# On the Module of Derivations of Certain Rings

Arindam Dey

Department of Mathematics

Indian Institute of Technology Guwahati

Guwahati, India- 781039

June, 2019

# On the Module of Derivations of Certain Rings

*Thesis Submitted*

*in partial fulfillment of the Degree of*

Doctor of Philosophy

*by*

**Arindam Dey**

(11612312)

*under the guidance of*

**Dr. Vinay Wagh**


**to the**

**DEPARTMENT OF MATHEMATICS**

**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI**

**GUWAHATI - 781039, ASSAM**

# Declaration

I do hereby declare that this thesis entitled **On the Module of Derivations of Certain Rings** is a presentation of my original research work done under the supervision of **Dr. Vinay Wagh**, Department of Mathematics, Indian Institute of Technology Guwahati for the award of the degree of Doctor of Philosophy and this work has not been submitted elsewhere for a degree.

June, 2019

Arindam Dey
Roll No. 11612312
Department of Mathematics
Indian Institute of Technology Guwahati

# Certificate

It is to certify that the work contained in this thesis entitled **On the Module of Derivation of Certain Rings** has been carried out by **Arindam Dey**, a student in the Department of Mathematics, Indian Institute of Technology Guwahati, under my supervision for the award of the degree of Doctor of Philosophy and this work has not been submitted elsewhere for a degree.

June, 2019

Dr. Vinay Wagh
Assistant Professor
Department of Mathematics
Indian Institute of Technology Guwahati

# Acknowledgements

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of the Ph.D. program. I am thankful for their aspiring guidance, invaluable constructive criticism and friendly advice during this work. I am sincerely grateful to them for sharing their truthful and illuminating views.

The work done in this thesis is a joint work with my Ph.D. supervisor Dr. Vinay Wagh. I am indebted to him for his invaluable guidance. His comments and discussions are always helpful to me. I owe more to him than I possibly can express here.

I am grateful to Prof. R. V. Gurjar of Indian Institute of Technology Bombay, for his valuable suggestions throughout. I am also thankful to Dr. Anupam Saikia, Dr. Shyamashree Upadhyay, Dr. K. V. Srikanth and many other teachers for the suggestions they have provided during this work.

I am thankful to Prof. Daniel Daigle of Ottawa University and Prof. J. K. Verma of Indian Institute of technology Bombay for reviewing the thesis and providing necessary corrections.

I am thankful to the authorities of Indian Institute of Technology Guwahati, for providing the necessary facilities required. I also thank the staff and members of the Department of Mathematics, Indian Institute of Technology Guwahati.

I can not thank my friends enough for the help and support I had received from them during the course of this work.

Finally I thank my family members for their support. I can never thank my parents enough for their understanding and constant encouragement. Last but not the least, I thank my wife Dipika for her love, understanding and inspiration.

# Abstract


## Introduction (Chapter 1)

In this chapter we discuss the idea of a derivation map over a ring (we only consider rings that are commutative, with unity). We will see that the set of all derivation maps over a ring forms a module, called the module of derivation. Then we discuss the concept of Kähler differential, and we discuss the relation between module of derivation and module of Kähler differentials. For a field $\mathbf{k}$, a commutative $\mathbf{k}$-algebra $A$ and an $A$-module $M$, we discuss the $A$-module isomorphism $\mathrm{Der}_{\mathbf{k}}(A, M) \cong \mathrm{Hom}_{\mathbf{k}}(\Omega_{A/\mathbf{k}}, M)$. Where $\mathrm{Der}_{\mathbf{k}}(A, M)$ is the module of $\mathbf{k}$-derivations from $A$ to $M$, and $\Omega_{A/\mathbf{k}}$ is the corresponding module of Kähler differentials. We then discuss certain results related to Der and $\Omega$.

## Ring of Invariants (Chapter 2)

In this chapter we discuss the concept of ring of invariants of $\mathbf{k}[X_1, \ldots, X_n]$, $\mathbf{k}$ being an algebraically closed field, under the action of a finite subgroup

of $GL(n, \mathbf{k})$, and we discuss some results, that help us to compute the ring of invariants. We discuss some known results of Hilbert and Noether for invariant subrings of finite sub-groups of general linear groups in the non-modular case (i.e. when characteristic of $\mathbf{k}$ is zero or coprime with the order of the group). Then we also discuss Molien's formula and compute the Hilbert series of certain rings of invariants. We use these results to calculate the rings of invariants of dihedral groups.

Next, we discuss the concept of pseudo-reflections, we discuss a result by Shepherd and Todd for the rings of invariants [ST54] under the action of finite groups generated by pseudo-reflections.

## Module of Derivations of Certain Rings of Invariants (Chapter 3)

Our motivation to study the generators of the module of derivations of ring of invariants comes from a result of Gurjar and Wagh [GW08]. They have proved that the module of derivations of the ring of invariants obtained by the linear action of a finite cyclic subgroup of $GL(2, \mathbb{C})$ on $\mathbb{C}[X, Y]$, is minimally generated by 4 elements.

Here we use the following notations: Let $\mathbf{k}$ denote an algebraically closed field of characteristic 0. Let $G$ be a finite cyclic subgroup of $GL(m, \mathbf{k})$ of order $n$. Let $R = \mathbf{k}[\underline{X}]^G = \mathbf{k}[X_1, \ldots, X_m]^G$ be the ring of invariants obtained by the linear action of $G$ on $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_m]$.

We give and upper bound for $\mu(\mathrm{Der}\, R)$. We also give an algorithm to obtain

an explicit generating set of the module of derivations.

## Module of Derivation of Certain Quotient Rings (Chapter 4)

In this chapter we consider the ring $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, where $\mathbf{k}$ is an algebraically closed field of characteristic zero and $f \in \mathbf{k}[X_1,\ldots,X_n]$ be a quasi-homogeneous polynomial. We give an explicit computation for the generators of Der $R$, using computation of certain syzygy module.

## An Alternative Approach Using the Theory of Projective Modules (Chapter 5)

In this chapter we study the module of derivations of the smooth hypersurfaces, given by $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, where $f \in \langle \frac{\partial f}{\partial X_1},\ldots,\frac{\partial f}{\partial X_n}\rangle \subset \mathbf{k}[X_1,\ldots,X_n]$. For a smooth hypersurface $R$ of dimension $n-1$, using a result by A. A. Suslin [Sus77], it can be shown that Der $R$ is free of rank $n-1$.

We compute a generating set for Der $R$ using well known properties of projective modules.

## Computing a Minimal Generating Set for $\operatorname{Der} R$ for a Special Case (Chapter 6)

In this chapter we study the special case when $n = 3$ and $f$ is quasi-homogeneous, i.e. we consider the ring

$$R = \frac{\mathbf{k}[X, Y, Z]}{\langle f + 1 \rangle}.$$

It is known that $\operatorname{Der} R$ is free of rank 2 [Sus77]. We give an explicit construction of a minimal generating set for $\operatorname{Der} R$, consisting of two derivations.

# List of Publications

1. **Dey A.**, Wagh, V., *On the module of derivations of certain rings of invariants*, J. Ramanujan Math. Soc. 33, No.2 (2018), 149-158

2. **Dey A.**, Wagh, V., *On the module of derivations of certain hypersurfaces*. (Accepted for publication in Journal of Algebra and Its Applications)

# Contents

# Chapter 1

# Introduction

The goal of this thesis is to study the module of derivations of certain rings. The module of derivations and the module of differentials play an important role in commutative algebra and algebraic geometry. They are analogous to the tangent bundles and cotangent bundles of manifolds. Zariski-Lipman conjecture asserts that the freeness of module of derivation implies non-singularity of a variety. Thus the study of the module of derivations is closely related to the study of singularity.

In this thesis we give an algorithmic way to compute generating sets of the module of derivations for certain rings.

The thesis is divided into two parts. In the first part of the thesis we study the module of derivations of certain rings of invariants. The motivation for this work comes from a result by R. V. Gurjar and V. Wagh [GW08]. They have proved that, for a finite cyclic subgroup $G$ of $GL(2,\mathbb{C})$ the module of

derivations of the ring of invariants is minimally generated by 4 elements. We have generalized this result.

Let $\mathbf{k}$ be an algebraically closed field of characteristic zero and $f \in \mathbf{k}[\underline{X}]$ be such that $f \in \left\langle \{\frac{\partial f}{\partial X_i} : 1 \leq i \leq n\} \right\rangle$, let $R = \frac{\mathbf{k}[\underline{X}]}{\langle f+1 \rangle}$. In the second part of this thesis we study the module of derivations of this ring. We discuss two different approaches to study this module, one is computational and the other uses theory of projective modules.

