} \subseteq \mathfrak{h}$. □

For $k \in \mathbb{Z}^+$, let

$$\mathfrak{h}_{\leq k} := \langle f \in \mathfrak{h} \mid \deg(f) \leq k \rangle$$

denote the ideal of $\mathbb{F}[V]$ generated by polynomials in $\mathfrak{h}$ of degree at most k. As a consequence of Lemma 3.7 and Lemma 3.8, we can deduce the following desired result.

Proposition 3.9 *The polynomial $F_{m,f}$ is in the ideal $\mathfrak{h}_{\leq p^2}$.*

Proof. It follows from Lemma 3.7 (iii) and Lemma 3.8. □

By the above representation of σ^p, we have

$$\sigma^p(x_i) = \begin{cases} x_i & \text{if } 1 \leq i \leq p, \\ x_1 + x_i & \text{if } i = p+1. \end{cases}$$

Therefore, the invariant ring $\mathbb{F}[V]^H$ is generated by $x_1, x_2, \ldots, x_p, \mathrm{N}^H(x_{p+1})$:

$$\mathbb{F}[V]^H \cong \mathbb{F}[x_1, x_2, \ldots, x_p, \mathrm{N}^H(x_{p+1})].$$

Notation 3.1. We use the following notations for simplicity.

(i) For a polynomial $f \in \mathbb{F}[V]$, $\deg_{x_i}(f)$ denotes the maximum degree of f in x_i.

(ii) For a monomial $m \in \mathbb{F}[V]$, $\deg_A(m)$ denotes the total degree of m with respect to variables in A.

Proposition 3.10 *If a polynomial f and a monomial m are given as above, $\mathrm{Tr}_H^G(fm)$ is in the ideal $\mathfrak{h}_{\leq p^2}$.*

Proof. We can rewrite the polynomial $F_{m,f}$ as:

$$F_{m,f} = \mathrm{Tr}_H^G(fm) + \sum_{S \subsetneq \{1,2,\ldots,p-1\}} (-1)^{|S|} m_{S'} \mathrm{Tr}_H^G(fm_S).$$

Notice that $\deg(fm_S)$ is strictly less than $\deg(fm)$ for each proper subset S of $\{1, 2, \ldots, p-1\}$. If $\deg_{x_{p+1}}(\mathrm{Tr}_H^G(fm_S)) > p^2$, then we can reduce it by dividing $\mathrm{N}^G(x_{p+1})$ using Lemma 2.16. Otherwise, $\deg_{x_{p+1}}(\mathrm{Tr}_H^G(fm_S)) \leq p^2 - p$, so it can be written as a product of an H-invariant (possibly containing $\mathrm{N}^H(x_{p+1})$) and a monomial of degree at least p in A. Therefore, using induction on $\deg(fm)$, we obtain that $\mathrm{Tr}_H^G(fm) \in \mathfrak{h}_{\leq p^2}$. □

Definition. A polynomial $f \in \mathbb{F}[V]^H$ of degree greater than p^2 is called *an invariant with enough invariants in* $A = \mathbb{F}[x_1, \ldots, x_p]$, or shortly said it *has enough invariants in* A if $f = \sum_{i=1}^{\ell} f_i m_i$ such that for each i,

(i) m_i is a monomial in A with $\deg(m_i) = p - 1$,

(ii) $f_i \in \mathbb{F}[V]^H$.

Lemma 3.11 *If f has enough invariants in A, then $\mathrm{Tr}_H^G(f)$ is in the ideal $\mathfrak{h}_{\leq p^2}$.*

Proof. By the linearity of the relative transfer, we have

$$\mathrm{Tr}_H^G(f) = \mathrm{Tr}_H^G(\sum_{i=1}^{\ell} f_i m_i) = \sum_{i=1}^{\ell} \mathrm{Tr}_H^G(f_i m_i).$$

Thus, by Proposition 3.10, we obtain the result. □

Proposition 3.12 *If $f \in \mathbb{F}[V]^H$ is of degree greater than p^2 and $\deg_{x_{p+1}}(f) < p^2$, then f has enough invariants in A.*

Proof. Suppose that $f \in L$ is of degree greater than p^2 and $\deg_{p+1}(f) < p^2$. Then $\deg_{p+1}(f)$ is a multiple of p because $\deg_{x_{p+1}}(\mathrm{N}^H(x_{p+1})) = p$. Therefore, f can be

written as a sum of polynomials which are a product of H-norm, $\mathrm{N}^H(x_{p+1})$ and some monomial of degree at least p in A. Thus, f has enough invariants in A. □

Proposition 3.13 *For any $f \in \mathbb{F}[V]^H$, the image of the relative transfer $\mathrm{Tr}_H^G(f)$ is in the ideal $\mathfrak{h}_{\leq p^2}$.*

Proof. If $f \in L$ is of degree greater than p^2 and $\deg_{x_{p+1}}(f) < p^2$, then by Proposition 3.12 and Lemma 3.11, we have $\mathrm{Tr}_H^G(f) \in \mathfrak{h}_{\leq p^2}$. If $\deg_{x_{p+1}}(f) \geq p^2$, the polynomial f has the form $f = \mathrm{N}^G(x_{p+1})g + h$ for some polynomials $g, h \in \mathbb{F}[V]^H$ with $\deg_{x_{p+1}}(h) < p^2$ by Lemma 2.16. Thus, h and $\mathrm{N}^G(x_{p+1})$ are in $\mathfrak{h}_{\leq p^2}$. Hence so is f. Finally, if $\deg(f) \leq p^2$, the result is clearly true. □

Hence, we obtain the following main result in this section.

Theorem 3.14 *For an indecomposable representation V_{p+1} of G, the corresponding Hilbert ideal $\mathfrak{h}$ is generated by invariants of degree at most p^2.*

Proof. By Corollary 3.6, $\mathbb{F}[V]^G$ is generated by the norm $\mathrm{N}^G(x_{p+1})$, invariants of degree less than p^2, and the image of the relative transfer Tr_H^G. Hence by Proposition 3.13, we get the desired result. □

3.3.2 Hilbert Ideal in $\mathbb{F}[V_n]$

In this section, we analyze the Hilbert ideal for a more general case. For the rest of this section, let V denote the n-dimensional indecomposable faithful representation of the cyclic group G of order p^2.

We need two technical results from [13]. The first one is obtained by taking $G = C_{p^2}$ with H as the nontrivial proper subgroup in [13, Lemma 2.2].

Lemma 3.15 *If $m = ww_0 \cdots w_{p^2-1}$ is a monomial in $\mathbb{F}[V]$ with degree greater than p^2, then*

$$\mathrm{Tr}^G(m) = \sum_{S \subsetneq \{0,1,\ldots,p^2-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(w_i) \mathrm{Tr}^G(w \prod_{i \in S} w_i).$$

Proof. For fixed $\ell \in \{0, 1, \ldots, p^2 - 1\}$, consider the following equality

$$\prod_{i=0}^{p^2-1} (\sigma^i(w_i) - \sigma^\ell(w_i)) = 0.$$

Expanding this eqution, we obtain that

$$\sum_{S \subseteq \{0,1,\ldots,p^2-1\}} (-1)^{|S|} \prod_{i \notin S} \sigma^i(w_i) \Big(\prod_{i \in S} \sigma^\ell(w_i) \Big) = 0.$$

Multiplying by $\sigma^\ell(w)$ for the fixed ℓ and summation over $\ell \in \{0, 1, \ldots, p^2 - 1\}$ gives

$$\sum_{\ell=0}^{p^2-1} \sigma^\ell(w w_0 w_1 \cdots w_{p^2-1}) + \sum_{S \subsetneq \{0,1,\ldots,p^2-1\}} (-1)^{|S|} \prod_{i \notin S} \sigma^i(w_i) \Big(\sum_{\ell=0}^{p^2-1} \sigma^\ell(w) \prod_{i \in S} \sigma^\ell(w_i) \Big) = 0.$$

It means that

$$\mathrm{Tr}^G(m) = \sum_{S \subsetneq \{0,1,\ldots,p^2-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(w_i) \mathrm{Tr}^G(w \prod_{i \in S} w_i).$$

□

Lemma 3.16 *If $f, f_0, \ldots, f_{p-1} \in \mathbb{F}[V]^H$, then*

$$\mathrm{Tr}_H^G(f f_0 f_1 \cdots f_{p-1}) = \sum_{S \subsetneq \{0,1,\ldots,p-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(f_i) \mathrm{Tr}_H^G(f \prod_{i \in S} f_i).$$

Proof. Consider the equality

$$\prod_{i=0}^{p-1} (\sigma^i(f_i) - \sigma^\ell(f_i)) = 0.$$

Expanding and multiplying by $\sigma^\ell(f)$, we obtain that

$$\sum_{S \subseteq \{0,1,\ldots,p-1\}} (-1)^{|S|} \prod_{i \notin S} \sigma^i(f_i) \Big(\prod_{i \in S} \sigma^\ell(f_i) \Big) \sigma^\ell(f) = 0.$$

Summation over $\ell \in \{0, 1, \dots, p-1\}$ gives

$$\sum_{i=0}^{p-1} \sigma^{\ell}(f f_0 f_1 \cdots f_{p-1}) + \sum_{S \subsetneq \{0,1,\dots,p-1\}} (-1)^{|S|} \prod_{i \notin S} \sigma^i(f_i) \Big(\sum_{\ell=0}^{p-1} \sigma^{\ell}(f) \prod_{i \in S} \sigma^{\ell}(f_i) \Big) = 0.$$

It means that

$$\mathrm{Tr}_H^G(f f_0 f_1 \cdots f_{p-1}) = \sum_{S \subsetneq \{0,1,\dots,p-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(f_i) \mathrm{Tr}_H^G(f \prod_{i \in S} f_i).$$

□

Remark. The previous lemma says that the image of the product of at least p-many H-invariant polynomials under the relative transfer can be written as a combination of some polynomials in $\mathfrak{h}$ of degree less than the first polynomial. Indeed, the lemmas provide a reduction in the degree of the given transfer image of polynomials.

Proposition 3.17 *For any polynomial $f \in \mathbb{F}[V]$,*

$$\mathrm{Tr}^G(f) \in \mathfrak{h}_{\leq p^2},$$

i.e., the image of the full transfer Tr^G is in the ideal $\mathfrak{h}_{\leq p^2}$.

Proof. Suppose that $\deg(f) > p^2$ because otherwise the result is trivial. Without loss of generality, we can assume that f is a monomial in $\mathbb{F}[V]$ by the linearity of the transfer map. Then, we can write $f = w w_0 w_1 \cdots w_{p^2-1}$ for some variables $w_0, \dots, w_{p^2-1}$ and some monomial w. By using Lemma 3.15, we obtain that

$$\mathrm{Tr}^G(f) = \sum_{S \subsetneq \{0,1,\dots,p^2-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(w_i) \mathrm{Tr}^G(w \prod_{i \in S} w_i).$$

Note that $\deg(\mathrm{Tr}^G(w \prod_{i \in S} w_i))$ is strictly less than $\deg(\mathrm{Tr}^G(f))$. Hence $\mathrm{Tr}^G(f)$ is either in $\mathfrak{h}_{\leq p^2}$ or in the ideal $\langle \mathrm{Tr}^G(f') \mid \deg(f') < \deg(f) \rangle$ for some monomial f' in $\mathbb{F}[V]$. Therefore, by using induction on $\deg(f)$, we obtain the desired result. □

Now, we try to deduce the same result for the image of the relative transfer.

Proposition 3.18 *Let $g = \prod_{i=0}^{k} f_i$, where each f_i is H-invariant of degree at most p for some k. Then*

$$\mathrm{Tr}_H^G(g) \in \langle\ \mathfrak{h}_{\leq p^2}, \mathrm{Tr}_H^G(g') \mid \deg(g') < \deg(g) \text{ and } g' \in \mathbb{F}[V]^H\ \rangle.$$

Proof. If $\deg(g) \leq p^2$, then there is nothing to prove. Otherwise, we obtain that k is at least p. That is, g is product of at least $p+1$ many H-invariants of degree at most p. Let $f = f_p f_{p+1} \cdots f_k$. Therefore from Lemma 3.16, we obtain that

$$\mathrm{Tr}_H^G(g) = \sum_{S \subsetneq \{0,1,\ldots,p-1\}} (-1)^{|S|+1} \prod_{i \notin S} \sigma^i(f_i) \mathrm{Tr}_H^G(f \prod_{i \in S} f_i).$$

Note that $\deg(\mathrm{Tr}_H^G(f \prod_{i\in S} f_i))$ is strictly less than $\deg(\mathrm{Tr}_H^G(g))$ for any proper subset S. Hence $\mathrm{Tr}_H^G(g)$ is either in $\mathfrak{h}_{\leq p^2}$ or in the ideal

$$\langle \mathrm{Tr}_H^G(g') \mid \deg(g') < \deg(g) \rangle$$

for H-invariant g' as a product of some f_i's. □

Remark. The result is true for any linear combination of the polynomials satisfying the hypothesis of Proposition 3.18 by linearity of the transfer. From now on, we will use the same approach for the simplicity of the notations.

Corollary 3.19 *If $g = \prod_{i=0}^{k} f_i$ with $f_i \in \mathbb{F}[V]^H$ of degree at most p, then*

$$\mathrm{Tr}_H^G(g) \in \mathfrak{h}_{\leq p^2}.$$

Proof. The result directly follows from Proposition 3.18 by induction on $\deg(g)$. □

The following result is given by Wehlau in [53]. Its difference from the result of Symonds given in Theorem 3.5 is that it is true for any representation not only for indecomposable one. Thus, it is suitable for Proposition 3.21 below since $\mathbb{F}[V]$ has decomposable structure as $\mathbb{F}H$-modules.