## 1.1 Notations and Assumptions

Throughout this thesis we assume:

- All rings are commutative with unity. Usually rings are denoted by $A$, $B$ or $R$, $S$, $T$ etc.
- The base field of a polynomial ring (denoted by $\mathbf{k}$) is an algebraically closed field of characteristic zero. In some results the base field is the field of complex numbers $\mathbb{C}$.
- All modules considered in this thesis, are finitely generated.
- For a ring $R$ we denote the minimal number of generators of an $R$-module $M$ by $\mu(M)$. It is defined as the minimum of the cardinal numbers of all $R$-generating sets of $M$.
- For a natural number $n$, let $\mathbf{k}[X_1, \ldots, X_n]$ denote the ring of polynomials in $n$ variables $X_1, \ldots, X_n$, with coefficients in the base field $\mathbf{k}$. For

simplicity we sometime denote it by $\mathbf{k}[\underline{X}]$.

## 1.2 Derivations and Differentials

**Definition.** *Let $A$ be a ring and $M$ be an $A$-module. A **derivation** from $A$ to $M$ is a map $D : A \to M$ satisfying the following:*

1. $D(a + b) = Da + Db$,
2. $D(ab) = bDa + aDb$ *(Leibniz rule).*

The set of all derivations from $A$ to $M$ is written as $\mathrm{Der}(A, M)$.

**Properties of Module of Derivations:**

1. $\mathrm{Der}(A, M)$ becomes an $A$-module in a natural way, with $D+D'$ and $aD$ defined as $(D + D')a = Da + D'a$ and $(aD)b = a(Db)$ for all $a, b \in A$ and $D, D' \in \mathrm{Der}(A, M)$.

2. If $A$ is a $\mathbf{k}$-algebra via a ring homomorphism $f : \mathbf{k} \to A$, we say that $D : A \to M$ is a $\mathbf{k}$-derivation or a derivation over $\mathbf{k}$, if $D \circ f = 0$. $D \circ f = 0$ is equivalent to say that $D$ is $\mathbf{k}$-linear. It can be easily verified using the fact that $D(1) = 0$; which follows from Leibniz Rule.

   The set of all $\mathbf{k}$-derivations from $A$ to $M$ is written as $\mathrm{Der}_{\mathbf{k}}(A, M)$, which is an $A$-sub-module of $\mathrm{Der}(A, M)$.

   Viewing $A$ as $\mathbb{Z}$-algebra we have $\mathrm{Der}(A, M) = \mathrm{Der}_{\mathbb{Z}}(A, M)$.

3. If $D \in \mathrm{Der}(A, M)$ by repeated use of Leibniz Rule, one can see that $D(a^n) = na^{n-1}Da$

   Thus if $A$ is of characteristic $p$, $D(a^p) = 0$ for all $a \in A$

4. If $D \in \mathrm{Der}(A, A)$ then we have a Leibniz formula for powers of $D$,

$$D^n(ab) = \sum_{i=0}^{n} \binom{n}{i} D^i a D^{n-i} b$$

   If $A$ has characteristic $p$, then this reduces to $D^p(ab) = D^p a + D^p b$

**Example.** Let $S = \mathbf{k}[x, y]$. Observe that $\frac{\partial}{\partial x}$ is a derivation from $S$ to itself. Also this derivation is $\mathbf{k}[y]$-linear. So $\frac{\partial}{\partial x} \in \mathrm{Der}_{\mathbf{k}[y]}(\mathbf{k}[x, y], \mathbf{k}[x, y])$

**Definition.** *Let $\mathfrak{M}_A$ denotes the category of $A$-modules, we have a co-variant functor $M \mapsto \mathrm{Der}_{\mathbf{k}}(A, M)$ from $\mathfrak{M}_A$ to itself, which turns out to be a representable functor. In other words, there exists a unique $A$-module $\Omega_{A/\mathbf{k}}$ and unique derivation map $d_{A/\mathbf{k}} \in \mathrm{Der}_{\mathbf{k}}(A, \Omega_{A/\mathbf{k}})$ with the following universal property;*

*For any $A$-module $M$ and any $D \in \mathrm{Der}_{\mathbf{k}}(A, M)$ there exists a unique $A$-linear map $f : \Omega_{A/\mathbf{k}} \to M$ such that $D = f \circ d_{A/\mathbf{k}}$*

*This $A$-module $\Omega_{A/\mathbf{k}}$ is called, the module of **Kähler Differentials** of $A$ over $\mathbf{k}$.*

**Properties of Module of Kähler Differentials:**

1. From the definition it easy to see that $\mathrm{Der}_{\mathbf{k}}(A, M) \cong \mathrm{Hom}_A(\Omega_{A/\mathbf{k}}, M)$, where the isomorphism is an $A$-module isomorphism.

2. $\Omega_{A/\mathbf{k}}$ is generated as an $A$-module by $\{d_{A/\mathbf{k}}(a) : a \in A\}$

3. If $A$ is generated as an $\mathbf{k}$-algebra by the subset $U \subset A$ then $\Omega_{A/\mathbf{k}}$ is generated as an $A$-module by $\{d_{A/\mathbf{k}}a : a \in U\}$

Indeed for any $a \in A$ there exists $n \in \mathbb{N}$ so that $f \in \mathbf{k}[x_1, x_2, \ldots, x_n]$ and $a_1, a_2, \ldots, a_n \in U$ such that $a = f(a_1, a_2, \ldots, a_n)$. Again we can write $d_{A/\mathbf{k}}a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}|_{(a_1,a_2,\ldots,a_n)} d_{A/\mathbf{k}}a_i$, hence the result follows.

**Example.** If $A = \mathbf{k}[x_1, x_2, \ldots x_n]$ then by the property mentioned above we can say that, $\Omega_{A/\mathbf{k}} = Ad_{A/\mathbf{k}}x_1 + \ldots + Ad_{A/\mathbf{k}}x_n$

**Proposition 1** (First Fundamental Exact Sequence)**.** *A composite $k \xrightarrow{f} A \xrightarrow{g} B$ of ring homomorphisms leads to an exact sequence of $B$-module,*

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0$$

*where $\alpha(d_{A/k}a \otimes b) = bd_{B/k}g(a)$ and $\beta(d_{B/k}b) = d_{B/A}b$*

**Proposition 2** (Second Fundamental Exact Sequence)**.** *Consider the case $k \xrightarrow{f} A \xrightarrow{g} B$ when $g$ is onto, set $\ker(g) = m$ so $B \cong A/m$ and $\Omega_{B/A} = 0$, then we get an exact sequence*

$$m/m^2 \xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \longrightarrow 0$$

Throughout this thesis we shall be dealing with the module of $\mathbf{k}$-derivations from a finitely generated $\mathbf{k}$-algebra $R$ to itself, i.e. $\mathrm{Der}_{\mathbf{k}}(R, R)$. This module is generally denoted as $\mathrm{Der}_{\mathbf{k}} R$ or $\mathrm{Der}\, R$ whenever there is no ambiguity about the base field $\mathbf{k}$.

## 1.3 Derivations of Graded Rings

**Definition** (Quasi-homogeneous Algebra)**.** *Let $R = \mathbf{k}[X_1, \ldots, X_n]$ be a polynomial ring over a field $\mathbf{k}$. Let $\omega = (\omega_1, \ldots, \omega_n)$ be a vector of positive integers. The $\omega$-degree of a monomial $\underline{X}^{\underline{\alpha}} = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is defined to be the sum $\sum_{i=1}^{n} \alpha_i \omega_i$. Let $R_d$ denote the vector space generated by all monomials $\underline{X}^{\underline{\alpha}}$ such that $\omega\text{-}\deg(\underline{X}^{\underline{\alpha}}) = d$. Then $R = \bigoplus_{d \geq 0} R_d$ is a graded algebra. This graded algebra is called as weighted polynomial algebra with respected to the weight vector $\omega$. Further, the elements of $R_d$ are called as quasi-homogeneous polynomials of $\omega$-degree $d$.*

**Proposition 3.** *Let $R = \mathbf{k}[X_1, \ldots, X_n]$ be a graded $\mathbf{k}$-algebra. Let $f \in \mathbf{k}[X_1, \ldots, X_n]$ be a weighted homogeneous polynomial for the weight vector $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{N}^n$. Then*

$$\sum_{i=1}^{n} \omega_i X_i \frac{\partial f}{\partial X_i} = \omega\text{-}\deg(f) \cdot f.$$

**Remark 1** (Euler Derivation)**.** *Let $f \in \mathbf{k}[X_1, \ldots, X_n]$ be a homogeneous polynomial with respect to the standard grading (i.e. all $X_i$'s have weight 1), then*

$$\sum_{i=1}^{n} X_i \frac{\partial f}{\partial X_i} = \deg(f) \cdot f$$

*The derivation given by the tuple $(X_1, \ldots, X_n)$, i.e.*

$$\delta_0 = \sum_{i=1}^{n} X_i \frac{\partial}{\partial X_i}$$

*is the Euler derivation for the ring $\frac{\mathbf{k}[X_1, \ldots, X_n]}{\langle f \rangle}$.*

**Remark 2.** *Let $f \in \mathbf{k}[X_1, \ldots, X_n]$ be a quasi-homogeneous polynomial with weight vector $\omega = (a_1, \ldots, a_n)$, then the derivation $\delta_0 = \sum_{i=0}^{n} a_i X_i \frac{\partial}{\partial X_i}$ is the*

*Euler derivation for the ring* $\frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f\rangle}$ *with respect to the weight vector* $\omega$.

**Remark 3.** *Let* $f \in \mathbf{k}[X_1,\ldots,X_n]$ *be a quasi-homogeneous polynomial. Then*

$$f \in \left\langle \frac{\partial f}{\partial X_1},\ldots,\frac{\partial f}{\partial X_n} \right\rangle \subset \mathbf{k}[X_1,\ldots,X_n].$$

A converse of this statement was proved by Kyoji Saito.

**Theorem 4** (Saito [Sai71])**.** *Suppose* $f \in \mathbf{k}[X_1,\ldots,X_n]$ *is a non-constant polynomial and has an isolated singularity at* $(0,\ldots,0)$*. If* $f \in \left\langle \frac{\partial f}{\partial X_1},\ldots,\frac{\partial f}{\partial X_n} \right\rangle$ *then* $f$ *is quasi-homogeneous.*

In Chapter 4, we study the module of derivations of certain hypersurfaces, related to the polynomials which are $k[\underline{X}]$-linear combination of its partials, i.e. $f \in \left\langle \frac{\partial f}{\partial X_1},\ldots,\frac{\partial f}{\partial X_n} \right\rangle$.

# Part I

# Chapter 2

# Ring of Invariants

## 2.1 Introduction

In this chapter we discuss the concept of ring of invariants of $\mathbf{k}[X_1, \ldots, X_n]$, where $\mathbf{k}$ is an algebraically closed field, under the action of a subgroup of $GL(n, \mathbf{k})$, we also discuss some results, that help us to compute the ring of invariants. We give proofs of some fundamental results of Hilbert and Noether for invariant subrings of finite sub-groups of general linear groups in the non-modular case (i.e. when characteristic of $\mathbf{k}$ is zero or coprime with the order of the group). Then we also discuss Molien's formula and compute the Hilbert series of certain rings of invariants. We use these results to calculate the ring of invariants of dihedral groups. Details of these theories can be found in [NS02].

Then we discuss the concept of pseudo-reflections, we will state a result by

Shephard and Todd for the rings of invariants under the action of finite groups generated by pseudo-reflections.

## 2.2 Theorems of Hilbert and Noether

**Definition.** *Let* $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$ *be a polynomial ring over* $\mathbf{k}$ *in* $n$ *indeterminates, and* $G < GL(n, \mathbf{k})$. *The ring of invariants of* $G$ *is the ring:*

$$\mathbf{k}[\underline{X}]^G = \{f \in \mathbf{k}[\underline{X}] \ : \ M(f) = f \ \forall M \in G\}$$

*where any* $M \in G$ *acts on the indeterminates linearly by the rule:*

$$(X_1, \ldots, X_n)^t \mapsto M(X_1, \ldots, X_n)^t$$

*This action extends to all* $f \in \mathbf{k}[\underline{X}]$ *so that* $f \mapsto M(f)$ *is an automorphism of* $\mathbf{k}[\underline{X}]$.

**Proposition 5.** *For a finite subgroup* $G$ *of* $GL(n, \mathbf{k})$ *the ring* $\mathbf{k}[\underline{X}]^G$ *has transcendence degree* $n$ *over* $\mathbf{k}$.

*Proof.* We know that, $\mathrm{trdeg}_{\mathbf{k}}\, \mathbf{k}[\underline{X}] = n$. Hence, it suffices to show that $X_1, \ldots, X_n$ are algebraic over $\mathbf{k}[\underline{X}]^G$.

For $i = 1, \ldots .n$, we define:

$$P_i(t) := \prod_{g \in G} (t - g(X_i))$$

We note that, all the coefficients of $P_i(t)$ is in $\mathbf{k}[\underline{X}]^G$. As $P_i(X_i) = 0$, $X_i$ is integral over $\mathbf{k}[\underline{X}]^G$ for $i = 1, \ldots, n$. Hence $\mathbf{k}[\underline{X}]$ and $\mathbf{k}[\underline{X}]^G$ have same transcendence degree over $\mathbf{k}$. □

**Definition.** *Let $R$ be a ring, $G$ be a finite group of automorphisms of $R$ such that $|G|$ is invertible in $R$. Let $S = R^G$ be the ring of invariants of $G$ acting on $R$. Consider the map $\rho : R \to S$, such that $\rho(r) = \frac{1}{|G|}\sum_{g\in G} g(r)$. One can see*

*(i) $\rho$ is $S$-linear,*

*(ii) $\rho|_S = id_s$.*

*$\rho : R \to S$ is called the Reynolds operator of the pair $S \subset R$.*

**Proposition 6.** *Let $S$ be a subring of a ring $R$ and $\rho : R \to S$ be a Reynolds operator. Then,*

*(i) $IR \cap S = I$ for all ideals $I$ of $S$.*

*(ii) If $R$ is Noetherian then so is $S$.*

*Proof.* (i) Let $\sum_{i=1}^{n} a_i r_i = a \in S$ where $a_1, \ldots, a_n \in I$ and $r_1, \ldots, r_n \in R$. Then $a = \rho(a) = \sum_{i=1}^{n} \rho(r_i)a_i \in I$.

(ii) Let $I_1 \subset I_2 \subset \ldots$ be an ascending chain of ideals in $S$. Then $I_n R = I_{n+1}R$ for some $n$, as $R$ is Noetherian. Hence

$$I_n = I_n R \cap S = I_{n+1}R \cap S = I_{n+1} = \ldots.$$

Thus $S$ is Noetherian. □

**Theorem 7** (Hilbert's Finiteness Theorem)**.** *Let $G$ be a subgroup of $GL(n, \mathbf{k})$ acting linearly on $\mathbf{k}[\underline{X}] = R$, let $S = R^G$. Suppose that there is a Reynolds operator $\rho : R \to S$. Then $S$ is a finitely generated $\mathbf{k}$- algebra.*

*Proof.* Let $M$ be the maximal ideal of $S$ generated by homogeneous elements of positive degree. Since $R$ is Noetherian $MR$ has finitely many generators. Let these be homogeneous elements $f_1, \ldots, f_s \in M$.

We claim that, $S = \mathbf{k}[\underline{X}]^G = \mathbf{k}[f_1, \ldots, f_s]$. Let $f \in S$ be homogeneous of degree $d$. We apply induction on $d$: if $d = 0$, $f \in \mathbf{k}$. Suppose $d > 0$, then $f \in M$. Hence there exists $g_1, \ldots, g_s \in R$ such that $f = g_1 f_1 + \ldots + g_s f_s$. Applying $\rho$ we get, $f = \rho(g_1) f_1 + \ldots + \rho(g_s) f_s$. We may assume that $g_i$s are homogeneous. Then $\deg \rho(g_i) = \deg(g_i) = \deg f - \deg f_i < \deg f$. Since $\rho(g_i)$s have degree smaller than that of $f$, by induction hypothesis $\rho(g_1), \ldots, \rho(g_s) \in \mathbf{k}[f_1, \ldots, f_s]$. Hence $f \in \mathbf{k}[f_1, \ldots, f_s]$. □

**Corollary 8.** *Let $G$ be a finite subgroup of $GL(n, \mathbf{k})$ acting linearly on $\mathbf{k}[\underline{X}]$. Suppose that $\operatorname{char} \mathbf{k} \nmid |G|$. Then $\mathbf{k}[\underline{X}]^G$ is a finitely generated $\mathbf{k}$-algebra.*

**Theorem 9** (Noether's bound)**.** *Let $G \subset GL(n, \mathbf{k})$ be a finite subgroup of order $g$ such that $\operatorname{char} \mathbf{k} \nmid |G|$, then $\mathbf{k}[\underline{X}]^G$ is generated by atmost $\binom{n+g}{n}$ invariants of degree atmost $g$.*

For the proof one can see chapter 2 of [NS02].