Theorem 3.20 *[53, Theorem 9.15] The invariant ring $\mathbb{F}[V]^H$ is generated by the H-norms, a finite set of H-transfers and a finite set of integral invariants.*

Proposition 3.21 *If the degrees of integral invariants in a generating set of* $\mathbb{F}[V]^H$ *are at most* p*, then the image of the relative transfer* Tr_H^G *is in the ideal* $\mathfrak{h}_{\leq p^2}$*.*

Proof. Suppose that the degrees of the integral invariants are at most p. Then by Corollary 3.19, the relative transfers of the integral invariants, the H-norms and their products are in $\mathfrak{h}_{\leq p^2}$. Now, let $\langle \mathrm{ImTr}^H \rangle$ be the ideal of $\mathbb{F}[V]^H$ generated by H-transfers. Let f be any element of $\langle \mathrm{ImTr}^H \rangle$. Then $f = h\mathrm{Tr}^H(g)$ for some $h \in \mathbb{F}[V]^H$ and $g \in \mathbb{F}[V]$. So we can write $f = \mathrm{Tr}^H(hg)$ since h is H-invariant. Therefore, $\mathrm{Tr}_H^G(f) = (\mathrm{Tr}_H^G \circ \mathrm{Tr}^H)(hg) = \mathrm{Tr}^G(hg)$. By Proposition 3.17, the image of the full transfer Tr^G is in $\mathfrak{h}_{\leq p^2}$. Thus, also the relative transfer of the ideal $\langle \mathrm{ImTr}^H \rangle$ is there. Hence the image of the relative transfer Tr_H^G is in the ideal $\mathfrak{h}_{\leq p^2}$. □

Remark. The result of Proposition 3.21 is satisfied in all known examples even if the hypothesis does not hold. Actually, there is an integral invariant of degree 6 for the case mV_4 in the list of Wehlau [53], but this invariant is not necessary for $p = 5$. For this particular representation of degree $4m$, p cannot be 2 or 3. Thus, the results of Proposition 3.21 and Corollary 3.22 are believed to be valid for more general cases then they appear.

Corollary 3.22 *If the degrees of integral invariants are at most* p *or the ones with degree greater than* p *are in the ideal* $\langle \mathrm{Im}\,\mathrm{Tr}^H \rangle$*, then the Hilbert ideal* $\mathfrak{h}$ *is generated by invariants of degree at most* p^2*.*

Proof. By Theorem 3.5, $\mathbb{F}[V]^G$ is generated by G-norm $\mathrm{N}^G(x_n)$, invariants of degree less than p^2, and the image of the relative transfer Tr_H^G. Thus, Proposition 3.21 gives the desired result. □

Let V be an $\mathbb{F}H$-module with the decomposition

$$V = V_{n_1} \oplus V_{n_2} \oplus \cdots V_{n_r}$$

into indecomposable $\mathbb{F}H$-modules by Lemma 2.13. Then $\mathbb{F}[V]$ has an $\mathbb{N}^r$-grading

given by

$$\mathbb{F}[V]_{d_1,d_2,\ldots,d_r} = \mathbb{F}[V_{n_1}]_{d_1} \otimes \mathbb{F}[V_{n_2}]_{d_2} \otimes \cdots \otimes \mathbb{F}[V_{n_r}]_{d_r},$$

where $\mathbb{F}[V_{n_i}]_{d_i}$ denotes the subspace of homogeneous polynomials of degree d_i for the vector space V_{n_i} of dimension n_i. Let z_i be an $\mathbb{F}H$-module generator of the dual space $V_{n_i}^*$ for $i = 1, 2, \ldots, r$. Define the norm of z_i by $N_i = \prod_{\ell=0}^{p-1} \sigma^{\ell p}(z_i)$ and define $\mathbb{F}[V]^\sharp$ to be the ideal of $\mathbb{F}[V]$ generated by the norms $N_1, N_2, \ldots, N_r$. The following famous result is known as the periodicity theorem (see [20, Lemma 2.9, 2.10]).

Theorem 3.23 (Periodicity Theorem) *The ideal $\mathbb{F}[V]^\sharp$ is a direct summand of the $\mathbb{F}H$-module $\mathbb{F}[V]$:*

$$\mathbb{F}[V] = \mathbb{F}[V]^\sharp \oplus \mathbb{F}[V]^\flat,$$

where $\mathbb{F}[V]^\flat$ is defined as the complement of $\mathbb{F}[V]^\sharp$ as $\mathbb{F}H$-modules. In particular, we obtain

$$\mathbb{F}[V]_{d_1,d_2,\ldots,d_r} = \mathbb{F}[V]^\sharp_{d_1,d_2,\ldots,d_r} \oplus \mathbb{F}[V]^\flat_{d_1,d_2,\ldots,d_r}.$$

Also, if there is an index i such that $d_i > p - n_i$, then $\mathbb{F}[V]^\flat_{d_1,d_2,\ldots,d_r}$ is a free $\mathbb{F}H$-module.

Lemma 3.24 *For $p < n \leq p^2$, V decomposes as an $\mathbb{F}H$-module*

$$rV_{k+1} \oplus (p-r)V_k,$$

where $n = kp + r$.

Proof. By the representation of σ^p:

$$\sigma^p = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \ldots & 1 & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & \ldots & 1 \end{bmatrix},$$

the corresponding Jordan canonical form consists of r-many V_{k+1} with basis elements $x_i, x_{p+i}, \dots, x_{kp+i}$ for each $i = 1, \dots, r$ and $(p-r)$-many V_k with basis elements $x_{r+i}, x_{p+r+i}, \dots, x_{(k-1)p+r+i}$ for each $i = 1, \dots, p-r$. This completes the proof. □

Lemma 3.25 *If f is an H-invariant in $\mathbb{F}[V]^\flat$ with degree greater than $p^2 - n$, then it is in the image of the H-transfer Tr^H.*

Proof. By Lemma 3.24, as an $\mathbb{F}H$-module, the decomposition of V is

$$V = rV_{k+1} \oplus (p-r)V_k$$

for $n = kp + r$. Since $r(p-(k+1)) + (p-r)(p-k) = p^2 - n$, it follows that f is an invariant in the free module which is a complement to the ideal generated by norms by the periodicity theorem. Then, the result follows from Lemma 2.15. □

Theorem 3.26 *For an indecomposable $\mathbb{F}G$-module V with $n \geq p^2 - 2p$, the corresponding Hilbert ideal $\mathfrak{h}$ is generated by invariants of degree at most p^2.*

Proof. It is enough to consider the image of the relative transfer Tr_H^G by Theorem 3.5. Moreover, by Theorem 3.20, we know that an H-invariant f is either a transfer, a norm or an integral invariant. The result is clear for the following cases: if f is in the ideal $\langle \mathrm{Im}\mathrm{Tr}^H \rangle$, by Corollary 3.22; if f is a product of some norms and integral invariants of degree $\leq p$, by Corollary 3.19; and if f is a product of some integral invariants which is not divided by any norm N_i and $\deg(f) > p^2 - n$, by Lemma 3.25. The only remaining case is to consider an invariant of degree greater than p^2 which is a product of some N_i's and some integral invariants of total degree at most $p^2 - n$. Without loss of generality, we can take $f = g \cdot h$, where h is the product of all H-norms dividing f and g is the product of integral invariants such that $\deg(g) \leq p^2 - n$. Since $\deg(f) > p^2$, we should have $\deg(h) > n \geq p^2 - 2p$. Thus, h is the product of at least $p-1$ many norms. Hence, we obtain that f is a product of at least p many H-invariants. This completes the proof by Lemma 3.16. □

Remark. Since $n \geq p+1$, for an indecomposable representation of G, we have $p+1 \geq p^2 - 2p$ for $p = 3$. Therefore, the corresponding Hilbert ideal $\mathfrak{h}$ is generated

by invariants of degree at most $p^2 = 9$. So, for the rest of the section, we can take $p \geq 5$.

We can extend our result to representations of degree at most $4p$ by using the list of generators in [53].

Theorem 3.27 *For an indecomposable $\mathbb{F}G$-module V with $p+1 \leq n \leq 4p$, the corresponding Hilbert ideal $\mathfrak{h}$ is generated by invariants of degree at most p^2.*

Proof. By Lemma 3.24, we have

$$\mathbb{F}[V] \cong \mathbb{F}[rV_{k+1} \oplus (p-r)V_k].$$

When $p+1 \leq n \leq 2p$, the result follows from the conjecture of Richman [35] which is proved by Campbell and Hughes in [3].

The integral invariants of $\mathbb{F}[rV_{k+1} \oplus (p-r)V_k]$ can be obtained from invariants of $\mathbb{C}[R_1 \oplus rR_k \oplus (p-r)R_{k-1}]^{\mathrm{SL}_2}$ by [53, Section 5]. Since $R_1 \oplus rR_k \oplus (p-r)R_{k-1}$ is a subrepresentation of $R_1 \oplus pR_k$, the invariants can be obtained by projection of invariants of $R_1 \oplus pR_k$. Complete set of generators for $k \leq 3$ are given in [53, Section 10].

If $2p < n \leq 3p$, it is sufficient to consider the invariants of $\mathbb{C}[R_1 \oplus pR_2]^{\mathrm{SL}_2}$. However, the integral invariants listed in [53, Theorem 10.5] have degrees at most 3, as required.

If $3p < n \leq 4p$, the set of covariants listed in [53, Table 10.3] have degrees at most 6. Since the polarization does not change the total degree of covariants, it follows that the degrees of generating covariants of pR_3 are at most 6. Therefore, by Corollary 3.22 if $p > 5$, we obtain the result.

The only case left is the integral invariants of $\mathbb{F}[V]^H$ when $p = 5$. If $p > 5$, $n > 3p$ so that $n \geq p^2 - 2p$. Hence, by Theorem 3.26, the corresponding Hilbert ideal is generated by invariants of degree at most p^2. This completes the proof. □

Remark. In this approach, we have used the idea of *vector invariants*. So, studying vector invariants for C_p, the cyclic group of order p, is still important in

modular invariant theory. We expect that, the only disadvantage of this approach, "finding generators for each dimension explicitly", can be avoided with a better understanding of vector invariants.

Chapter 4

Generalized Invariants

In this chapter, we define *generalized invariants* of any finite group as a new concept in the literature. They are appeared as an extension of the notion of invariants. They give a new point of view to modular invariant theory. We consider general and structural properties of generalized invariants. Then, we examine them in non-modular case.

4.1 History of Generalized Invariants

The concept of generalized invariants is firstly introduced by Kac-Peterson in [21] as *ideal of generalized invariants*. However, the ideal of generalized invariants was defined only for pseudo-reflection groups in [21] and used the same definition in an other study [28]. In this section, we give Kac-Peterson's definition in order to show that our definition is distinct from it.

Definition. A linear automorphism $s : V \to V$ is said to be a *pseudoreflection* if

(i) $s \neq 1$,

(ii) the order of s is finite,

(iii) s fixes a hyperplane of s.

Definition. Let $\rho : G \hookrightarrow \mathrm{GL}(V)$ be a faithful representation. The group G is called a *pseudoreflection group* if G is generated by its pseudoreflections. Pseudoreflection groups are a generalization of reflection groups. Sometimes, the term reflection is used for a pseudoreflection.

Let $s : V \to V$ be a pseudoreflection with hyperplane $H_s = \mathrm{Ker}(1 - s)$. Then $\mathrm{Im}(1 - s)$ is a 1-dimensional subspace of V. Thus, if x_s is a nonzero vector in $\mathrm{Im}(1 - s)$, then $\mathrm{Im}(1 - s) = \mathbb{F}x_s$. Since $sv - v \in \mathrm{Im}(1 - s)$ for $v \in V$, it follows that

$$sv = v + \ell_s(v)x_s,$$

where $\ell_s : V \to \mathbb{F}$ is a linear functional with $\mathrm{Ker}(\ell_s) = H_s$. Here, ℓ_s depends only on the choice of x_s. For $f \in \mathbb{F}[V]$, consider the polynomial $sf - f$. Its division with ℓ_s gives

$$sf - f = q\ell_s + r,$$

where r is a constant. Let $u \in H_s$. Then,

$$\begin{aligned}(sf - f)(u) &= sf(u) - f(u)\\ &= f(s^{-1}(u)) - f(u)\\ &= f(u) - f(u)\\ &= 0.\end{aligned}$$

Thus, $r(u) = 0$ since $u \in \mathrm{Ker}(\ell_s)$. It implies that $r = 0$. So, $\ell_s \,|\, (sf - f)$. We define $\Delta_s(f)$ to be the quotient:

$$sf - f = \Delta_s(f)\ell_s.$$

Thus, $\Delta_s(f) \in \mathbb{F}[V]$ has degree $\deg(f) - 1$ and Δ_s depends only on the choice of x_s.

Definition. The *ideal of generalized invariants* J of $\mathbb{F}[V]$ is defined by [21]

$$J := \{\, f \in \mathbb{F}[V]^+ \;\mid\; \Delta_{s_1} \cdots \Delta_{s_k}(f) \in \mathbb{F}[V]^+ \;\; \forall\, s_1, \ldots, s_k \in G \,\},$$

where $\mathbb{F}[V]^+$ is the ideal of $\mathbb{F}[V]$ generated by positive degree polynomials.

The following theorem is one of the main results in [21]. An analog of the theorem is mentioned in Section 5.3 in terms of our definition. Thus, the theorem is given for the completeness of the context.

Theorem 4.1 *[21, Theorem A] Let J be the ideal of generalized invariants as defined above. Then*

(i) J is generated by a regular sequence, say of degrees $d_1, d_2, \ldots,$

(ii) If G is finite, then $|G| = \prod_i d_i$ if and only if $J = \mathfrak{h}$.

4.2 Properties of Generalized Invariants

We redefine the concept of generalized invariant not only for pseudo-reflection groups but also for any group. Although the notations in this section are similar to ones used in Kac-Peterson's definition, their meaning is completely different. In order to give the definition of generalized invariants, firstly we need to consider a twisted derivation on the polynomial ring.

4.2.1 Twisted Derivation

Let V be an n-dimensional representation of a finite group G over a field $\mathbb{F}$ of characteristic p, and let $\sigma \in G$. We define Δ_σ (or simply, Δ if σ is clear from the context) as the element $\sigma - 1$ of the group algebra $\mathbb{F}G$, and we extend the action of G to $\mathbb{F}G$ on $\mathbb{F}[V]$. Actually, Δ_σ is an $\mathbb{F}$-linear map on $\mathbb{F}[V]$ such that for any $f \in \mathbb{F}[V]$,

$$\begin{aligned} \Delta_\sigma(f) &= (\sigma - 1)(f) \\ &= \sigma(f) - f, \end{aligned}$$

and satisfying a twisted product rule (Leibniz rule):

$$\Delta_\sigma(fh) = \Delta_\sigma(f)h + \sigma(f)\Delta_\sigma(h),$$

where $f, h \in \mathbb{F}[V]$. For this reason, Δ_σ is known as the *twisted derivation on* $\mathbb{F}[V]$ in the literature.

For any $\ell \in \mathbb{N}_0$, we write Δ_σ^ℓ for $(\sigma - 1)^\ell$ in $\mathbb{F}G$, and $\Delta_\sigma^0 = 1$. The general twisted product rule of Δ_σ has the following form:

$$\Delta_\sigma^\ell(fh) = \sum_{i=0}^{\ell} \binom{\ell}{i} \sigma^i\big(\Delta_\sigma^{\ell-i}(f)\big)\Delta_\sigma^i(h) \tag{4.1}$$

for any $f, h \in \mathbb{F}[V]$.