**Theorem 10** (Molien's Theorem)**.** *Let $G$ be a finite subgroup of $GL(n, \mathbb{C})$ acting linearly on $R = \mathbb{C}[\underline{X}]$. Let $\mathbb{C}[\underline{X}]_i^G$ denote the vector space generated by all homogeneous invariants of degree $i$.*

*If we define,*

$$H\left(\mathbb{C}[\underline{X}]^G, \lambda\right) := \sum_{i=0}^{\infty} \dim \mathbb{C}[\underline{X}]_i^G \lambda^i$$

*then,*

$$H\left(\mathbb{C}[\underline{X}]^G, \lambda\right) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(I - \lambda M)}.$$

*Proof.* Let $g := |G|$. The Reynolds operator $\rho : R \to R^G$ is a $\mathbb{C}$-linear map. Hence it induces a linear map,

$$\rho|_{R_i} = \rho_i : R_i \to R_i$$

where $(\ )_i$ denotes elements of degree $i$. Clearly ${\rho_i}^2 = \rho_i$. Thus 0 and 1 are the only eigenvalue of $\rho_i$. Thus $\operatorname{rank}(\rho_i) = \operatorname{tr}(\rho_i) = \dim(R^G)_i$.

Therefore,

$$H\left(\mathbb{C}[\underline{X}]^G, \lambda\right) = \sum_{i=0}^{\infty} \dim\left(R^G\right)\lambda^i = \sum_{i=0}^{\infty} \operatorname{tr}(\rho_i)\lambda^i = \frac{1}{g}\sum_{M\in G}\left(\sum_{i=0}^{\infty} \operatorname{tr} M|_{R_i}\lambda^i\right)$$

We now prove that

$$\sum_{i=0}^{\infty} \operatorname{tr} M|_{R_i}\lambda^i = \frac{1}{\det(I - \lambda M)}.$$

Since $\mathbb{C}$ is algebraically closed and each $M$ has finite order, $M$ can be diagonalized. Let $v_1, \ldots, v_n$ be a basis of $R_1$ consisting of eigenvectors $M|_{R_1} : R_1 \to R_1$, and $\lambda_i$ be the eigenvalue corresponding to $v_i$.

The set $\left\{ v_1^{\alpha_1} \cdots v_n^{\alpha_n} | \sum_{j=1}^{n} \alpha_j = i \right\}$ is a basis of $R_i$ consisting of eigenvectors of $M|_{R_i} : R_i \to R_i$ and $M(v_1^{\alpha_1} \cdots v_n^{\alpha_n}) = \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n} v_1^{\alpha_1} \cdots v_n^{\alpha_n}$.

Thus

$$\operatorname{tr} M|_{R_i} = \sum_{\alpha_1+\ldots+\alpha_n=i} {\lambda_1}^{\alpha_1} \cdots {\lambda_n}^{\alpha_n}.$$

Hence

$$\begin{aligned}\sum_{i=0}^{\infty} \operatorname{tr} M|_{R_i}\lambda^i &= \prod_{j=1}^{n} \frac{1}{(1 - \lambda_j\lambda)} \\ &= \prod_{j=1}^{n} \frac{{\lambda_j}^{-1}}{({\lambda_j}^{-1} - \lambda)} = \frac{\det M^{-1}}{\det(M^{-1} - \lambda I)} = \frac{1}{\det(I - \lambda M)}.\end{aligned}$$

Therefore $H\left(R^G, \lambda\right) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(I - \lambda M)}$ □

## 2.3 Computing Ring of Invariants Under the Action of a Dihedral Group

The dihedral group $D_{2n}$ is the group of symmetries of a regular $n$-gon centered at the origin. As a subgroup of $GL(2, \mathbb{C})$, it is generated by,

$$\rho = \begin{bmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{bmatrix}, \; r = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Thus $D_{2n} = \{r^i \rho^j | i = 0, 1; j = 1, 2, \ldots, n-1\}$. The matrix $\rho$ is diagonalizable with eigenvalues $\lambda = e^{2\pi i/n}$ and $\lambda^{-1} = \overline{\lambda}$. Hence $\det(1 - \rho^i t) = (1 - \lambda^i t)(1 - \lambda^{-i} t)$. The reflections $r\rho^i$ are all diagonalizable with eigenvalues 1 and $-1$. Hence $\det(1 - r\rho^i t) = (1 - t)(1 + t) = (1 - t^2)$. By Molien's theorem we have,

$$H\left(\mathbb{C}[x, y]^{D_{2n}}, t\right) = \frac{1}{2n} \left\{ \frac{n}{1 - t^2} + \sum_{i=0}^{n-1} \frac{1}{(1 - \lambda^i t)(1 - \lambda^{-i} t)} \right\}$$

We now calculate the sum

$$\sum_{i=0}^{n-1} \frac{1}{(1 - \lambda^i t)(1 - \lambda^{-i} t)}$$

We consider the cyclic group $C_n$ generated by $\rho$. The matrix of $\rho$ can be diagonalized and its diagonal form is $\mathrm{diag}\,(\lambda, \lambda^{-1})$. We have

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda^{-1} y \end{bmatrix}.$$

Hence monomials $x^a y^b$ are mapped to monomials $(\lambda x)^a(\lambda^{-1}y)^b$. Applying the Reynold's operator on $x^a y^b$ we get:

$$\frac{1}{n}\sum_{i=0}^{n-1}\lambda^{i(a-b)}x^a y^b.$$

Therefore the monomial $x^a y^b$ is an invariant if and only if $(\lambda^i x)^a(\lambda^{-i}y)^b = \lambda^{i(a-b)}x^a y^b = x^a y^b$, i.e. if and only if $n|a-b$. Write $a = na_1 + r_1$, $b = nb_1 + s_1$ where $0 \leq r, s \leq n-1$. As $a - b = n(a_1 - b_1) + (r_1 - s_1)$, we must have $r_1 = s_1$. Therefore invariant monomials are $x^{na}y^{nb}(xy)^c$ where $0 \leq c \leq n-1$ and $a, b \in \mathbb{N}$. Thus

$$\mathbb{C}[x,y]^{C_n} = \bigoplus_{i=0}^{n-1}\mathbb{C}[x^n, y^n](xy)^i.$$

Hence

$$H\left(\mathbb{C}[x,y]^{C_n}, t\right) = \sum_{i=0}^{n-1}\frac{t^{2i}}{(1-t^n)^2}.$$

Therefore

$$\frac{1}{n}\sum_{i=0}^{n-1}\frac{1}{(1-\lambda^i t)(1-\lambda^{-i}t)} = \frac{1+t^2+t^4+\ldots+t^{2n-2}}{(1-t^n)^2}.$$

We substitute the above expression into the Molien series of $D_{2n}$,

$$\begin{aligned} H\left(\mathbb{C}[x,y]^{D_{2n}}, t\right) &= \frac{1}{2n}\left\{\frac{n(1+t^2+\ldots+t^{2n-2})}{(1-t^n)^2} + \frac{n}{1-t^2}\right\} \\ &= \frac{1}{(1-t^n)(1-t^2)} \end{aligned}$$

Hence the Molien series is the Hilbert series of a polynomial algebra with generators of degree 2 and degree $n$. The matrices in $D_{2n}$ are orthogonal hence they preserve $f = x^2 + y^2$. Now we look for degree $n$ invariant. The vertices $\left(\cos\frac{2\pi p}{n}, \sin\frac{2\pi p}{n}\right)$ are permuted by the action of the matrices in $D_{2n}$.

Let $\theta = \frac{2\pi}{n}$, then for $p = 0, 1, \ldots, n-1$ we have

$$\begin{aligned}\rho(x\cos p\theta + y\sin p\theta) &= (x\cos\theta - y\sin\theta)\cos p\theta + (x\sin\theta + y\cos\theta)\sin p\theta \\ &= x\cos(p-1)\theta + y\sin(p-1)\theta \\ r(x\cos p\theta + y\sin p\theta) &= x\cos(-p\theta) + y\sin(-p\theta)\end{aligned}$$

Hence $h = \prod_{p=0}^{n-1}(x\cos p\theta + y\sin p\theta)$ is an invariant of degree $n$. Moreover the invariants $f$ and $h$ are algebraically independent by the fact that

$$\det\begin{bmatrix} f_x & f_y \\ h_x & h_y \end{bmatrix} = \begin{vmatrix} 2x & 2y \\ h_x & h_y \end{vmatrix} = 2(xh_y - yh_x) \neq 0$$

In order to conclude that $\mathbb{C}[x,y]^{D_{2n}} = \mathbb{C}[f,h]$, we use the fact that if $S \subset S'$ are graded sub-algebras of $\mathbb{C}[x,y]$ with the same Hilbert function then $S = S'$. Thus we can compute ring of invariants of $D_{2n}$ using Molien's theorem.