Remark. The following lemma demonstrates in particular that Δ^ℓ is a non-zero map for non-modular representations. However, in the modular case, this situation does not continue to hold. For example, if $\sigma \in G$ is of order p^k, then

$$\Delta_\sigma^{p^k} = \sigma^{p^k} - 1 = 0$$

since the characteristic of the ground field $\mathbb{F}$ is p.

Lemma 4.2 *For any group G, let $\sigma \in G$ of order $p^k m$ with $\gcd(p, m) = 1$, $m \neq 1$ and $k \in \mathbb{N}_0$. Then $\Delta_\sigma^\ell \neq 0$ for all $\ell \in \mathbb{N}_0$.*

Proof. Suppose that ℓ is the minimum number satisfying $\Delta_\sigma^\ell = (\sigma - 1)^\ell = 0$. Then $\tau = (\sigma - 1)^{\ell-1} \neq 0$ and $(\sigma - 1)\tau = 0$ implies that $\sigma\tau = \tau$. In this case, note that $\ell \geq 2$ since $\sigma \neq 1$, and

$$\tau = \sigma^{p^k}\tau = \cdots = \sigma^{p^k(m-1)}\tau.$$

If $\ell > p^k$,

$$\begin{aligned} m\tau &= \tau + \sigma^{p^k}\tau + \cdots + \sigma^{p^k(m-1)}\tau \\ &= (1 + \sigma^{p^k} + \cdots + \sigma^{p^k(m-1)})\tau \\ &= (1 + \sigma^{p^k} + \cdots + \sigma^{p^k(m-1)})(\sigma-1)^{p^k}(\sigma-1)^{\ell-1-p^k} \\ &= (1 + \sigma^{p^k} + \cdots + \sigma^{p^k(m-1)})(\sigma^{p^k}-1)(\sigma-1)^{\ell-1-p^k} \\ &= (\sigma^{p^k m}-1)(\sigma-1)^{\ell-1-p^k} \\ &= 0. \end{aligned}$$

It implies that $p \,|\, m$, which is a contradiction. If $\ell \leq p^k$, then $(\sigma-1)^{p^k} = 0$. Thus, $\sigma^{p^k} = 1$ since $\mathrm{char}(\mathbb{F}) = p$. But it is again contradiction because the order of σ is $p^k m$. Hence, $(\sigma-1)^\ell \neq 0$ for all ℓ. □

4.2.2 Definition of Generalized Invariants

Definition. An element $f \in \mathbb{F}[V]$ is called *a generalized invariant* if for every $1 \neq \sigma_1, \ldots, \sigma_k \in G$, there exist $\ell_1, \ldots, \ell_k \in \mathbb{N}_0$ such that

$$\Delta_{\sigma_1}^{\ell_1} \cdots \Delta_{\sigma_k}^{\ell_k}(f) = 0$$

provided that $\Delta_{\sigma_1}^{\ell_1} \cdots \Delta_{\sigma_k}^{\ell_k} \neq 0$. We denote the set of all generalized invariants analogously by $\mathbb{F}[V]_\Delta^G$.

The condition $\Delta_{\sigma_1}^{\ell_1} \cdots \Delta_{\sigma_k}^{\ell_k} \neq 0$ cannot be removed from the definition, because otherwise, any element of $\mathbb{F}[V]$ for p-groups becomes a generalized invariant.

Also, generalized invariants can equivalently be defined as follows. We use this simplified definition for our purposes.

Lemma 4.3 (Simplified Definition)

$$\mathbb{F}[V]_\Delta^G = \{\, f \in \mathbb{F}[V] \mid \forall\, 1 \neq \sigma \in G,\ \exists\, \ell \in \mathbb{N}_0 : \Delta_\sigma^\ell(f) = 0 \text{ provided that } \Delta_\sigma^\ell \neq 0 \,\}.$$

Proof. We label the first definition with 1 and the second definition with 2.
$(1 \Rightarrow 2)$ Take $k = 1$.
$(2 \Rightarrow 1)$ Let f be a generalized invariant with respect to the definition 2. Then for all $1 \neq \sigma_k \in G$, there exists $\ell_k \in \mathbb{N}_0$ such that $\Delta_{\sigma_k}^{\ell_k}(f) = 0$ and $\Delta_{\sigma_k}^{\ell_k} \neq 0$. Thus, for given $\sigma_1, \ldots, \sigma_k \in G$,

$$\Delta_{\sigma_1}^{0} \cdots \Delta_{\sigma_{k-1}}^{0} \Delta_{\sigma_k}^{\ell_k}(f) = 0.$$

Hence, f is a generalized invariant with respect to the first definition. □

Remark. Note that the ring of invariants can be written in terms of Δ notation as follows:

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid \Delta_\sigma(f) = 0 \text{ for all } \sigma \in G\}.$$

Therefore, $\mathbb{F}[V]^G$ is always contained in $\mathbb{F}[V]_\Delta^G$. Also it means that generalized invariants are a natural extension of the usual invariants.

The following is an example which will often be mentioned in the next sections and given in this part as a sample for the generalized invariants.

Example 4.1. Let $\mathbb{F}_3[V] = \mathbb{F}_3[x, y, z]$, and $G = C_3 \times C_3$ be a group generated by σ and τ. Consider the action of G on $\mathbb{F}_3[V]$ defined as

$$\sigma = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \tau = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then the polynomial yz is in $\mathbb{F}[V]_\Delta^{\langle\sigma\rangle}$; indeed,

$$\Delta_\sigma^2(yz) = (\sigma - 1)^2(yz) = (\sigma^2 + \sigma + 1)(yz) = 0.$$

Similarly, $yz \in \mathbb{F}[V]_\Delta^{\langle\tau\rangle}$.

4.3 Module Structure of Generalized Invariants

We determine an introduce the structure of the set $\mathbb{F}[V]^G_\Delta$ in this section. Firstly, we investigate whether it satisfies the ring axioms since the set of invariants has a ring structure. We consider Example 4.1. In this example, while the polynomial $y \in \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta$, the polynomial y^2 is not in $\mathbb{F}[V]^{\langle\sigma\rangle}_\Delta$ since $\Delta^2_\sigma(y^2) = 2x^2$ and $\Delta^3_\sigma = 0$. Because $\Delta^2_\sigma(y^2)$ can not be written as $\Delta^2_\sigma(y)\Delta^2_\sigma(y)$ as usual product rule. If we use the general form of twisted derivations (4.1) in Section 4.2.1, we can see that $\Delta^\ell_\sigma(fh)$ may not be nonzero for any ℓ satisfying $\Delta^\ell_\sigma \neq 0$ while f and h are generalized invariants. This demonstrates that for any group G, $\mathbb{F}[V]^G_\Delta$ has no ring structure in contrast to the invariant ring $\mathbb{F}[V]^G$. Indeed, it is due to the twisted product property of the operator Δ. However, the set of generalized invariants $\mathbb{F}[V]^G_\Delta$ has an $\mathbb{F}[V]^G$-module structure as shown below.

Proposition 4.4 *$\mathbb{F}[V]^G_\Delta$ is an $\mathbb{F}[V]^G$-submodule of $\mathbb{F}[V]$. In particular, it is a finitely generated $\mathbb{F}[V]^G$-module.*

Proof. By Corollary 2.8, $\mathbb{F}[V]^G$ is a Noetherian ring and $\mathbb{F}[V]$ is a Noetherian $\mathbb{F}[V]^G$-module for a finite group G. Since for each $f \in \mathbb{F}[V]^G_\Delta$ and $g \in \mathbb{F}[V]^G$, $\Delta^\ell(gf) = g\Delta^\ell(f)$, we can obtain that $\mathbb{F}[V]^G_\Delta$ has an $\mathbb{F}[V]^G$-module structure. Thus, $\mathbb{F}[V]^G_\Delta$ becomes an $\mathbb{F}[V]^G$-submodule of the Noetherian module $\mathbb{F}[V]$. This gives the result. □

Remark. We consider the algebra $\mathbb{F}[f_1, \ldots, f_k]$ generated by a homogeneous system of parameters (h.s.o.p.) $\{f_1, \ldots, f_k\}$ of $\mathbb{F}[V]^G$. Since f_i's are invariant polynomials, we can say that $\mathbb{F}[V]^G_\Delta$ has also an $\mathbb{F}[f_1, \ldots, f_k]$-module structure.

4.4 Generalized Invariants for non-Modular Representations

The concept of generalized invariant modules is created as an alternative structure to the invariant ring. But these two structures are the same for non-modular

representations as shown below. From this viewpoint, generalized invariants are a generalization of the usual invariants from the non-modular case to the modular one. Therefore, they are worth studying only in modular case.

Proposition 4.5 *Let G be a finite group with non-modular representation V. Then $\Delta_\sigma^\ell(f) = 0$ for some ℓ satisfying $\Delta_\sigma^\ell \neq 0$ if and only if $\Delta_\sigma(f) = 0$ for any $\sigma \in G$.*

Proof. It is clear that every σ-invariant is a generalized σ-invariant. For the converse statement, suppose that $\Delta_\sigma^\ell(f) = 0$ for $\sigma \in G$. Then $\Delta_\sigma^{\ell-1}(f) \in \mathbb{F}[V]^G$. Since $\mathrm{Tr}^G \circ \Delta_\sigma = \Delta_\sigma \circ \mathrm{Tr}^G$ and the image of Tr^G is invariant, we have $\mathrm{Tr}^G(\Delta_\sigma^{\ell-1}(f)) = \Delta_\sigma(\mathrm{Tr}^G(\Delta_\sigma^{\ell-2}(f))) = 0$. Thus, $\Delta_\sigma^{\ell-1}(f) \in \mathrm{Ker}(\mathcal{R}^G)$, where $\mathcal{R}^G$ is the Reynolds operator $\frac{1}{|G|}\mathrm{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$. In Section 2.4.3, we showed that $\mathcal{R}^G$ is surjective and $\mathbb{F}[V] = \mathbb{F}[V]^G \oplus \mathrm{Ker}(\mathcal{R}^G)$. Therefore, we get $\Delta_\sigma^{\ell-1}(f) = 0$. Proceeding the induction on ℓ, we conclude that $\Delta_\sigma(f) = 0$. □

This result can be extended to any non-modular subrepresentation of a group using same method above.

Corollary 4.6 *Let H be a subgroup of G such that its order is coprime with p. Then $\mathbb{F}[V]^H_\Delta = \mathbb{F}[V]^H$.*

Chapter 5

Generalized Invariants of Cyclic Groups

In many aspects, the cyclic group C_p of order p plays a central role in modular invariant theory. As mentioned in previous sections, there are many studies investigating C_p-invariants in characteristic p. In this chapter, in order to understand the structure of generalized invariants, we start to analyze the generalized invariant module of the basic group C_p. In the first section, the general structure and some properties of $\mathbb{F}[V]_{\Delta}^{C_p}$ is given. Then for the lower dimensional indecomposable representations, the structure of $\mathbb{F}[V]_{\Delta}^{C_p}$ is considered explicitly. In the last section, the generalized Hilbert ideal of $\mathbb{F}[V]_{\Delta}^{C_p}$ in $\mathbb{F}[V]$ is defined and an analog of the Hilbert ideal conjecture is proved for this ideal.

Unless otherwise stated, for the rest of this chapter, we take G as a cyclic group of order p and σ as a generator of G. We identify $G = \{1, \sigma, \ldots, \sigma^{p-1}\}$ whenever elements are explicitly required. Note that generalized invariants of C_p corresponds to usual invariants when $p = 2$. Thus, it is meaningful to take $p > 2$ in this chapter.

5.1 Structural Properties

In this section, we consider some properties of generalized invariant module $\mathbb{F}[V]^G_\Delta$. The following result can be used as a definition of generalized invariant module of a cyclic group of order p.

Proposition 5.1 *An element $f \in \mathbb{F}[V]$ is a generalized invariant if and only if $\mathrm{Tr}^G(f) = 0$. In particular, $\mathbb{F}[V]^G_\Delta = \mathrm{Ker}\,\mathrm{Tr}^G$.*

Proof. By the identity, $(t-1)^{p-1} = \frac{(t-1)^p}{t-1} = \frac{1-t^p}{1-t} = 1 + t + t^2 + \cdots + t^{p-1}$ over $\mathbb{F}$ for $t \neq 1$, we can write $\Delta^{p-1} = 1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1} = \mathrm{Tr}^G$. Moreover, $\Delta^p = \sigma^p - 1 = 0$. Therefore, a polynomial f is a generalized invariant if and only if $\Delta^\ell(f) = 0$ for some $\ell \leq p-1$. Hence, the result follows. □

Remark. The proof of Proposition 5.1 demonstrates that a polynomial is C_p-generalized invariant if and only if it is generalized invariant with respect to the generator σ.

Proposition 5.2 *For any finite group G and for all $\sigma \in G$,*

$$\mathrm{Im}\,\Delta_\sigma \subseteq \mathrm{Ker}\,\mathrm{Tr}^G.$$

Proof. Let f be a polynomial in $\mathbb{F}[V]$. Then the result follows

$$\mathrm{Tr}^G\big(\Delta_\sigma(f)\big) = \Delta_\sigma\big(\mathrm{Tr}^G(f)\big) = 0.$$

□

Corollary 5.3 *If G is the cyclic group C_p, for all $\sigma \in G$,*

$$\mathrm{Im}\,\Delta_\sigma \subseteq \mathbb{F}[V]^G_\Delta.$$

Proof. As well as this is a corollary of Proposition 5.1 and Proposition 5.2, the result is obvious since Δ is nilpotent operator for C_p in characteristic p. □

The relation between $\mathbb{F}[V]^G_\Delta$ and $\operatorname{Ker}\operatorname{Tr}^G$ for any finite group G is given in Section 6.1. Now, it is worth noting that the above inclusion is strict as showed in the following example.

Example 5.1. Let $V = V_2$ be a 2-dimensional representation of C_p for an odd prime p. By choosing an appropriate basis, we can write $\mathbb{F}[V] = \mathbb{F}[x, y]$ where $\Delta(y) = x$ and $\Delta(x) = 0$. Note that $\Delta^2(y) = 0$ and therefore $\Delta^{p-1}(y) = \operatorname{Tr}^{C_p}(y) = 0$, hence $y \in \operatorname{Ker}\operatorname{Tr}^{C_p} \setminus \operatorname{Im}(\Delta) = \mathbb{F}[V]^{C_p}_\Delta \setminus \operatorname{Im}(\Delta)$.