## Theorem of Shephard and Todd

**Definition** (Pseudo-reflection [NS02]). *A linear automorphism $s : V \longrightarrow V$ of a finite dimensional vector space $V$ over a field $\mathbf{k}$ is called a pseudo-reflection if*

*i. it has finite order.*

*ii. it leaves a co-dimension 1 subspace pointwise fixed.*

The subspace of co-dimension 1, pointwise fixed under $s$ is called hyperplane of $s$.

The subspace $\mathrm{Im}(I - s)$ of $V$ is therefore of dimension 1. It is called the direction of $s$.

**Definition** (Pseudo-reflection Group [NS02]). *If a finite group $G$ has a representation*

$$\rho : G \hookrightarrow GL(n, \mathbf{k})$$

*such that $\rho(G)$ is generated by pseudo-reflections, then $G$ is called a pseudo-reflection group.*

H. S. M. Coxeter in [Cox34] based on his classification of real reflection groups i.e., Coxeter groups has observed that the invariants of such a real Coxeter representations are always a polynomial algebra.

Later G. C. Shephard and J. A. Todd [ST54] observed the same phenomenon for $\mathbf{k} = \mathbb{C}$ based on a list of all examples of finite complex pseudo-reflection groups.

**Theorem 11** (Shephard-Todd [ST54]). *Let $G < GL(m, \mathbb{C})$ be a finite subgroup acting linearly on the polynomial ring $T = \mathbb{C}[X_1, \ldots, X_m]$ and let $R = T^G$ be the ring of invariants. Then $G$ is generated by pseudo-reflections if and only if $R = T^G$ is a polynomial ring.*

C. Chevalley in [Che55] provided a proof of H. S. M. Coxeter's observation. J.-P. Serre in [Ser68] noticed that C. Chevalley's proof was adequate to handle all non-modular cases.

Chevalley's proof of Shephard-Todd's theorem is discussed below.

Throughout this discussion, let $V$ be a finite dimensional vector space over the field $\mathbf{k}$, we denote by $\mathbf{k}[V]$ the graded algebra of polynomial functions on $V$, which is defined to be the symmetric algebra on $V^*$, the dual of $V$. In other words the homogeneous component of $\mathbf{k}[V]$ of degree $m$ is $S^m(V^*)$, the $m$-th symmetric power of $V^*$. $S^m(V^*)$ is the quotient of $\bigotimes_m V^*$ by the subspace spanned by all elements of the form $w_1 \otimes \cdots \otimes w_m - w_{\sigma(1)} \otimes \cdots \otimes w_{\sigma(m)}$, as $\sigma$ ranges over all permutations of $\{1, \ldots, m\}$.

If $z_1, \ldots, z_n \in V^*$ is a basis, we also denote $\mathbf{k}[V]$ by $\mathbf{k}[z_1, \ldots, z_n]$. The elements of $\mathbf{k}[z_1, \ldots, z_n]$ are just homogeneous polynomials in the linear forms $z_1, \ldots, z_n$ with coefficients in $\mathbf{k}$. A monomial is an element which may be written as a product of the basis elements for $V^*$, so after rearranging terms it has the form ${z_1}^{k_1} \cdots {z_n}^{k_n}$.

Let $G$ be a finite group and $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbf{k})$ a representation of $G$ over $\mathbf{k}$. Then, via $\rho$, $G$ acts on the left of the vector space $V = \mathbf{k}^n$. This action induces an action on the algebra of the polynomial functions $\mathbf{k}[V]$ on $V$. This induced action arises from the left action of $G$ on $V^*$ defined by

$$(g \cdot z)v = z(\rho(g)^{-1}v)$$

for $g \in G$, $z \in V^*$ and $v \in V$; and its extension to $S^m(V^*)$ for $m \in \mathbb{N}_0$. These fit together to give a left $G$-action on $\mathbf{k}[V]$ by algebra automorphisms. By definition the ring of invariants is the fixed sub-algebra

$$\mathbf{k}[V]^G := \{f \in \mathbf{k}[V] \ : \ g \cdot f = f \ \forall \ g \in G\}.$$

**Theorem 12** (Corollary 3.1.5, [NS02]). *Let $G \hookrightarrow GL(n, \mathbf{k})$ be a faithful representation of a finite group $G$. If the characteristic of $\mathbf{k}$ does not divide*

*the order of $G$ and $\mathbf{k}[V]^G = \mathbf{k}[f_1, \ldots, f_n]$, such that deg $(f_i) = d_i$ for $i = 1, \ldots, n$; then $|G| = d_1 \cdots d_n$ and $|s(G)| = \sum_{i=1}^{n}(d_i - 1)$. Where $s(G)$ denotes the set of all pseudo-reflections in $G$.*

For a pseudo-reflection group $G$ we will discuss the fact that $\mathbf{k}[V]^G$ is a polynomial algebra using some well known results as follows:

**Theorem 13** ([Ser68])**.** *Let $A$ be a finitely generated commutative graded connected algebra over a field $\mathbf{k}$. If $\mathbf{k}$ has a finite global dimension $d$, then $A \cong \mathbf{k}[z_1, \ldots, z_d]$, where $z_1, \ldots, z_d$ are indeterminates.*

**Corollary 14.** *Suppose $A$ is a graded sub-algebra of the graded polynomial algebra $\mathbf{k}[h_1, \ldots, h_n]$. If the algebra $\mathbf{k}[h_1, \ldots, h_n]$ is free as an $A$-module, then $A = \mathbf{k}[f_1, \ldots, f_k]$ with $f_1, \ldots, f_k$ a regular sequence in $\mathbf{k}[h_1, \ldots, h_n]$ such that $k \leq n$.*

Before proving the theorem of Shephard and Todd we will state four lemmas. Proofs can be found in [NS02].

**Lemma 15.** *Let $\rho : G \hookrightarrow GL(n, \mathbf{k})$ be a representation of a finite group $G$ over the field $\mathbf{k}$. Then the following map is a zero map:*

$$\mathrm{Tor}_1^{\mathbf{k}[V]^G}\left(\mathbf{k}, \mathrm{Tr}^G\right) : \mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V]) \longrightarrow \mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V]),$$

*where $\mathrm{Tr}^G : \mathbf{k}[V] \to \mathbf{k}[V]^G$ is the transfer homomorphism given by $\mathrm{Tr}^G(f) = \sum_{g \in G} g \cdot f$ for $f \in \mathbf{k}[V]$.*

**Lemma 16.** *Let $\rho : G \hookrightarrow GL(n, \mathbf{k})$ be a representation of a finite group $G$ over the field $\mathbf{k}$. If $|G|$ is invertible in $\mathbf{k}$, then*

$$\mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V])^G = 0$$

**Lemma 17.** *Let $\rho : G \hookrightarrow GL(n, \mathbf{k})$ be a representation of a finite group $G$ over the field $\mathbf{k}$. Suppose $\rho(G)$ is generated by pseudo-reflections. Then $\mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V])^G = 0$ if and only if $\mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V]) = 0$*

**Lemma 18.** *Let $A$ be a commutative graded connected algebra over a field $\mathbf{k}$ and $M$ a positively graded $A$-module. Then the following are equivalent:*

*i. $M$ is a free $A$-module.*

*ii. $M$ is a projective $A$-module.*

*iii. $M$ is a flat $A$-module.*

*iv. $\mathrm{Tor}_A^1(\mathbf{k}, M) = 0$.*

**Theorem 19** (G. C. Shephard- J. A. Todd, C. Chevalley)**.** *Let $V$ be a finite-dimensional vector space over the field $\mathbf{k}$ and $\rho : G \hookrightarrow GL(V)$ a representation of a finite group $G$. Assume that $|G|$ is relatively prime to the characteristic of $\mathbf{k}$. Then the following are equivalent:*

*i. $G$ is generated by pseudo-reflections.*

*ii. $\mathbf{k}[V]^G$ is a polynomial algebra.*

*Proof.* Suppose that $\rho$ is a pseudo-reflection representation. Since $|G| \in \mathbf{k}^*$, it follows from Lemma 16, that $\mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V])^G = 0$. Since $\rho(G)$ is generated by pseudo-reflections, applying Lemma 17, we obtain $\mathrm{Tor}_1^{\mathbf{k}[V]^G}(\mathbf{k}, \mathbf{k}[V]) = 0$. Therefore $\mathbf{k}[V]$ is a flat $\mathbf{k}[V]^G$ module, and hence $\mathbf{k}[V]^G$ is a polynomial algebra by Lemma 18 and Corollary 14.