Remark (Group Cohomology)**.** Generalized invariant module of G corresponds to an important structure in modular invariant theory. Indeed, by the projective resolution of $\mathbb{F}G$, we have the following complex

$$\cdots \xrightarrow{\Delta} \mathbb{F}G \xrightarrow{\mathrm{Tr}} \mathbb{F}G \xrightarrow{\Delta} \mathbb{F}G \xrightarrow{\mathrm{Tr}} \mathbb{F}G \xrightarrow{\Delta} \mathbb{F}G \xrightarrow{\mathrm{Tr}} \mathbb{F}G \xrightarrow{\Delta} \mathbb{F}G.$$

When the functor $\operatorname{Hom}_{\mathbb{F}G}(., \mathbb{F}[V])$ is applied and the cohomology of the complex is taken, we obtain

$$\begin{aligned} \mathrm{H}^0(G, \mathbb{F}[V]) &= \mathbb{F}[V]^G \\ \mathrm{H}^{2k+1}(G, \mathbb{F}[V]) &= \frac{\mathrm{Ker}\mathrm{Tr}^G}{\mathrm{Im}\Delta} = \frac{\mathbb{F}[V]^G_\Delta}{\mathrm{Im}\Delta} \\ \mathrm{H}^{2k}(G, \mathbb{F}[V]) &= \frac{\mathrm{Ker}\Delta}{\mathrm{Im}\mathrm{Tr}^G} = \frac{\mathbb{F}[V]^G}{\mathrm{Im}\mathrm{Tr}^G} \end{aligned}$$

for $k > 0$.

Let V be an indecomposable representation of G. Recall that by the Jordan canonical form of σ given in Section 2.4.4, $\sigma(x_i) = x_i + x_{i-1}$ for $n \geq i > 1$ and $\sigma(x_1) = x_1$. Denote the norm of x_i by $\mathrm{N}(x_i)$ so that $\mathrm{N}(x_i) = \prod_{k=0}^{p-1} \sigma^k(x_i)$. The following weight condition characterizes the monomials in $\mathbb{F}[V]^G_\Delta$.

Lemma 5.4 (Weight condition) *For a monomial* $m = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, *if* $\mathbf{wt}(m) := \sum_{i=1}^{n} (i-1)a_i < p-1$, *then* $\operatorname{Tr}^G(m) = 0$.

Proof. Note that

$$\begin{aligned}\mathrm{Tr}^G(m) &= \sum_{i=0}^{p-1} \sigma^i(x_1)^{a_1}\sigma^i(x_2)^{a_2}\cdots\sigma^i(x_n)^{a_n} \\ &= \sum_{i=0}^{p-1} x_1^{a_1}(x_2+ix_1)^{a_2}\cdots\left(x_n+ix_{n-1}+\cdots+\binom{i}{n-1}x_1\right)^{a_n}.\end{aligned}$$

with the convention that $\binom{i}{j} = 0$ whenever $i < j$. By expanding the binomial coefficients as a polynomial in i, we conclude that the maximum degree of i in the last sum is equal to $\mathbf{wt}(m)$ and $\mathbf{wt}(m) < p-1$. By Lemma 2.3,

$$\sum_{i=0}^{p-1} i^\alpha = \begin{cases} -1, & p-1 \mid \alpha, \\ 0, & p-1 \nmid \alpha. \end{cases}$$

Then we deduce that all coefficients in the expansion of the transfer map vanish, hence $\mathrm{Tr}^G(m) = 0$. □

Lemma 5.5 *If $f \in \mathbb{F}[V]^G_\Delta$ and $f = q\mathrm{N}(x_n) + r$ where the degree $\deg_{x_n}(r)$ of r in x_n is less than p, then $q, r \in \mathbb{F}[V]^G_\Delta$.*

Proof. Since $\mathrm{N}(x_n) \in \mathbb{F}[V]^G$, for any integer $\ell > 0$, we have

$$\Delta^\ell(f) = \Delta^\ell(q)\mathrm{N}(x_n) + \Delta^\ell(r).$$

Moreover, $\deg_{x_n}\Delta^\ell(r) \le \deg_{x_n} r < p$ while $\deg_{x_n}\mathrm{N}(x_n) = p$. Therefore, $\Delta^{p-1}(f) = 0$ implies that $\Delta^{p-1}(q) = 0$ and $\Delta^{p-1}(r) = 0$. Hence, $q, r \in \mathbb{F}[V]^G_\Delta$. □

The result in Lemma 5.5 does not hold when f is divided by the norm of the other variables $x_1, \ldots, x_{n-1}$ as showed in the next example.

Example 5.2. Suppose that $\mathbb{F}[V] = \mathbb{F}[x, y, z]$. For any $f \in \mathbb{F}[V]^G_\Delta$, if

$$f = q\mathrm{N}(y) + r$$

with $\deg_y r < p$, we would not say that q and r are in $\mathbb{F}[V]^G_\Delta$. Indeed, $\deg_y \Delta(r)$ may be greater than $\deg_y(r)$ depending on $\deg_z(r)$ and the division algorithm does

not work. For $p = 5$, $f = y^5z^3 + xy^3z^4 + x^2y^2z^4 + 2x^3yz^4 + 3x^4z^4 + 2x^5z^3 \in \mathbb{F}[V]^G_\Delta$. If it is divided by $\mathrm{N}(y) = y^5 + 4x^4y$, we obtain that $f = z^3\mathrm{N}(y) + r$ with $\deg_y r < 5$. But z^3 is not in $\mathbb{F}[V]^G_\Delta$. Notice that $\deg_y \Delta(r) = 4$ while $\deg_y r = 3$.

Recall that a generating set of a module is called minimal if it satisfies that the leading monomials of the polynomials in it are minimal and its each proper subset cannot generate the whole module. Note that the action of G (and Δ) is represented by a triangular matrix, therefore if necessary, we can refine any generating set to a minimal generating set with minimal leading monomials by the usual Gaussian elimination. The monomial order is the graded reverse lex-order given by $x_1 \prec \cdots \prec x_n$.

Proposition 5.6 *If $f \in \mathbb{F}[V]^G_\Delta$ is in a minimal generating set of $\mathbb{F}[V]^G_\Delta$, then $\deg_{x_1} \mathrm{LM}(f) = 0$ and $\deg_{x_n} \mathrm{LM}(f) \leq p - 2$.*

Proof. Let $m = \mathrm{LM}(f)$ and suppose that $m = x_n^{a_n} \cdots x_1^{a_1}$ with $a_1 > 0$. Then all the other terms of f are also divisible by $x_1^{a_1}$. Thus, $f = x_1^{a_1} g$ for some $g \in \mathbb{F}[V]$. Since $f \in \mathbb{F}[V]^G_\Delta$ and $\mathrm{Tr}^G(f) = x_1^{a_1}\mathrm{Tr}^G(g) = 0$, we get $\mathrm{Tr}^G(g) = 0$ and therefore $g \in \mathbb{F}[V]^G_\Delta$. This contradicts with the minimality of f. Hence $\deg_{x_1} m = 0$.

By Lemma 5.5, we have $\deg_{x_n} m < p$. Suppose for contradiction that $\deg_{x_n} m = p - 1$. By the first part, we have $m = {x_n}^{p-1} x_{n-1}^{a_{n-1}} \cdots x_2^{a_2}$. So,

$$\begin{aligned}
\mathrm{Tr}^G(m) &= \sum_{\alpha=0}^{p-1} (x_n + \alpha x_{n-1} + \cdots)^{p-1} (x_{n-1} + \cdots)^{a_{n-1}} \cdots (x_2 + \alpha x_1)^{a_2} \\
&= x_{n-1}^{a_{n-1}+p-1} x_{n-2}^{a_{n-2}} \cdots x_2^{a_2} \sum_{\alpha=0}^{p-1} \alpha^{p-1} + \text{lower terms} \\
&= -x_{n-1}^{a_{n-1}+p-1} x_{n-2}^{a_{n-2}} \cdots x_2^{a_2} + \text{lower terms},
\end{aligned}$$

hence $\mathrm{LM}(\mathrm{Tr}^G(m)) = x_{n-1}^{a_{n-1}+p-1} x_{n-2}^{a_{n-2}} \cdots x_2^{a_2}$. Since $\mathrm{Tr}^G(f) = 0$, the leading monomial of $\mathrm{Tr}^G(m)$ should be annihilated by the transfer of another term in f, say $u = x_n^{b_n} \cdots x_1^{b_1}$ such that $\mathrm{LM}(\mathrm{Tr}^G(u)) = x_{n-1}^{a_{n-1}+p-1} x_{n-2}^{a_{n-2}} \cdots x_2^{a_2}$.

Since $m \succ u$, we have $b_1 = a_1, \ldots, b_{i-1} = a_{i-1}$ and $b_i > a_i$ for some $1 \leq i \leq n$, where we take $a_1 = 0$ and $a_n = p - 1$. Moreover, f is homogeneous, therefore

$\sum_{i=1}^{n} b_i = \sum_{i=1}^{n} a_i$. Finally, since the action is triangular, $\sum_{i=k}^{n} b_i \geq \sum_{i=k}^{n} a_i$ for all $1 \leq k \leq n-1$. This system of inequalities implies that $b_1 = a_1, \ldots, b_{n-2} = a_{n-2}$ and $b_n + b_{n-1} = a_n + a_{n-1}$.

Therefore, $b_{n-1} > a_{n-1}$ and $b_n < a_n = p-1$. Let $b_n = p-k$ and $b_{n-1} = a_{n-1} + k - 1$ for some $k > 1$. But then the coefficient of $x_{n-1}^{a_{n-1}+p-1} x_{n-2}^{a_{n-2}} \cdots x_2^{a_2}$ in $\mathrm{Tr}^G(u)$ is evaluated to $\sum_{\alpha=0}^{p-1} \alpha^{p-k} = 0$ since $k \neq 1$. Thus, $\mathrm{LM}(\mathrm{Tr}^G(m))$ cannot be annihilated, contradicting to the fact that $\mathrm{Tr}^G(f) = 0$. Hence, $\deg_{x_n} m \leq p-2$. □

5.2 Lower Dimensional Representations and Free Modules

When it is desired to give completely the structure of generalized invariants, it becomes more complicated for higher dimensional representations, even for indecomposable representations. In this section, we give the structure of generalized invariant modules for 2 and 3 dimensional indecomposable representations of $G = C_p$ with some counterexamples. Recall that by remark in Section 4.3, these $\mathbb{F}[V]^G$-modules are also $\mathbb{F}[f_1, \ldots, f_k]$-modules for an h.s.o.p. $\{f_1 \ldots, f_k\}$ of $\mathbb{F}[V]^G$. We investigate whether they are free modules over $\mathbb{F}[V]^G$ or $\mathbb{F}[f_1, \ldots, f_k]$. For the rest of this section, we consider the h.s.o.p. $\{x_1, \mathrm{N}(x_2), \ldots, \mathrm{N}(x_n)\}$ consisting of the norms of x_i. For simplicity of notations, we denote the polynomial ring $\mathbb{F}[x_1, \mathrm{N}(x_2), \ldots, \mathrm{N}(x_n)]$ by A.

5.2.1 Structure of 2-Dimensional Representations

Proposition 5.7 *Let V be a 2-dimensional indecomposable representation of G with dual basis x, y. Then*

$$\mathbb{F}[V]_{\Delta}^{G} = \bigoplus_{i=0}^{p-2} y^i A$$

where A is the polynomial ring $\mathbb{F}[x, \mathrm{N}(y)] = \mathbb{F}[V]^G$. In particular, $\mathbb{F}[V]^G_\Delta$ is a free A-module.

Proof. By Lemma 5.4 and Proposition 5.6, we have $\mathbb{F}[V]^G_\Delta = \sum_{i=0}^{p-2} y^i A$. Note that leading monomials of any $f \cdot g$ are different for $f \in A$ and $g \in \{1, y, \ldots, y^{p-2}\}$. Indeed,

$$\mathrm{LM}\left(x^a \mathrm{N}(y)^b y^i\right) = x^a y^{bp+i}.$$

Hence, the above sum is direct and $\mathbb{F}[V]^G_\Delta$ is a free module over $A = \mathbb{F}[V]^G$. □

In general, $\mathbb{F}[V]^G_\Delta$ is not a free $\mathbb{F}[V]^G$-module as shown in the next example.

Example 5.3. Let $V = V_2 \oplus V_2$ be a representation of G where V_2 denotes the 2-dimensional indecomposable representation and the action is diagonally extended to the direct sum. By Corollary 2.19, we know that $\mathbb{F}[V]^G = \mathbb{F}[x_1, x_2, \mathrm{N}(y_1), \mathrm{N}(y_2), u_{12}]$ where $u_{12} = y_1 x_2 - x_1 y_2$. Moreover, by direct calculation, it can be shown that $\mathbb{F}[V]^G_\Delta = \sum_{0 \le i+j \le p-2} y_1^i y_2^j \mathbb{F}[V]^G$. Notice that since $y_1, y_2 \in \mathbb{F}[V]^G_\Delta$ and $x_1, x_2 \in \mathbb{F}[V]^G$, the invariant u_{12} can be decomposed as a linear combination of $y_1 x_2$ and $y_2 x_1$. It can also be written as $1 \cdot u_{12}$, for $1 \in \mathbb{F}[V]^G_\Delta$ and $u_{12} \in \mathbb{F}[V]^G$. Therefore, $\mathbb{F}[V]^G_\Delta$ cannot be free as an $\mathbb{F}[V]^G$-module. However, $\mathbb{F}[V]^G_\Delta$ is a free A-module, where $A = \mathbb{F}[x_1, x_2, \mathrm{N}(y_1), \mathrm{N}(y_2)]$.

Remark. If we consider all vector spaces $mV_2 = \oplus_{i=1}^m V_2$ instead of $2V_2$, it can be seen that

$$\mathbb{F}[mV_2]^G_\Delta = \sum_{0 \le i_1 + \cdots + i_m \le p-2} y_1^{i_1} \cdots y_m^{i_m} \cdot A.$$

However, although $\mathbb{F}[2V_2]^G_\Delta$ has a free module structure over the polynomial ring A, this situation does not proceed along all representations mV_2. By calculations in Magma, we have constructed a counterexample for the representation $3V_2$ in characteristic $p = 3$. In this case, $\mathbb{F}[3V_2]^G_\Delta$ has the following 8 generators in degree

3:

$$
\begin{aligned}
f_1 &= 2x_2y_3^2 + y_2x_3y_3,\\
f_2 &= 2x_1y_3^2 + y_1x_3y_3,\\
f_3 &= 2x_1y_2y_3 + y_1x_2y_3,\\
f_4 &= 2x_1y_2y_3 + y_1y_2x_3,\\
f_5 &= 2x_2y_2y_3 + y_2^2x_3,\\
f_6 &= 2x_1y_1y_3 + y_1^2x_3,\\
f_7 &= 2x_1y_2^2 + y_1x_2y_2,\\
f_8 &= 2x_1y_1y_2 + y_1^2x_2.
\end{aligned}
$$

The generators f_1, f_2, f_3 gives the following relation between generators:

$$x_1f_1 - x_2f_2 + x_3f_3 = 0.$$

Hence, $\mathbb{F}[3V_2]^G_\Delta$ can not be a free module over the polynomial ring A.

5.2.2 Structure of 3-Dimensional Representations

In this part, we construct a minimal generating set of the generalized invariant module for 3-dimensional representations and investigate freeness of the generalized invariant module. For the rest of this section, V denotes the 3-dimensional representation V_3. In this case, we use x, y, z for the dual basis elements x_1, x_2, x_3.

Lemma 5.8 *Let f be in a minimal generating set of $\mathbb{F}[V]^G_\Delta$. If $f \in \mathrm{Im}(\Delta)$, then*

$$\deg_y \mathrm{LM}(f) \leq p.$$

Proof. Suppose that $\mathrm{LM}(f) = x^ay^bz^c$ and $b > p$. By Proposition 5.6, $a = 0$ and $c \leq p-2$. Since $f \in \mathrm{Im}(\Delta)$, $f = \Delta(g)$ for some $g \in \mathbb{F}[V]$. Thus, $\mathrm{LM}(g) = y^{b-1}z^{c+1}$, where $b-1 \geq p$. So, we have $g = q\mathrm{N}(y)+r$ for some $q, r \in \mathbb{F}[V]$ such that $\deg_y r < p$. Hence, we get $f = \Delta(q)\mathrm{N}(y) + \Delta(r)$. Note that $\Delta(q), \Delta(r) \in \mathbb{F}[V]^G_\Delta$. Therefore, it is sufficient for contradiction to show that $\mathrm{LM}(\Delta(r)) \prec \mathrm{LM}(f)$.

Notice that $\mathrm{LM}(r) \prec \mathrm{LM}(g)$. Furthermore, $\deg_y r < p$ implies that $\mathrm{LM}(r)$ is divisible by x, and so is $\mathrm{LM}(\Delta(r))$. Hence, $\mathrm{LM}(\Delta(r)) \prec \mathrm{LM}(f)$. Therefore, f is not in a minimal generating set, a contradiction. Thus, $b \leq p$ as required. □

In Lemma 5.8, we can refine the condition $f \in \mathrm{Im}(\Delta)$ as follows.

Lemma 5.9 *If $f \in \mathbb{F}[V]^G_\Delta$ and $\mathrm{LM}(f) = y^b z^c$ with $b > p$, then f is not in a minimal generating set of $\mathbb{F}[V]^G_\Delta$.*

Proof. Suppose that f is in a minimal generating set of $\mathbb{F}[V]^G_\Delta$. Then $c \leq p-2$ by Proposition 5.6, and $f \notin \mathrm{Im}(\Delta)$ by Lemma 5.8. Let $m = y^{b-1}z^{c+1}$ and note that $\mathrm{LM}(\Delta(m)) = y^b z^c$, as $b > 0$ and $c \leq p-2$. Then, $g := f - \Delta(m) \neq 0$ because f is not in $\mathrm{Im}(\Delta)$. Moreover, $g \in \mathbb{F}[V]^G_\Delta$ and $\mathrm{LM}(g) \prec \mathrm{LM}(f)$. The condition $b > p$ implies that $\Delta(m)$ can be written as an A-module combination of generalized invariants with smaller leading monomials by the proof of Lemma 5.8. Hence, f cannot be in a minimal generating set. □

The following lemma gives a bound on the exponent of the variable z for a polynomial in a minimal generating set when the exponent of y is p.

Lemma 5.10 *If f is in a minimal generating set of $\mathbb{F}[V]^G_\Delta$ and $\mathrm{LM}(f) = y^p z^c$, then $c \geq \frac{p-1}{2}$.*

Proof. By the hypothesis, f can be written as $f = \mathrm{N}(y)q + r$, where $\deg_y r < p$ and $\mathrm{LM}(q) = z^c$. If $c < \frac{p-1}{2}$, then $\mathrm{Tr}^G(z^c) = 0$ by Lemma 5.4. Moreover, for any monomial $u := x^a y^b z^d$ appearing in q, we have $a + b + d < \frac{p-1}{2}$ and thus $\mathbf{wt}(u) < p-1$. Therefore, $\mathrm{Tr}^G(q) = 0$ and $q \in \mathbb{F}[V]^G_\Delta$. By the same arguments of the previous proof, we have $r \in \mathbb{F}[V]^G_\Delta$ with $\mathrm{LM}(r) \prec \mathrm{LM}(f)$. Hence, f is not in a minimal generating set. □

Corollary 5.11 *There is a minimal generating set $\mathbb{F}[V]^G_\Delta$ consisting of polynomials with the leading monomials*

(i) $z^j, \quad 1 \leq j < (p-1)/2,$

(ii) $y^i z^j, \quad 1 \leq i < p,\ 0 \leq j \leq p-2,$

(iii) $y^p z^j, \quad (p-1)/2 \leq j \leq p-2.$

Proof. Note that the monomials z^j of the first item satisfy the hypothesis of Lemma 5.4; hence, they are generalized invariants. Moreover, by Proposition 5.6, Proposition 5.9, and Lemma 5.10, the monomials in the second and the third items list all other possible monomials. Finally, $f = \Delta(y^{i-1}z^{j+1}) \in \mathbb{F}[V]^G_\Delta$ and $\mathrm{LM}(f) = y^i z^j$ for any $1 \leq i \leq p,\ 0 \leq j \leq p-2$, hence we obtain a generating set, with required leading monomials listed in the second and the third items.

For the minimality condition, observe that the leading monomials given in the first and the second items cannot be obtained from the other generators as an element of $\mathbb{F}[V]^G_\Delta$. Note that only $y^p z^j$ can also be obtained as $\mathrm{LM}(\mathrm{N}(y)z^j)$, provided that $z^j \in \mathbb{F}[V]^G_\Delta$. By Lemma 5.10, the case $y^p z^j$ for $j < \frac{p-1}{2}$ is excluded. Hence, the result follows. □

Theorem 5.12 $\mathbb{F}[V]^G_\Delta$ *is a free* A*-module.*

Proof. For a generator g from a minimal generating set satisfying the Corollary 5.11, we have either

- $LM(fg) = x^a y^{pb} z^{pc+j}, \quad 1 \leq j < (p-1)/2$, or
- $LM(fg) = x^a y^{p(b+1)} z^{pc+j}, \quad (p-1)/2 \leq j \leq p-2$, or
- $LM(fg) = x^a y^{pb+i} z^{pc+j}, \quad 1 \leq i < p,\ 0 \leq j \leq p-2$

for some nonnegative integers a, b, c and any $f \in A$. Suppose that $\sum_i f_i g_i = 0$, where $f_i \in A$ and g_i's are in the minimal generating set of $\mathbb{F}[V]^G_\Delta$. Then for each i, $\mathrm{LM}(g_i)$ has the form $y^{b_i} z^{c_i}$ such that $b_i \leq p$ and $c_i \leq p-2$. If a term of f_i is divided by a power of x or z^p, so is a term of f_j for each $j \neq i$. Therefore, the only remaining case which can satisfy the equation $\sum_i f_i g_i = 0$ is that y^p divides a term of f_i for some i and that $b_j = p$ for a generator $g_j \neq g_i$. In this case, for the generator g_i corresponding to f_i, $\mathrm{LM}(g_i) = z^{c_i}$,where $c_i \geq \frac{p-1}{2}$. But while

$\mathrm{LM}(g_i) = z^{c_i}$ with $c_i \geq \frac{p-1}{2}$, g_i is not a generalized invariant by Lemma 5.10. Hence, we can not obtain such a relation $\sum_i f_i g_i = 0$. It means that $\mathbb{F}[V]^G_\Delta$ is a free A-module. □

Remark. Since $\mathbb{F}[V_2]^G_\Delta$ and $\mathbb{F}[V_3]^G_\Delta$ are free modules over the corresponding polynomial ring A, it can be asked whether it holds for all indecomposable representations of G. But, based on calculations in Magma [2], we have shown that $\mathbb{F}[V]^G_\Delta$ is not a free A-module for $V = V_4$ over characteristic $p = 5$. Indeed, there is a unique relation of degree 12 among 100 generators. For the details in calculations, see [26].

5.3 Ideal of Generalized Invariants

If we return to Chapter 3.3, the Hilbert ideal $\mathfrak{h}$ is the ideal in $\mathbb{F}[V]$ generated by invariants of positive degree, i.e.,

$$\mathfrak{h} = \langle f \in \mathbb{F}[V]^G \mid \deg f > 0 \rangle.$$

As an analogy of the Hilbert ideal, we define $\mathfrak{h}_\Delta$ as the ideal in $\mathbb{F}[V]$ generated by positive degree elements of $\mathbb{F}[V]^G_\Delta$.

Now, we give an analogue of Theorem 4.1 proved by Kac-Peterson in [21].

Theorem 5.13 *For an indecomposable representation $V = V_n$ of a cyclic group G of order p,*

(i) $\mathfrak{h}_\Delta$ is generated by a regular sequence, say of degrees $d_1, \ldots, d_n$,

(ii) $d_1 \cdots d_n = |G|$ if and only if $\beta(\mathfrak{h}_\Delta) = \beta(\mathfrak{h})$.

Proof. Since $\mathrm{Im}(\Delta) \subset \mathbb{F}[V]^G_\Delta$, we have $\{x_1, \ldots, x_{n-1}\} \subset \mathbb{F}[V]^G_\Delta$ as $\Delta(x_i) = x_{i-1}$ for $1 < i \leq n$. Hence $\langle x_1, \ldots, x_{n-1} \rangle \subset \mathfrak{h}_\Delta$.

If $n < p$, then $\mathbf{wt}(x_n) = n - 1 < p - 1$ and hence $x_n \in \mathbb{F}[V]^G_\Delta$. Therefore, $\mathfrak{h}_\Delta$ is the unique maximal ideal in $\mathbb{F}[V]$, with generators $\{x_1, \ldots, x_n\}$.

Otherwise, we have $n = p$. Note that, $\mathrm{LM}(\mathrm{N}(x_n)) = x_n^p$, hence $x_n^p \in \mathfrak{h}_\Delta$. Moreover, any polynomial $f \in \mathbb{F}[V]$ with $\mathrm{LT}(f) = \alpha x_n^a$ cannot be a generalized invariant for $a < p$ by the fact that $\mathrm{LT}(\mathrm{Tr}^G(f)) = -\alpha\binom{a}{b}x_{n-k}^{a-b}x_{n-k-1}^b$ where $k = \lfloor \frac{p-1}{a} \rfloor$ and $b = p - 1 - ak$. Therefore,

$$\mathfrak{h}_\Delta = \begin{cases} \langle x_1, \ldots, x_n \rangle & n < p, \\ \langle x_1, \ldots, x_{n-1}, x_n^p \rangle & n = p. \end{cases}$$

It is clear that these generating sets are regular. Finally, it is known by [38] that $\beta(\mathfrak{h}) = p$. Therefore, $\beta(\mathfrak{h}_\Delta) = \beta(\mathfrak{h})$ if and only if $n = p$ which is only possible when $d_1 \cdots d_n = p = |G|$. □

As a result of this proof, the ideal $\mathfrak{h}_\Delta$ of generalized invariants for C_p has the following generators:

$$\mathfrak{h}_\Delta = \begin{cases} \langle x_1, \ldots, x_n \rangle & n < p, \\ \langle x_1, \ldots, x_{n-1}, x_n^p \rangle & n = p. \end{cases}$$

This shows that the Hilbert ideal conjecture is satisfied for generalized invariants of C_p.

Corollary 5.14 *The ideal $\mathfrak{h}_\Delta$ is generated by polynomials of degree at most the group order p.*

Chapter 6

Structure of Generalized Invariants

In Chapter 5, we determined explicitly the structure of generalized invariant modules for 2 and 3 dimensional indecomposable representations of the cyclic group C_p. However, it is hard to obtain the same result for any representation. Instead of this, we give a general structure of generalized invariant module of any group G and bring out the core modules of the structure. Especially, generalized invariant module of its subgroups of order p plays a key role. Therefore, as in Chapter 5, we take $p > 2$ for the rest of the thesis.

6.1 Relation with Subgroups

Along this section, we consider some subgroup properties of generalized invariants. We compare these structures with generalized invariant module of any group. Moreover, we check that generalized invariant module has some properties of invariant rings. For the rest of the section, let V be a modular representation of a finite group G.

Lemma 6.1 *If H is a subgroup of G, then $\mathbb{F}[V]^G_\Delta \subseteq \mathbb{F}[V]^H_\Delta$. In particular, $\mathbb{F}[V]^G_\Delta = \bigcap_{H \leq G} \mathbb{F}[V]^H_\Delta$.*

Proof. It is immediate consequence of the definition of generalized invariants. □

For the cyclic group C_p of order p, we proved that $\mathbb{F}[V]_\Delta^{C_p} = \operatorname{Ker}\operatorname{Tr}^{C_p}$ in Proposition 5.1. The following result investigates the relation between $\mathbb{F}[V]_\Delta^G$ and $\operatorname{Ker}\operatorname{Tr}^G$ for any finite group G using the subgroup property.

Proposition 6.2 *For a modular representation V of the finite group G,*

$$\mathbb{F}[V]_\Delta^G \subseteq \operatorname{Ker}\operatorname{Tr}^G.$$

Proof. It is known that G has a cyclic subgroup H of order p by Sylow Theorem. Then by Proposition 5.1,

$$\mathbb{F}[V]_\Delta^H = \operatorname{Ker}\operatorname{Tr}^H.$$

Since $\operatorname{Tr}^G = \operatorname{Tr}_H^G \circ \operatorname{Tr}^H$, we always have

$$\operatorname{Ker}\operatorname{Tr}^H \subseteq \operatorname{Ker}\operatorname{Tr}^G.$$

On the other hand, $\mathbb{F}[V]_\Delta^G \subseteq \mathbb{F}[V]_\Delta^H$ by Lemma 6.1. Hence,

$$\mathbb{F}[V]_\Delta^G \subseteq \mathbb{F}[V]_\Delta^H = \operatorname{Ker}\operatorname{Tr}^H \subseteq \operatorname{Ker}\operatorname{Tr}^G.$$

□

Note that for all $g, h \in G$ and $f \in \mathbb{F}[V]$, we have the following relation

$$\Delta_{gh}(f) = g\Delta_h(f) + \Delta_g(f). \tag{6.1}$$

Thus, if $f \in \mathbb{F}[V]$ is invariant with respect to the generators $\{g_1, \ldots, g_k\}$ for G, then $f \in \mathbb{F}[V]^G$, i.e.,

$$\mathbb{F}[V]^G = \bigcap_{i=1}^{k} \mathbb{F}[V]^{\langle g_i \rangle}.$$

In Section 5.1, as a similar property, we proved that $f \in \mathbb{F}[V]_\Delta^{C_p}$ if it is a generalized invariant with respect to a generator of C_p. We can extend this result as follows.