Conversely, suppose $\mathbf{k}[V]^G$ is a polynomial algebra, with polynomial generators $f_1, \ldots, f_n$ of degrees $d_1 \leq \ldots \leq d_n$. Let $H \leq G$ be the subgroup of $G$ generated by $s(G)$, the set of pseudo-reflections in $G$. By previous argument $\mathbf{k}[V]^H$ is a polynomial algebra. Choose generators $h_1, \ldots, h_n$ for $\mathbf{k}[V]^H$ and let their degree be $e_1 \leq \ldots \leq e_n$. Of course, $f_i \in \mathbf{k}[h_1, \ldots, h_n]$ for $i = 1, \ldots, n$. By Theorem 12 we have,

$$|G| = d_1 \cdots d_n |s(G)| = \sum_{i=1}^{n} (d_i - 1)$$

$$|H| = e_1 \cdots e_n |s(H)| = \sum_{i=1}^{n} (e_i - 1)$$

We claim that $d_i \geq e_i$ for $i = 1, \ldots, n$. For $i = 1$ this is clear. Assume that $e_i \leq d_i$ for $i = 1, \ldots, m$ and consider $f_{m+1}$. If $d_{m+1} < e_{m+1}$, then $f_{m+1}$ must be a polynomial in $h_1, \ldots, h_m$, and hence $f_1, \ldots, f_{m+1} \in \mathbf{k}[h_1, \ldots, h_m]$ would be algebraically independent, which is not possible. Therefore $d_i \geq e_i$ for $i = 1, \ldots, n$ as claimed.

Since $G$ and $H$ have the same pseudo-reflections, we obtain from theorem 12 that

$$\sum_{i=1}^{n} (d_i - 1) = \sum_{i=1}^{n} (e_i - 1)$$

and it follows that $d_i = e_i$ for $i = 1, \ldots, n$. But then $|G| = d_1 \cdots d_n = e_1 \cdots e_n = |H|$. So $H = G$, and hence $G$ is generated by pseudo-reflections.

□

# Chapter 3

# Module of Derivations of Rings of Invariants

Our motivation to study the generators of the module of derivations of ring of invariants comes from a result of Gurjar and Wagh [GW08]. They have proved that the module of derivations of the ring of invariants obtained by the linear action of a finite cyclic subgroup of $GL(2, \mathbb{C})$ on $\mathbb{C}[X, Y]$, is minimally generated by 4 elements.

Throughout this chapter we use the following notations: Let $\mathbf{k}$ denote an algebraically closed field of characteristic 0. Let $G$ be a finite cyclic subgroup of $GL(m, \mathbf{k})$ of order $n$. Let $R = \mathbf{k}[\underline{X}]^G = \mathbf{k}[X_1, \ldots, X_m]^G$ be the ring of invariants obtained by linear action of $G$ on $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_m]$. $\operatorname{Der} R$ denotes the module of $\mathbf{k}$-derivations of $R$.

**Remark 4.** *In view of Theorem 11, it suffices to consider only those finite*

*subgroups of $GL(m, \mathbf{k})$, which do not contain (non-trivial) pseudo-reflections.*

Justification: Note that for any $g \in G$ and a pseudo-reflection $\rho \in G$, the element $g\rho g^{-1}$ is also a pseudo-reflection. Thus, the subgroup generated by pseudo-reflections, say $N$, is a normal subgroup in $G$. Thus, following Theorem 11, the ring of invariants $\mathbf{k}[\underline{X}]^N$ is a polynomial ring, say $\mathbf{k}[Y_1, \ldots, Y_r]$; and $\mathbf{k}[\underline{X}]^G \cong (\mathbf{k}[\underline{X}]^N)^{G/N} \cong \mathbf{k}[Y_1, \ldots, Y_r]^{G/N}$

Thus we will assume that, $G$ does not contain a pseudo-reflection.

**Remark 5.** *As $G$ is a finite cyclic group of order $n$, it can be easily seen that there exists a diagonal element in $GL(m, \mathbf{k})$ such that,*

$$G \cong \left\langle \begin{bmatrix} \omega^{\alpha_1} & 0 & \ldots & 0 \\ 0 & \omega^{\alpha_2} & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \omega^{\alpha_m} \end{bmatrix} \right\rangle,$$

*where $\omega$ is a primitive $n$-th root of unity and $\alpha_i$'s are non-negative integers less than $n$, with $\gcd(\alpha_1, \ldots, \alpha_m, n) = 1$. We denote this generator by $\sigma$.*

Justification: Note that for some $j$, if $d_j = \gcd(\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_m, n) > 1$, then $\sigma^{\frac{n}{d_j}}$ is a (non-trivial) pseudo-reflection.

Further note that if $\gcd(\alpha_1, \ldots, \alpha_m, n) = d > 1$ then $\sigma^{\frac{n}{d}} = I$, which contradicts the assumption that the $o(\sigma) = o(G) = n$. Therefore $\alpha_i$'s are such that $\gcd(\alpha_1, \ldots, \alpha_m, n) = 1$ and $d_j = 1$ for each $j$, $1 \leq j \leq m$.

By this observation and Lemma 22, it suffices to consider only the finite cyclic subgroups of $GL(m, \mathbf{k})$, generated by diagonal elements.

Let $G$ be as above and $R = \mathbf{k}[\underline{X}]^G$ be the ring of invariants. We give a bound on the minimal number of generators of Der $R$, in terms of order of the group $G$ and the number of variables in the polynomial ring $\mathbf{k}[\underline{X}]$.

In section 3.1, we find a $k$-algebra generating set for the ring of invariants $R = \mathbf{k}[\underline{X}]^G$. We also recall some well-known results.

Section 3.2 contains the main theorem, giving a bound on $\mu(\text{Der } R)$. This result generalizes the result in [GW08] to higher dimensions, covering the cases of all finite cyclic subgroups of $GL(m, \mathbf{k})$, which do not contain a pseudo-reflection.

In section 3.3, we give an algorithm to compute an explicit generating set of Der $R$.

## 3.1 Some Well-Known Results

In this section we find a generating set (as $\mathbf{k}$-algebra) for the ring of invariants $R = \mathbf{k}[\underline{X}]^G$. Then we further explore the relation between $\mathbf{k}[\underline{X}]^G$ and the group $G$, by showing the isomorphism of the rings of invariants of the subgroups conjugates to $G$.

**Lemma 20.** *For a polynomial $f$, invariant under $G$-action, all the monomials appearing in $f$ are invariant under $G$-action.*

*Proof.* Writing

$$f = \sum_{\substack{\underline{\gamma}\in(\mathbb{N}\cup\{0\})^m \\ \underline{\gamma}\neq 0}} c_{\underline{\gamma}}\underline{X^{\gamma}}$$

and using $\sigma(f) = f$, we get,

$$\sigma(f) = \sigma\left(\sum_{\substack{\underline{\gamma}\in(\mathbb{N}\cup\{0\})^m \\ \underline{\gamma}\neq 0}} c_{\underline{\gamma}}\underline{X^{\gamma}}\right) = \sum_{\substack{\underline{\gamma}\in(\mathbb{N}\cup\{0\})^m \\ \underline{\gamma}\neq 0}} c_{\underline{\gamma}}\underline{X^{\gamma}} = f.$$

Note that $\sigma$ is a $\mathbf{k}$-linear operator over $\mathbf{k}[\underline{X}]$ and for a monomial $m(\underline{X}) = a_{\underline{\gamma}}\underline{X^{\gamma}} \in \mathbf{k}[\underline{X}]$ (where $a_{\underline{\gamma}} \in \mathbf{k}$) the action of $\sigma$ is as follows:

$$\sigma\left(m(\underline{X})\right) = \omega^{\underline{\alpha\gamma}} a_{\underline{\gamma}}\underline{X^{\gamma}} = \omega^i m(\underline{X}) \text{ for } 0 \leq i \leq (n-1)$$

Therefore each monomial appearing in $f$, is an eigenvector corresponding to the eigenvalue $\omega^i$ of $\sigma$ for some $i$ such that $0 \leq i \leq n-1$.

Since all monomials are $\mathbf{k}$-linearly independent, $f$ lies in the eigenspace corresponding to the eigenvalue 1. Thus it can be easily seen that $R$ is the eigenspace corresponding to the eigenvalue 1. □

This gives us a generating set (over $\mathbf{k}$) for the ring of invariants.