Lemma 6.3 *Let G be a cyclic group with a generator σ and $f \in \mathbb{F}[V]$. If f is a σ-generalized invariant, then $f \in \mathbb{F}[V]^G_\Delta$.*

Proof. Using the above relation (6.1), for any $\sigma^k \in G$,

$$\Delta_{\sigma^k}(f) = (\sigma^k + \sigma^{k-1} + \cdots + 1)\Delta_\sigma(f).$$

This proves the result. □

However, this property does not hold for generalized invariants of all groups as shown in the next example.

Example 6.1. We consider the polynomial ring $\mathbb{F}_3[x, y, z]$ and the group action in Example 4.1. We showed that $yz \in \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta \cap \mathbb{F}[V]^{\langle\tau\rangle}_\Delta$. But,

$$\Delta^2_{\sigma\tau}(yz) = 2x^2 \neq 0$$

while $\Delta^3_{\sigma\tau} = 0$. Thus, $yz \notin \mathbb{F}[V]^G_\Delta$. Hence, $\mathbb{F}[V]^G_\Delta \neq \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta \bigcap \mathbb{F}[V]^{\langle\tau\rangle}_\Delta$.

Despite the previous counterexample, generating set of a group is still important for generalized invariants. Having a *non-modular generating set*, in the sense that the orders of its elements are co-prime with p provides that the generalized invariant module acts as in the non-modular case as follows.

Proposition 6.4 *If G has a non-modular generating set, then $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^G$.*

Proof. Let $A = \{g_1, \ldots, g_k\}$ be a generating set of G such that $p \nmid |\langle g_i\rangle|$ for each $i = 1, \ldots, k$. Then by Corollary 4.6, $\mathbb{F}[V]^{\langle g_i\rangle}_\Delta = \mathbb{F}[V]^{\langle g_i\rangle}$. Thus, by Lemma 6.1,

$$\bigcap_{i=1}^{k} \mathbb{F}[V]^{\langle g_i\rangle} = \mathbb{F}[V]^G \subseteq \mathbb{F}[V]^G_\Delta \subseteq \bigcap_{i=1}^{k} \mathbb{F}[V]^{\langle g_i\rangle}_\Delta = \bigcap_{i=1}^{k} \mathbb{F}[V]^{\langle g_i\rangle}.$$

Hence, $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^G$. □

Remark. By Proposition 6.4, the invariant rings of some important groups as dihedral groups, symmetric groups, reflection groups, more generally Coxeter

groups are equal to their generalized invariant module. This demonstrates that if the generalized invariant module can be calculated more efficiently, then the invariant rings of these groups will be calculated more effectively.

6.2 Generalized Invariant Module of Some Special Groups

Some groups have a fundamental importance to understand the structure of groups, such as cyclic groups, p-groups, quotient groups, p-residual subgroups. As we explain below, they will also help to comprehend the structure of the generalized invariants.

6.2.1 Cyclic p-Groups

In Chapter 5, we have analyzed the generalized invariant module of a cyclic group of order p. Now, we consider cyclic p-groups.

Proposition 6.5 (Generalized Invariants of Cyclic p-Groups) *If $G = \langle\sigma\rangle$ is a cyclic group of order p^k and $H_i = \langle\sigma^{p^{k-i}}\rangle$ is the subgroup of G of order p^i for each $i = 1, \ldots, k-1$, then*

$$\mathbb{F}[V]_\Delta^G = \mathbb{F}[V]_\Delta^{H_{k-1}} = \cdots = \mathbb{F}[V]_\Delta^{H_1}.$$

Proof. By Lemma 6.1, we have

$$\mathbb{F}[V]_\Delta^G \subseteq \mathbb{F}[V]_\Delta^{H_{k-1}} \subseteq \cdots \subseteq \mathbb{F}[V]_\Delta^{H_1}.$$

Let $f \in \mathbb{F}[V]_\Delta^{H_1}$. Then there exists ℓ such that $\Delta^\ell_{\sigma^{p^{k-1}}}(f) = 0$ and $\Delta^\ell_{\sigma^{p^{k-1}}} \neq 0$. Since $\mathrm{char}(\mathbb{F}) = p$, it follows that $\Delta_\sigma^{\ell p^{k-1}}(f) = 0$ and $\Delta_\sigma^{\ell p^{k-1}} \neq 0$. Thus, f is a generalized invariant with respect to σ. Hence, $f \in \mathbb{F}[V]_\Delta^G$ by Lemma 6.3. It completes the proof. □

Lemma 6.5 shows that the generalized invariant module of cyclic p-groups has the same structure with the module of C_p. Thus, we can extend the structural properties of $\mathbb{F}[V]_\Delta^{C_p}$ to the module of cyclic p-groups.

Corollary 6.6 *With notations in Proposition 6.5,*

(i) $\mathbb{F}[V]_\Delta^G = \operatorname{Ker} \operatorname{Tr}^{H_1}$,

(ii) $\operatorname{Im} \Delta_{H_1} \subseteq \mathbb{F}[V]_\Delta^G$,

(iii) $\mathfrak{h}_\Delta^G = \mathfrak{h}_\Delta^{H_1}$.

Proof. They are the consequences of Proposition 5.1, Proposition 5.2, Corollary 5.14 respectively with Proposition 6.5. □

6.2.2 p-Groups

Proposition 6.7 (Generalized Invariants of p-Groups) *If G is a p-group, then $\mathbb{F}[V]_\Delta^G$ is the intersection of the generalized invariant modules of its subgroups of order p, i.e.,*

$$\mathbb{F}[V]_\Delta^G = \bigcap_{\substack{\sigma \in G \\ |\sigma| = p}} \mathbb{F}[V]_\Delta^{\langle \sigma \rangle}.$$

Proof. Note that $\mathbb{F}[V]_\Delta^G = \bigcap_{g \in G} \mathbb{F}[V]_\Delta^{\langle g \rangle}$ by definition. Since any element of G has p-power order, it is enough to take generalized invariants with respect to all elements of order p by Proposition 6.5. □

The following is an immediate result of Proposition 5.1.

Corollary 6.8 *If G is a p-group, then*

$$\mathbb{F}[V]_\Delta^G = \bigcap_{\substack{\sigma \in G \\ |\sigma| = p}} \operatorname{Ker} \operatorname{Tr}^{\langle \sigma \rangle}.$$

The elements of order p in a p-group has an important structure in the group theory as considered below.

Definition. Let G be a group. The subgroup generated by the minimal normal subgroups of G is called the *socle of the group* G and denoted by $\mathrm{Soc}(G)$.

Remark. By the definition, the socle of a finite p-group G consists of the elements of order p in the center of G. Therefore, if G is also abelian,

$$\mathrm{Soc}(G) = \langle\, \sigma \in G : |\sigma| = p \,\rangle.$$

Proposition 6.9 *If G is abelian p-group, $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^{\mathrm{Soc}(G)}_\Delta$.*

Proof. Since $\mathrm{Soc}(G) = \langle\, \sigma \in G : |\sigma| = p \,\rangle$,

$$\bigcap_{\substack{\sigma \in G \\ |\sigma| = p}} \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta \subseteq \mathbb{F}[V]^{\mathrm{Soc}(G)}_\Delta.$$

Moreover, $\langle\sigma\rangle \leq \mathrm{Soc}(G)$ for each $\sigma \in G$ with $|\sigma| = p$. Thus, $\mathbb{F}[V]^{\mathrm{Soc}(G)}_\Delta \subseteq \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta$. It completes the proof. □

6.2.3 Quotient Groups

The following result is well-known and enables us to describe the invariant ring with smaller groups.

Lemma 6.10 *Let V be a representation of G and H be a normal subgroup of G. Then G acts on the invariant ring $\mathbb{F}[V]^H$. In particular, $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$.*

Proof. Let $\sigma \in G$, $\tau \in H$. By the normality of H in G, we have $\tau\sigma = \sigma\tau'$ for some $\tau' \in H$. If $f \in \mathbb{F}[V]^H$, then

$$\tau(\sigma f) = (\tau\sigma)f = (\sigma\tau')f = \sigma f.$$

Therefore, $\sigma f \in \mathbb{F}[V]^H$ and G acts on $\mathbb{F}[V]^H$. Since the action is defined, it follows that $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^G$. Note that H trivially acts on $\mathbb{F}[V]^H$. Hence, $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$. □

Also, we can say that G acts on the generalized invariant module $\mathbb{F}[V]^H_\Delta$, which is proved in the next section after the required structure theorem. However, in order to describe generalized invariant module of G using smaller groups H and G/H, we need an additional condition.

Proposition 6.11 *If $H \trianglelefteq G$ and $\mathbb{F}[V]^H_\Delta = \mathbb{F}[V]^H$, then $\mathbb{F}[V]^G_\Delta = (\mathbb{F}[V]^H_\Delta)^{G/H}_\Delta$.*

Proof. Since G acts on $\mathbb{F}[V]^H$, clearly we have $(\mathbb{F}[V]^H)^G_\Delta = \mathbb{F}[V]^G_\Delta$ and also, G/H acts on $\mathbb{F}[V]^H$. Moreover, the normal subgroup H satisfies

$$(\sigma H - H)^\ell = (\sigma - 1)^\ell H^\ell$$

for any $\ell \in \mathbb{N}$. Thus, we obtain that $(\mathbb{F}[V]^H)^{G/H}_\Delta = \mathbb{F}[V]^G_\Delta$. □

Remark. The previous proposition does not hold without the additional condition $\mathbb{F}[V]^H_\Delta = \mathbb{F}[V]^H$. Example 6.1 shows that $\mathbb{F}[V]^G_\Delta \neq \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta \cap \mathbb{F}[V]^{\langle\tau\rangle}_\Delta$ by the given representation G, in other words,

$$\mathbb{F}[V]^G_\Delta \neq (\mathbb{F}[V]^{\langle\sigma\rangle}_\Delta)^{\langle\tau\rangle}_\Delta$$

since $G/\langle\sigma\rangle \cong \langle\tau\rangle$.

6.2.4 p-Residual Subgroups

Definition. The subgroup generated by all elements of G whose order is coprime with p is called the *p-residual subgroup* of G, and it is denoted commonly by $O^p(G)$. However, we simply denote it with N in the rest of the text:

$$N = \langle\, g \in G \mid \gcd(\,|g|, p\,) = 1 \,\rangle.$$

The following is the known results about p-residual subgroups.

Lemma 6.12 *The p-residual subgroup N of a group G is characteristic in G. In particular, N is normal in G.*

Proof. Let φ be an automorphism of G. If the order of $\varphi(g)$ for $g \in N$ were divided by p, $p \,|\, |g|$ because $\varphi \in \mathrm{Aut}(G)$. Thus, N is characteristic in G. The last result follows by Lemma 2.1. □

Note that for the p-residual subgroup N of G, the quotient group G/N is a p-group by the definition.

Corollary 6.13 *We have the following results about p-residual subgroups:*

(i) $\mathbb{F}[V]^N_\Delta = \mathbb{F}[V]^N$.

(ii) $\mathbb{F}[V]^G_\Delta = (\mathbb{F}[V]^N_\Delta)^{G/N}_\Delta$.

Proof. By the definition of a p-residual group, N has a non-modular generating set. Thus, the results are immediate consequences of Proposition 6.4 and Proposition 6.11. □

6.3 Structure Theorem of Generalized Invariants

In this section, we consider a general structure of generalized invariants module of any finite group G. Actually, this structure gives the core modules of the generalized invariant module with their intersection. Even though it can not determine all structural properties, we get some important consequences using the following structure theorem.

Theorem 6.14 (Structure of the Generalized Invariant Module) *For any finite group G, $\mathbb{F}[V]^G_\Delta$ is the intersection of the generalized invariant modules of subgroups of order p with the invariant ring of p-residual subgroup N, i.e.,*

$$\mathbb{F}[V]^G_\Delta = (\bigcap_{\substack{\sigma\in G\\ |\sigma|=p}} \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta)\bigcap \mathbb{F}[V]^N.$$

Proof. Generalized invariant module $\mathbb{F}[V]^G_\Delta$ clearly lies in the righthand-side of the equation by Lemma 6.1 and Corollary 6.13. For the converse, suppose that f is in the above intersection. Let g be a nonidentity element of G of order $p^k m$. When $m = 1$, $|g| = p^k$. By Proposition 6.5, there exists ℓ such that $\Delta^\ell_g(f) = 0$ and $\Delta^\ell_g \neq 0$. If $m \neq 1$, $g^{p^k} \in N$ so that $(g^{p^k} - 1)(f) = 0$ and $g^{p^k} - 1 \neq 0$. Therefore, $\Delta^{p^k}_g(f) = 0$ and $\Delta^{p^k}_g \neq 0$. Since g is arbitrary, $f \in \mathbb{F}[V]^G_\Delta$. □

Remark. This structure theorem provides a useful method to compute $\mathbb{F}[V]^G_\Delta$ by first calculating all generalized invariants of elements just of order p in $G\backslash N$ and then intersecting them with the invariant ring $\mathbb{F}[V]^N$.

We have the following result by Proposition 6.9

Corollary 6.15 *For a finite abelian group G,*

$$\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^{\mathrm{Soc}(G)}_\Delta \bigcap \mathbb{F}[V]^N.$$

Using the following lemma, it is enough to take the quotient group PN/N of order p^{a-b} for a Sylow subgroup P of G instead of all elements of order p in the Structure Theorem for the Generalized Invariant Module. Although the proof of the Lemma is elementary, it is given for the completeness of the section.

Lemma 6.16 *If G is a group of order $p^a m$ with $(p, m) = 1$, P is a Sylow p-subgroup of G, and H is a normal subgroup of G of order $p^b n$ with $(p, n) = 1$, then $|P \cap H| = p^b$ and $|PH/H| = p^{a-b}$.*

Proof. By the diamond isomorphism theorem, $PH \leq G$, $H \trianglelefteq PH$, $P \cap H \trianglelefteq P$ and $PH/H \cong P/P \cap H$. Since $P \leq PH$ and $PH \leq G$, Lagrange Theorem implies

that $|PH| = p^a k$. Then $|H| \mid |PH|$; so, we have $|PH/H| = p^{a-b}u$ for some integer u with $(p, u) = 1$. Because $|P/P \cap H|$ is a p-power and $PH/H \cong P/P \cap H$, we obtain that $u = 1$. Therefore, $|P/P \cap H| = |PH/H| = p^{a-b}$. Hence, $|P \cap H| = p^b$. □

Corollary 6.17 *If N is proper in G and P is a Sylow p-subgroup of G, then*

$$\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^P_\Delta \bigcap \mathbb{F}[V]^N.$$

Proof. Let $|G| = p^a m$ such that $(p, m) = 1$ and $|N| = p^b m$ for some non-negative integer $b < a$. By Lemma 6.16, we obtain $|PN/N| = p^{a-b}$. Since G/N is the largest p-group onto which G surjects and $PN/N \leq G/N$, $|G/N| = p^{a-b}$ and $G/N = PN/N$. Furthermore, $G = PN$ since $|PN| = \frac{|P||N|}{|P|} = p^a m$. Then by Proposition 6.11, we have

$$\begin{aligned}
\mathbb{F}[V]^G_\Delta &= (\mathbb{F}[V]^N_\Delta)^{G/N}_\Delta \\
&= (\mathbb{F}[V]^N)^{G/N}_\Delta \\
&= (\mathbb{F}[V]^N)^{PN/N}_\Delta \\
&= \mathbb{F}[V]^N \bigcap \mathbb{F}[V]^P_\Delta.
\end{aligned}$$

□

Remark. Previous corollary emphasizes that the generalized invariant module of Sylow p-subgroups plays a fundamental role to understand the difference of the generalized invariant module of a group from its invariant ring.

Example 6.2. Consider a representation of the cyclic group $G = C_2 \times C_p$ in 2-dimension represented by

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

By Theorem 6.14 and Proposition 5.7,

$$\begin{aligned}\mathbb{F}[V]^G_\Delta &= \mathbb{F}[V]^{C_p}_\Delta \bigcap \mathbb{F}[V]^{C_2} \\ &= \Big(\bigoplus_{i=0}^{p-2} y^i \mathbb{F}[x, N^{C_p}(y)]\Big) \bigcap \big(\mathbb{F}[x^2, y^2] \oplus xy\mathbb{F}[x^2, y^2]\big).\end{aligned}$$

Hence, $\mathbb{F}[V]^G_\Delta = \left(\bigoplus_{i=0}^{p-1} y^{2i}\mathbb{F}[x^2, N^2(y)]\right) \oplus \left(\bigoplus_{i=0}^{p-1} xy^{2i+1}\mathbb{F}[x^2, N^2(y)]\right)$ for the h.s.o.p. $\{x^2, N^2(y)\}$ of $\mathbb{F}[V]^G$.

In general, for $G = C_p \times C_q$ with $q \,|\, (p-1)$,

$$\begin{aligned}\mathbb{F}[V]^G_\Delta &= \mathbb{F}[V]^{C_p}_\Delta \bigcap \mathbb{F}[V]^{C_q} \\ &= \Big(\bigoplus_{i=0}^{p-2} y^i \mathbb{F}[x, N^{C_p}(y)]\Big) \bigcap \Big(\bigoplus_{\substack{i+j=q \\ i,j<q}} x^i y^j \mathbb{F}[x^q, y^q]\Big).\end{aligned}$$

$\mathbb{F}[V]^G_\Delta = \left(\bigoplus_{i=0}^{p-1} y^{2i}\mathbb{F}[x^2, N^2(y)]\right) \oplus \left(\bigoplus_{i=0}^{p-1} xy^{2i+1}\mathbb{F}[x^2, N^2(y)]\right)$ for the h.s.o.p. $\{x^2, N^2(y)\}$ of $\mathbb{F}[V]^G$.

Example 6.3. Let G be the group $\mathrm{SL}_2(\mathbb{F}_3)$ of order 24 for the vector space V over the field $\mathbb{F}_3$ of characteristic 3. It is generated by

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

Then its p-residual subgroup N is generated by the first two elements in the above set and has order 8; also clearly, the other element generates the cyclic group C_3. By Proposition 5.7 and using calculations in Magma, we obtain that

$$\begin{aligned}\mathbb{F}[V]^{C_3}_\Delta &= \mathbb{F}[f_1, f_2] \bigoplus h\mathbb{F}[f_1, f_2] \\ \mathbb{F}[V]^N &= \mathbb{F}[hf_2 + f_1^4, f_1 f_2] \bigoplus (f_2^2 + f_1^6)\mathbb{F}[hf_2 + f_1^4, f_1 f_2],\end{aligned}$$

where $\{f_1, f_2\}$ and $\{hf_2 + f_1^4, f_1 f_2\}$ are h.s.o.p. of $\mathbb{F}[V]^{C_3}$ and $\mathbb{F}[V]^N$, respectively,

and

$$\begin{aligned} f_1 &= x, \\ f_2 &= y^3 + 2x^2y, \\ h &= y. \end{aligned}$$

We know that $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^{C_3}_\Delta \bigcap \mathbb{F}[V]^N$ by Theorem 6.14. If we rewrite this intersection using the h.s.o.p. $\{f_1 f_2, f_2^2 + f_1^6\}$ of $\mathbb{F}[V]^G$, then

$$\mathbb{F}[V]^G_\Delta = \mathbb{F}[f_1 f_2, f_2^2 + f_1^6] \bigoplus (hf_2 + f_1^4)\mathbb{F}[f_1 f_2, f_2^2 + f_1^6].$$

6.3.1 Results of the Structure Theorem

The following lemma is promised in Section 6.2.3. Therefore, it is given as a consequence of Theorem 6.14 in this section.

Lemma 6.18 *Let V be a representation of G and H be a normal subgroup of G. Then G acts on the generalized invariant module $\mathbb{F}[V]^H_\Delta$.*

Proof. If $f \in \mathbb{F}[V]^H_\Delta$ and $\tau \in G \setminus H$, then for each element $\sigma \in H$ of order p, $\mathbb{F}[V]^H_\Delta \subseteq \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta$ and $\mathrm{Tr}^{\langle\sigma\rangle}(f) = 0$ by Lemma 6.1 and Proposition 5.1. Because of the normality of H, we have

$$\mathrm{Tr}^{\langle\sigma\rangle}(\tau f) = \tau \mathrm{Tr}^{\langle\sigma\rangle}(f) = 0.$$

Thus,

$$\tau f \in \bigcap_{\substack{\sigma \in H \\ |\sigma| = p}} \mathrm{Ker}\, \mathrm{Tr}^{\langle\sigma\rangle} = \bigcap_{\substack{\sigma \in H \\ |\sigma| = p}} \mathbb{F}[V]^{\langle\sigma\rangle}_\Delta.$$

Moreover, if f is invariant, so is τf by Lemma 6.10. Hence, Theorem 6.14 shows that $\tau f \in \mathbb{F}[V]^H_\Delta$. □

In Section 6.2.1, we obtained the structure of the generalized invariant module of cyclic p-groups as the kernel of the transfer map. Now, we extend this result

to the groups in which the index of their p-residual subgroups is p.

Proposition 6.19 *Let G be a finite group and N be its p-residual subgroup. If $[G : N] = p$, then*

$$\mathbb{F}[V]^G_\Delta = \operatorname{Ker} \operatorname{Tr}^G_N.$$

Proof. Since $|G/N|$ is a cyclic group of order p, $\mathbb{F}[V]^{G/N}_\Delta = \operatorname{Ker} \operatorname{Tr}^{G/N}$. Thus the structure theorem gives

$$\mathbb{F}[V]^G_\Delta = \operatorname{Ker} \operatorname{Tr}^{G/N} \bigcap \mathbb{F}[V]^N.$$

Hence, $\mathbb{F}[V]^G_\Delta = \operatorname{Ker} \operatorname{Tr}^G_N$. □

Chapter 7

Generalized Invariants and Ladder Method

In Section 4.4, it is proved that the usual invariants and the generalized invariants are the same for non-modular representations. Also, in this chapter, we answer the question when they are equal in the modular case. Our tool is the ladders which are used efficiently in characteristic zero (see [25], [34], [53]). The ladder method is also studied in the modular case (see [42], [4]). In the first section, we review these studies. Then, we give the results obtained from the ladder technique.

7.1 Ladder Method

It is known that $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$ for a normal subgroup H of G (Lemma 6.10). Thus, computing $\mathbb{F}[V]^G$ can be reduced to the problem of computing $\mathbb{F}[V]^H$ and then G/H-invariants of $\mathbb{F}[V]^H$. However, $\mathbb{F}[V]^H$ is generally not a polynomial ring. It causes a difficulty on computing G/H-invariants of $\mathbb{F}[V]^H$. When G/H is a reductive group, this problem can be solved by replacing successfully $\mathbb{F}[V]^H$ by a polynomial ring as follows:

Let $D = (\mathbb{F}[V]^{H,+})^2$ be the ideal of the decomposable invariants in $\mathbb{F}[V]^H$. Then D is G/H-stable. Since G/H is a reductive group, it follows that

$$\mathbb{F}[V]^H = D \oplus Q,$$

for some G/H-stable complement of D in $\mathbb{F}[V]^H$. Thus, a basis $\{f_1, \ldots, f_m\}$ of Q can be extended to a generating set of $\mathbb{F}[V]^H$. We consider a G/H-action on the algebra $\mathbb{F}[y_1, \ldots, y_m]$ with indeterminates $y_1, \ldots, y_m$ of degree 1 using the G/H-action on Q:

$$\sigma \cdot y_i := \sum_{j=1}^{r} \alpha_{i,j}^{\sigma} y_j,$$

where $\alpha_{i,j}^{\sigma}$ is given by

$$\sigma \cdot f_i = \sum_{j=1}^{r} \alpha_{i,j}^{\sigma} f_j.$$

Let W denote the representation dual to the space generated by $y_1, \ldots, y_m$. Then we have the following G/H-equivariant epimorphism

$$\rho : \mathbb{F}[W] \cong \mathbb{F}[y_1, y_2, \ldots, y_m] \to \mathbb{F}[f_1, f_2 \ldots, f_m] = \mathbb{F}[V]^H,$$

defined as $\rho(y_i) = f_i$ for each $i = 1, \ldots, m$. Since G/H is a reductive group, the restriction of ρ to $\mathbb{F}[W]^{G/H}$

$$\mathbb{F}[W]^{G/H} \cong \mathbb{F}[y_1, y_2, \ldots, y_m]^{G/H} \to \mathbb{F}[f_1, f_2 \ldots, f_m]^{G/H} = \mathbb{F}[V]^G$$

is an epimorphism.

If G/H is not reductive, there are some modifications as follows. In this case, we need a G/H-stable vector space Q as in the previous case. But here we only give the desired construction since our aim is not the computation of $\mathbb{F}[V]^G$.

Let H be a normal subgroup of G. Suppose that $\{f_1, f_2, \ldots f_m\}$ is a set of generators for the invariant ring $\mathbb{F}[V]^H$. Define

$$Q := \mathrm{span}_{\mathbb{F}}\{\sigma \cdot f_i \,|\, \sigma \in G \text{ and } i = 1, \ldots, m\}.$$

Then Q is a G/H-stable vector space over $\mathbb{F}$. Take $\{h_1, h_2 \ldots, h_r\}$ as a basis for Q. We consider the polynomial ring $\mathbb{F}[y_1, y_2, \ldots, y_r]$ of Krull dimension r and define an action of $\sigma \in G/H$ on $\mathbb{F}[y_1, y_2, \ldots, y_r]$ as follows:

$$\sigma \cdot y_i := \sum_{j=1}^{r} \alpha_{i,j}^{\sigma} y_j$$

where $\alpha_{i,j}^{\sigma}$ is defined by

$$\sigma \cdot h_i = \sum_{j=1}^{r} \alpha_{i,j}^{\sigma} h_j.$$

Let $\mathbb{F}[W] = \mathbb{F}[y_1, y_2, \ldots, y_r]$ such that $W \cong Q$ is the r-dimensional G/H-representation dual to $\text{span}_{\mathbb{F}}\{y_1, y_2, \ldots, y_r\}$. Define

$$\rho : \mathbb{F}[W] \cong \mathbb{F}[y_1, y_2, \ldots, y_r] \to \mathbb{F}[h_1, h_2 \ldots, h_r] = \mathbb{F}[V]^H$$

as $\rho(y_i) = h_i$ for all $i = 1, \ldots, r$. By the above construction, ρ is G/H-equivariant algebra surjection. The restriction of ρ into $\mathbb{F}[y_1, y_2, \ldots, y_r]^{G/H}$ is defined onto $(\mathbb{F}[V]^H)^{G/H} = \mathbb{F}[V]^G$, but not surjective as shown in the following example.