**Corollary 21.** *The ring of invariants, $R = \mathbf{k}[\underline{X}]^G$ is generated (as $\mathbf{k}$-algebra) by the following monomials:*

$$\left\{\underline{X^{\beta}} = \prod_{i=1}^{m} {X_i}^{\beta_i} \ : \ \sum_{i=1}^{m} \alpha_i\beta_i \equiv 0 \pmod{n}\right\}$$

**Lemma 22.** *Let $\eta \in GL(m, \mathbf{k})$ be an element of finite order and $\sigma = \tau^{-1}\eta\tau$ be the diagonalization of $\eta$. If $G = \langle\sigma\rangle$ and $G' = \langle\eta\rangle$. Then $\mathbf{k}[\underline{X}]^G \cong \mathbf{k}[\underline{Y}]^{G'}$ as $\mathbf{k}$-algebra, where $\underline{Y} = \tau(\underline{X})$.*

*Proof.* For $p(\underline{X}) \in \mathbf{k}[\underline{X}]^G$, we have $\sigma(p(\underline{X})) = p(\underline{X})$. Now, $\tau$ induces a natural automorphism of $\mathbf{k}[\underline{X}]$, such that $\tau(p(\underline{X})) = p(\underline{Y})$ for all $p(\underline{X}) \in \mathbf{k}[\underline{X}]$.

Now,

$$\begin{aligned}\eta(p(\underline{Y})) &= (\tau\sigma\tau^{-1})(p(\underline{Y})) \\ &= (\tau\sigma\tau^{-1})\tau(p(\underline{X})) \\ &= \tau(p(\underline{X})) \\ &= p(\underline{Y})\end{aligned}$$

Thus, $p(\underline{Y})$ is invariant under $\eta$, i.e. $p(\underline{Y}) \in \mathbf{k}[\underline{Y}]^{G'}$.

Conversely, for any $q(\underline{Y}) \in \mathbf{k}[\underline{Y}]^{G'}$, we have

$$\begin{aligned} & \eta(q(\underline{Y})) && = && q(\underline{Y}) \\ \implies \quad & (\tau\sigma\tau^{-1})(q(\underline{Y})) && = && q(\underline{Y}), \\ \implies \quad & \sigma(\tau^{-1}q(\underline{Y})) && = && \tau^{-1}q(\underline{Y}) \\ \implies \quad & \sigma(q(\underline{X})) && = && q(\underline{X}).\end{aligned}$$

Thus, $q(\underline{X}) \in \mathbf{k}[\underline{X}]^G$. This completes the proof. □

The next lemma will be used in the proof of the main theorem.

**Lemma 23** ([DW18])**.** *For $m, n \in \mathbb{N}$ and $a_1, \ldots, a_m, b \in \mathbb{Z}$, the congruence,*

$$a_1x_1 + \ldots + a_mx_m \equiv b \pmod{n}$$

*with $\gcd(a_1, \ldots, a_m, n) = d$ and $d \mid b$, has exactly $d \cdot n^{(m-1)}$ solutions in ${\mathbb{Z}_n}^m$.*

*Proof.* We will show this using induction on $m$.

For $m = 1$, note that solving the congruence $ax \equiv b \pmod{n}$ is equivalent to solve the diophantine equation $ax - ny = b$ for $x, y \in \mathbb{Z}$. This equation has solutions if and only if $d = \gcd(a, n)$ divides $b$.

Let $(x_0, y_0)$ be a solution, then all other solutions of this equation will be of the form

$$x = x_0 + \frac{tn}{d} \qquad y = y_0 + \frac{ta}{d}, \qquad \text{for } t \in \mathbb{Z}.$$

Note that, varying $t \in \mathbb{Z}$, we will get all incongruent solutions modulo $n$. For any $\alpha \in \mathbb{Z}$ there exists $\beta \in \mathbb{Z}$ such that,

$$\begin{aligned} & \alpha \equiv \beta \pmod{d}. \\ \text{i.e.} \quad & d \mid (\alpha - \beta). \\ \text{Therefore,} \quad & n \mid \frac{n}{d}(\alpha - \beta). \\ \text{i.e.} \quad & \frac{\alpha n}{d} \equiv \frac{\beta n}{d} \pmod{n}. \\ \text{Hence,} \quad & x_0 + \frac{\alpha n}{d} \equiv x_0 + \frac{\beta n}{d} \pmod{n}. \end{aligned}$$

Further, note that for any $\gamma, \delta$ with $\gamma \not\equiv \delta \pmod{d}$, we have,

$$x_0 + \gamma\frac{n}{d} \not\equiv x_0 + \delta\frac{n}{d} \pmod{n}.$$

Thus the congruence $ax \equiv b \pmod{n}$ has exactly $d$ incongruent solutions modulo $n$, namely

$$x = x_0 + \frac{tn}{d} \qquad y = y_0 + \frac{ta}{d}, \qquad 0 \le t \le d - 1.$$

Now assume that the result is true for $m = k - 1$ for some $k > 1$, i.e. the congruence

$$a_1x_1 + \ldots + a_{k-1}x_{k-1} \equiv b \pmod{n}$$

has exactly $d_{k-1} \cdot n^{k-2}$ incongruent solutions modulo $n$, where

$$d_{k-1} = \gcd(a_1, \ldots, a_{k-1}, n)$$

.

Consider the congruence,

$$a_1x_1 + \ldots + a_kx_k \equiv b \pmod{n} \tag{a}$$

such that $d_k = \gcd(a_1, \ldots, a_k, n) \mid b$. Now, congruence (a) can be re-written as,

$$a_1x_1 + \ldots + a_{k-1}x_{k-1} \equiv b - a_kx_k \pmod{n} \tag{b}$$

For a fixed $x_k$, congruence (b) will have a solution if and only if

$$d_{k-1} \mid (b - a_kx_k), \text{where } d_{k-1} = \gcd(a_1, \ldots, a_{k-1}, n)$$

if and only if

$$a_kx_k \equiv b \pmod{d_{k-1}}. \tag{c}$$

Since $d_k = \gcd(a_k, d_{k-1})$ and $d_k \mid b$, congruence (c) will have a solution.

Rewriting congruence (c) as

$$\frac{a_kn}{d_{k-1}}x_k \equiv \frac{bn}{d_{k-1}} \pmod{n},$$

we have exactly $\gcd\left(\frac{a_k n}{d_{k-1}}, n\right)$ number of incongruent solutions modulo $n$.

Thus, by the induction hypothesis, congruence (a) will have exactly

$$d_{k-1}n^{k-2} \cdot \gcd\left(\frac{a_k n}{d_{k-1}}, n\right) = d_k n^{k-1}$$

number of solutions which are incongruent modulo $n$. □

The next lemma is used in the proof of Theorem 25.

**Lemma 24.** *Let $A = \mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_m]$, $G$ a finite cyclic subgroup of $GL(m, \mathbf{k})$, and $R = A^G$. Assume that $G$ is generated by a diagonal matrix $\sigma$ and that $G$ does not contain any non-trivial pseudo-reflections. Then the following hold:*

*i. Each $\mathbf{k}$-derivation $\delta : R \to R$ extends uniquely to a $\mathbf{k}$-derivation $D : A \to A$.*

*ii. Consider the map $\varepsilon : \mathrm{Der}_{\mathbf{k}} R \to \mathrm{Der}_{\mathbf{k}} A$, $\delta \mapsto D$ where $D$ is the unique extension of $\delta$. Then $\varepsilon$ is an injective homomorphism of $R$-modules and*

$$Im\ \varepsilon = \{D \in \mathrm{Der}_{\mathbf{k}} A | D \circ \sigma = \sigma \circ D\}.$$

*The $\sigma$ that occurs in $D \circ \sigma = \sigma \circ D$ is the automorphism of $A$ induced by the matrix $\sigma$.*

*Proof.* Let $n = o(G)$ and let $\omega$ be some primitive $n$th root of unity. Then

$G = \langle \sigma \rangle$ where:

$$\sigma = \begin{bmatrix} \omega^{\alpha_1} & 0 & \dots & 0 \\ 0 & \omega^{\alpha_2} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \omega^{\alpha_m} \end{bmatrix}$$

for some $\alpha_1, \dots, \alpha_m \in \{0, 1, \dots, n-1\}$. The fact that $\sigma$ has order $n$ implies that

$$\gcd(\alpha_1, \dots, \alpha_m, n) = 1 \tag{3.1}$$

and the fact that $G$ does not contain non-trivial pseudo-reflections implies that

$$\text{for each } i \in \{1, \dots, m\}, \text{ we have } \gcd(\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_m, n) = 1 \tag{3.2}$$

To prove *(i)*, consider an arbitrary $\delta \in \mathrm{Der}_{\mathbf{k}} R$. Then $\delta$ has a unique extension to a derivation $\delta' : K \to K$, where $K$ is the field of fractions of $R$. Since $\mathrm{char}\,\mathbf{k} = 0$, $\delta'$ has a unique extension to a derivation $\delta'' : L \to L$ where $L = \mathbf{k}(\underline{X})$ is the field of fractions of $A$.