Example 7.1. [4, Example 14.2.3] Consider the field $\mathbb{F}_4 = \{0, 1, w, w^2\}$ of order 4 with $w^2 + w + 1 = 0$. Consider the following 3-dimensional representation G generated by

$$\sigma^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \tau^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ w & 0 & 1 \end{bmatrix}.$$

Let G act on the polynomial ring $\mathbb{F}_4[V] = \mathbb{F}_4[x, y, z]$ and H be the subgroup of G generated by σ. Then H has the order 4 and it is a normal subgroup of G since the order of G is 8. By calculations in Magma, we can easily obtain that

$\mathbb{F}[V]^H = \mathbb{F}_4[f_1, f_2, f_3, f_4]$, where

$$\begin{aligned} f_1 &= x, \\ f_2 &= y^2 + xy, \\ f_3 &= y^3 + xy^2 + xz^2 + x^2z, \\ f_4 &= z^4 + x^2z^2 + y^2z^2 + xyz^2 + xy^2z + x^2yz. \end{aligned}$$

Let Δ denote $\tau - 1$. Then G/H-action on $\mathbb{F}[V]^H$ is given by

$$\begin{aligned} \Delta(f_1) &= 0, \\ \Delta(f_2) &= 0, \\ \Delta(f_3) &= f_1^3, \\ \Delta(f_4) &= f_1^2(f_2 + f_1^2). \end{aligned}$$

Let $W = 2V_1 \oplus 2V_2$ such that the dual space W^* has the basis $\{u_1, u_2, u_3, v_3, u_4, v_4\}$ with

$$\begin{aligned} \rho(u_i) &= u_i \text{ for } i = 1, 2, 3, 4, \\ \rho(v_i) &= u_i + v_i \text{ for } i = 3, 4. \end{aligned}$$

Now, define $\rho : \mathbb{F}_4[W] \to \mathbb{F}_4[V]^H$ as

$$\begin{aligned} \rho(u_1) &= f_1, \\ \rho(u_2) &= f_2, \\ \rho(v_3) &= f_3, \\ \rho(u_3) &= \Delta(f_3) = f_1^3, \\ \rho(v_4) &= f_4 \\ \rho(u_4) &= \Delta(f_4) = f_1^4 + f_1^2 f_2. \end{aligned}$$

Then ρ is G/H-equivariant surjective map. Consider the image

$$\begin{aligned}\rho(\mathbb{F}_4[W]^{G/H}) &= \rho(\mathbb{F}_4[u_1, u_2, v_3^2 + u_3v_3, v_4^2 + u_4v_4, u_3v_4 + u_4v_3]) \\ &= \mathbb{F}_4[f_1, f_2, f_3^2 + f_1^3f_3, f_4^2 + f_1^4f_4 + f_1^2f^2f_4, f_1^3f_4 + f_1^4f_3 + f_1^2f_2f_3].\end{aligned}$$

Let $f_5 := y^5 + xz^4 + x^3y^2 + x^4z$. Since $\Delta(f_5) = x(wx)^4 + x^4(wx) = 0$, $f_5 \in \mathbb{F}[V]^G$. If $f_5 \in \rho(\mathbb{F}_4[W]^{G/H})$, then $f_5 \in \mathbb{F}_4[f_1, f_2]_5$ because $\deg(f_i) = i$. However, each element of $\mathbb{F}_4[f_1, f_2]_5$ is divisible by $f_1 = x$ and the leading monomial of f_5 is y^5. Thus, we obtain $f_5 \notin \mathbb{F}_4[f_1, f_2]_5$. So, $f_5 \notin \rho(\mathbb{F}_4[W]^{G/H})$. Hence, the restriction of the epimorphism ρ into $\mathbb{F}_4[W]^{G/H}$ is not surjective.

7.2 The Results

Now, we consider the relation of the ladder method with generalized invariants. Actually, we don't give this method as a convenience for the calculation of generalized invariants. Only we use it as a tool to answer the question when generalized invariants are the usual invariants in modular case.

We saw in the Example 7.1 that the ladder method is not efficient as in the reductive groups since the restriction of the map ρ into the invariant ring $\mathbb{F}[W]^{G/H}$ is not generally surjective. On the contrary to this situation, we can obtain the following result.

Lemma 7.1 *Suppose that H is a normal subgroup of G such that the quotient G/H is a p-group. By the notations introduced in Section 7.1, if $y_i \notin \mathbb{F}[W]^{G/H}$, then*

$$h_i = \rho(y_i) \notin \mathbb{F}[V]^G.$$

Proof. If y_i is not in $\mathbb{F}[W]^{G/H}$, we can consider non-zero $\Delta_\sigma(y_i)$ for $\sigma \in G/H$. Because of the p-group structure of G/H, $\Delta_\sigma(y_i) = y_{i-1}$ after a reordering of the indeterminates. Suppose that $h_i \in \mathbb{F}[V]^G$. Then for G/H-equivariant map ρ, we have

$$h_{i-1} = \rho(y_{i-1}) = \rho\Delta(y_i) = \Delta(\rho(y_i)) = \Delta(h_i) = 0.$$

Since h_{i-1} is a basis element, it is a contradiction. So, $h_i \notin \mathbb{F}[V]^G$. □

The following gives the main result of this chapter.

Theorem 7.2 *The group G has a non-modular generating set if and only if $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^G$. In particular, $G = N$ if and only if $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^G$.*

Proof. If G has generators whose order is coprime with p, then the equality $\mathbb{F}[V]^G_\Delta = \mathbb{F}[V]^G$ is satisfied by Proposition 6.4. For the converse statement, let N be the p-residual subgroup of G and suppose that N is proper in G. Since N is a normal subgroup, we can use the construction given Section 7.1 and the same notations only changing H with N. Then there exists $y_i \in \mathbb{F}[W]^{G/N}_\Delta \backslash \mathbb{F}[W]^{G/N}$. Since ρ is G/N-equivariant, $\rho(y_i)$ is also in $\mathbb{F}[V]^G_\Delta$, and not in $\mathbb{F}[V]^G$ by Lemma 7.1. Hence, $\mathbb{F}[V]^G_\Delta \neq \mathbb{F}[V]^G$. □

Remark. The necessary and sufficient condition of the previous theorem shows not only that usual and generalized invariants are same for a representation with non-modular generating set, but also it gives information about the group structure when these two structures are same.

BIBLIOGRAPHY

[1] D. J. Benson, *Polynomial Invariants of Finite Groups*, London Mathematical Society Lecture Note Series, 190. Cambridge Univ. Press, Cambridge, 1993.

[2] W. Bosma, J. Cannon, and C. Playoust, The Magma Algebra System I The User Language *J. Symbolic Comput.* **24** (1997), 235–265.

[3] H. E. A. E. Campbell, I. P. Hughes, Vector Invariants of $U_2(\mathbb{F}_p)$: a Proof of a Conjecture of Richman, *Adv. Math.* **126** (1997), no. 1, 1–20.

[4] H. E. A. E. Campbell, D. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Mathematical Science 139. Invariant Theory and Algebraic Transformation Groups, 8. Springer-Verlag, Berlin, 2011.

[5] C. Chevalley, Invariants of Finite Groups Generated by Reflections, *Amer. J. Math.*, **77** (1955), 778–782.

[6] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, third ed., Undergraduate Texts in Mathematics. Springer, New York, 2007.

[7] H. S. M. Coxeter, Discrete Groups Generated by Reflections, *Ann. Of Math.*, **35** (1934), 588–621.

[8] H. Derksen, G. Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I. Encyclopaedia of Mathematical Sciences, 130. Springer-Verlag, Berlin, 2002.

[9] D. Erdemirci Erkuş, U. Madran, On Generators of the Hilbert Ideal for Cyclic Groups in Modular Invariant Theory, *J. Algebra* **422** (2015), 306–317.

[10] D. Erdemirci Erkuş, U. Madran, On Generalized Invariants of Cyclic Groups, *J. Pure and Applied Algebra* **219** (2015), no. 6, 2463–2470.

[11] D. Erdemirci Erkuş, U. Madran, The Structure of Modular Generalized Invariants, submitted.

[12] P. Fleischmann, The Noether Bound in Invariant Theory of Finite Groups, *Adv. Math.* **156** (2000), no. 1, 23–32.

[13] P. Fleischmann, On invariant theory of finite groups, *Invariant theory in all characteristics*, CRM Proc. Lecture Notes, 35, Amer. Math. Soc., Providence, RI, **35** (2004) 43–69.

[14] J. Fogarty, *On Noether's Bound for Polynomial Invariants of Finite Groups*, Electronic Research Announcements of the AMS **7** (2001), 5–7.

[15] G. Gaeta, F. D. Grosshans, J. Scheurle, S. Walcher, Reduction and Reconstruction for Symmetric Ordinary Differential Equations, *J. Differential Equations* **244** (2008), no. 7, 1810–1839.

[16] P. Gordan, Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist, *J. Reine Angew. Math.* **69** (1868), 323–354.

[17] F. D. Grosshans, S. Walcher, Modules of Higher Order Invariants, *Proceedings of the Amer. Math. Soc.* **143** (2015), no. 2, 531–542.

[18] D. Hilbert, Über die Theorie der algebraischen Formen, *Math. Ann.* **36** (1890), 473–534.

[19] D. Hilbert, Über die vollen Invariantensysteme, *Math. Ann.* **42** (1893), 313–370.

[20] I. Hughes, G. Kemper, Symmetric Power of Modular Representations, Hilbert Series and Degree Bounds, *Comm. Algebra* **28** (2000), no. 4, 2059–2089.

[21] V. G. Kac and D. H. Peterson, Generalized invariants of groups generated by reflections, *Geometry today (Rome, 1984), Progr. Math.*, Birkhäuser Boston, Boston, MA **60** (1985), 231–249.

[22] V. G. Kac, K. I. Watanabe, Finite Linear Groups whose Ring of Invariants is a Complete Intersection, *Bull. Amer. Math. Soc.* (N.S.) **6** (1982), no. 2, 221–223.

[23] R. Kane, *Reflection groups and invariant theory*, CMS Books in Mathematics, 5. Springer-Verlag, New York, 2001.

[24] M. Kohls, M. Sezer, Gröbner Bases for the Hilbert Ideal and Coinvariants of the Dihedral Group D_{2p}, *Mathematische Nachrichten* **285** (2012), no. 16, 1974–1980.

[25] P. Littelmann, Koreguläre und äquidimensionale Darstellungen, *J. Algebra* **123** (1989), no. 1, 193–222.

[26] U. Madran, *Project on Generalized Invariants*, avaliable online: http://homes.ieu.edu.tr/%7eumadran/ginv, Accessed: 2015-February-13.

[27] H. Nakajima, Regular Rings of Invariants of Unipotent Groups, *J. Algebra* **85** (1983), 253–286.

[28] F. Neumann, M. D. Neusel and L. Smith, Rings of generalized and stable invariants of pseudoreflections and pseudoreflection groups, *J. Algebra* **182** (1996), no. 1, 85–122.

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

[30] M. D. Neusel, M. Sezer, The Invariants of Modular Indecomposable Representations of $\mathbb{Z}_{p^2}$, *Math. Ann.* **341** (2008), no. 3, 575–587.

[31] M. Neusel and L. Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monograms **94**, Amer. Math. Soc., Providence, RI, 2002.

[32] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1915), no. 1, 89–92.

[33] E. Noether, Der Endlichkeitssatz der Invarianten endlicher linear Gruppen der Charakteristik p, *Nachr. Akad. Wiss.* Göttingen (1926) 28–35.

[34] V. L. Popov, Constructive Invariant Theory, *Young Tableaux and Schur Functors in Algebra and Geometry (Toruń, 1980)*, Astérisque, **87**, Soc. Math. France, Paris, 303334, 1981.

[35] D. R. Richman, On Vector Invariants over Finite Fields, *Adv. Math.* **81** (1990), no. 1, 30–65.

[36] D. R. Richman, Invariants of Finite Groups over Fields of Characteristic p, *Adv. Math.* **124** (1996), no. 1, 25–48.

[37] J. P. Serre, Groupes Finis d'Automorphismes d'Anneaux Locaux Rguliers (French) *Colloque d'Algbre* (1968), 8–11.

[38] M. Sezer, A Note on the Hilbert Ideals of a Cyclic Group of Prime Order, *J. Algebra* **318** (2007), no. 1, 372–376.

[39] M. Sezer, R. J. Shank, On the Coinvariants of Modular Representations of Cyclic Groups of Prime Order, *J. Pure Appl. Algebra* **205** (2006), no. 1, 210–225.

[40] M. Sezer, Ö. Ünlü, Hilbert Ideals of Vector Invariants of S_2 and S_3, *Journal of Lie Theory* **22** (2012), no. 4, 1181–1196.

[41] R. J. Shank, D. L. Wehlau, The Transfer in Modular Invariant Theory, *J. Pure Appl. Algebra*, **142** (1999), 63–77.

[42] R. J. Shank, D. L. Wehlau, Computing Modular Invariants of p-Groups, *J. Symbolic Comput.*, **34** (2002), 307–327.

[43] R. J. Shank, D. L. Wehlau, Decomposing Symmetric Powers of Certain Modular Representations of Cyclic Groups, Symmetry and Spaces, *Progress in Mathematics*, Birkhuser Boston, Inc., Boston, MA, **278** (2010) 169–196.

[44] R. J. Shank, D. L. Wehlau, Noether Numbers for Subrepresentations of Cyclic Groups of Prime Order, *Bull. London Math. Soc.* **34** (2002), no. 4, 438–450.

[45] G. C. Shephard, J. A. Todd, Finite Unitary Reflection Groups, *Canadian J. Math.* **6** (1954), 274–304.

[46] L. Smith, On the Invariant Theory of Finite Pseudoreflection Groups, *Arch. Math.* (Basel) **44** (1985), no. 3, 225–228.

[47] L. Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters Ltd., Wellesley, MA, 1995.

[48] P. Symonds, Cyclic Group Actions on Polynomial Rings, *Bull. Lond. Math. Soc.* **39** (2007), no. 2, 181–188.

[49] P. Symonds, On the Castelnuovo-Mumford Regularity of Rings of Polynomial Invariants, *Ann. of Math.* (2) **174** (2011), no. 1, 499–517.

[50] R. Tanimoto, The image membership algorithm for twisted derivations in modular invariant theory, *Saitama Math. J.*, **29** (2012), 55–64.

[51] H. Toda, Cohomology mod 3 of the Classifying Space BF_4 of the Exceptional Group F_4, *J. of Math.*, Kyto Univ. **13** (1973), 97–115.

[52] D. Wehlau, Equidimensional Representations of 2-Simple Groups, *J. Algebra* **154** (1993), no. 2, 437–489

[53] D. L. Wehlau, Invariants for the Modular Cyclic Group of Prime Order via Classical Invariant Theory, *J. Eur. Math. Soc.* **15** (2013), no. 3, 775–803.

VITA

Deniz Erdemirci Erkuş was born in Ankara, Turkey, on July 30, 1985, the daughter of Leyla and Mevlüt Erdemirci. In 2011, she married to Soner Erkuş of Elazığ, Turkey.

She received her B.Sc. degree in 2008 from the Department of Mathematics, in Dokuz Eylül University. She began Ph.D. Program with Dilek Pusat in the Department of Mathematics of İzmir Institute of Technology. She took part in the TÜBİTAK (The Scientific and Technological Research Council of Turkey) project titled *Homological Properties of Supplemented and Complemented Submodules* between the years 2008-2010. She spent her 2009-2010 Spring semester at the University of Murcia in Spain working with Pedro A. Guil Assensio on the project included in the learning agreement of the Erasmus entitled *Pure-Injectivity in some Module Categories*.

She continued her academic studies with Uğur Madran in the Department of Mathematics of İzmir University of Economics since 2012. They have studied on the TÜBİTAK project (114F059) titled *The Structural Properties of Generalized Invariant Module and the Relation with Invariant Ring* since 2014.

She completed the requirements for the doctor of philosophy degree at İzmir University of Economics. She has been awarded by TÜBİTAK as a Ph.D. scholarship since 2009. Her research interest including (modular) invariant theory, commutative algebra and representation theory.