There exist $f_1, \dots, f_m \in A$ and $g \in A \setminus 0$ such that $\delta''(X_i) = \frac{f_i}{g}$ for all $i$. Moreover, we may choose $f_1, \dots, f_m$ and $g$ so that

$$\gcd(f_1, \dots, f_m, g) = 1 \text{ in } A. \tag{3.3}$$

To prove *(i)*, it suffices to show that $g$ is a unit of $A$ (if $g$ is a unit then $\delta''(A) \subseteq A$, so $\delta''|_A : A \to A$ extends $\delta$). We first observe that:

$$\text{for each } i \in \{1, \dots, m\} \text{ we have } g | {X_i}^{n-1} f_i \text{ in } A. \tag{3.4}$$

Indeed, we have ${X_i}^n \in R$, so $R \ni \delta({X_i}^n) = \delta''({X_i}^n) = n{X_i}^{n-1}\frac{f_i}{g}$, so ${X_i}^{n-1} f_i \in gR \subseteq gA$, proving equation 3.4.

Let $p$ be an irreducible element of $A$ such that $p|g$ in $A$. By equation 3.3, we may choose $j$ such that $p \nmid f_j$. We have $g|{X_j}^{n-1}f_j$ in $A$ by equation 3.4, so $p|{X_j}^{n-1}f_j$ in $A$. As $p \nmid f_j$ we obtain $p = X_j$ (upto multiplication by a unit). This argument shows that $g$ is a monomial. So it suffices to show that $X_i \nmid g$ for all $i$.

By contradiction suppose that some $X_i|g$. Without loss of generality, we may assume that $X_1|g$. It follows from equation 3.4 that $X_1|f_i$ for all $i > 1$: so equation 3.3 implies that $X_1 \nmid f_1$. Since equation 3.2 implies that $\gcd(\alpha_2, \ldots, \alpha_m, n) = 1$ it follows from the Lemma 23 that there exist $\beta_2, \ldots, \beta_m \in \mathbb{N}$ such that $\sum_{i=2}^{m} \alpha_i\beta_i \equiv -\alpha_1 \pmod{n}$. So we see that there exist $\beta_1, \ldots, \beta_m \in \mathbb{N}$ such that $\beta_1 = 1$, $\beta_i > 0$ for all $i$, and $\sum_{i=1}^{m} \alpha_i\beta_i \equiv 0 \pmod{n}$. Then the monomial $M = \prod_{i=1}^{m} {X_i}^{\beta_i}$ belongs to $R$ and consequently $R \ni \delta(M) = \delta''(M) = \sum_{i=1}^{m} \frac{\partial}{\partial X_i}(M)\frac{f_i}{g}$.

Then

$$\sum_{i=1}^{m} \frac{\partial}{\partial X_i}(M) f_i \; gR \subseteq gA$$

Since $X_1|g$ and $X_1|f_i$ for each $i > 1$, we get $X_1|\frac{\partial}{\partial X_1}(M)f_1 = {X_2}^{\beta_2} \cdots {X_m}^{\beta_m} f_1$, so $X_1|f_1$, a contradiction. This shows that no $X_i$ divides $g$, so $g$ is a unit and hence *(i)* is proved.

Proof of *(ii)*: Clearly $\varepsilon : \mathrm{Der}_{\mathbf{k}} R \to \mathrm{Der}_{\mathbf{k}} A$ is a homomorphism of $R$-modules. Let us now assume that $\delta \in \ker \varepsilon$ $D = \varepsilon(\delta) = 0$, then $D(r) = 0$ for all $r \in R$. Thus $\delta = D|_R = 0$, which shows that $\varepsilon$ is injective.

We note that the derivation $\sigma\delta - \delta\sigma$ is 0 in $R$. Since the extension $\delta \mapsto D$ is unique. Thus for all $D \in \mathrm{Im}\ \varepsilon$, we must have $\sigma D = D\sigma$.

Conversely, for $D \in \mathrm{Der}_{\mathbf{k}} A$, satisfying $\sigma D = D\sigma$ we see that:

$$\sigma D(r) = D\sigma(r) = D(r) \text{ for all } r \in R.$$

Thus $D(R) \subseteq R$. Hence $\delta = D|_R \in \mathrm{Der}_{\mathbf{k}} R$ is the pre-image of $D$. □

## 3.2 Main Theorem

**Theorem 25.** *Let $G \leq GL(m, \mathbf{k})$ be a finite, cyclic subgroup of order $n$ and $R = \mathbf{k}[X]^G$. Then*

$$\mu(\mathrm{Der}\, R) \quad \leq \quad m(1 + n^{m-2}).$$

*Proof.* In view of Remark 4, Remark 5 and Lemma 22 it suffices to prove the result when

1. $\sigma$ is diagonal.

2. $G$ does not contain a non-trivial pseudo-reflection.

We observe that the action of $\sigma$ on $\frac{\partial}{\partial X_i}$ is as follows.

$$\sigma \left( \frac{\partial}{\partial X_i} \right) \sigma^{-1} = \frac{1}{\omega^{\alpha_i}} \cdot \frac{\partial}{\partial X_i}.$$

Let $\delta \in \mathrm{Der}\, R$ be a derivation. By Lemma 24 $\delta$ induces a derivation of the polynomial ring $\mathbf{k}[X_1, \ldots, X_m]$, which is invariant under the action of $G$. We denote this derivation by the same notation $\delta$.

Writing,

$$\delta = \sum_{i=1}^{m} f_i(\underline{X}) \frac{\partial}{\partial X_i},$$

it is easy to see that,

$$\begin{aligned} f_1(\omega^{\alpha_1} X_1, \ldots, \omega^{\alpha_m} X_m) &= \omega^{\alpha_1} f_1(\underline{X}) \\ f_2(\omega^{\alpha_1} X_1, \ldots, \omega^{\alpha_m} X_m) &= \omega^{\alpha_2} f_2(\underline{X}) \\ &\vdots \\ f_m(\omega^{\alpha_1} X_1, \ldots, \omega^{\alpha_m} X_m) &= \omega^{\alpha_m} f_m(\underline{X}) \end{aligned} \tag{3.5}$$

Further, each monomial appearing in the above $f_i$'s, also satisfies the corresponding equation. Suppose, $\underline{X}^{\underline{\beta}} = {X_1}^{\beta_1} \cdots {X_m}^{\beta_m} \in \mathbf{k}[\underline{X}]$ is a monomial appearing in $f_j$.

Then

$$\omega^{\underline{\alpha}\underline{\beta}} \underline{X}^{\underline{\beta}} = \omega^{\alpha_j} \underline{X}^{\underline{\beta}}, \tag{3.6}$$

where $\underline{\alpha}\underline{\beta} = \sum_{i=1}^{m} \alpha_i \beta_i$. Thus we can assume that $f_i$'s are monomials.

Now we solve the equation (3.6) for $\underline{\beta}$, using the following congruence:

$$\sum_{i=1}^{m} \alpha_i \beta_i \equiv \alpha_j \pmod{n} \text{ for } 1 \leq j \leq m$$

Clearly, $\gcd(\alpha_1, \ldots, \alpha_m, n) | \alpha_j$, guaranteeing existence of a solution; and we see that the following is a solution (for $\underline{\beta} = (\beta_1, \ldots, \beta_m)$),

$$(0, \ldots, 1, \ldots, 0). \qquad\qquad j^{th} \text{ position} \tag{3.7}$$

Thus, $X_j \dfrac{\partial}{\partial X_j}$ is in $\operatorname{Der} R$.

For a fixed $j$, let $\underline{\gamma} = (\gamma_1, \ldots, \gamma_m)$ be any other solution for $\underline{\beta}$. Note that it suffices to consider $0 \leq \gamma_i \leq n-1$ for each $1 \leq i \leq m$. For if $\gamma_i > n$, then writing $\gamma_i = nq + r$ with $0 \leq r < n$, we have,

$$X_i{}^{\gamma_i} = (X_i{}^n)^q \cdot X_i{}^r, \qquad \text{and} \qquad X_i{}^n \in R.$$

Consider the following two cases:

**Case 1:** $\gamma_j > 0$:

Note that $(0, \ldots, 1, \ldots, 0)$ and $\underline{\gamma}$ are both solutions for $\underline{\beta}$. Thus, subtracting the two congruences, we get

$$\alpha_1\gamma_1 + \ldots + \alpha_j(\gamma_j - 1) + \ldots + \alpha_m\gamma_m \equiv 0 \pmod{n}.$$

Therefore the monomial,

$$X_1{}^{\gamma_1} \cdots X_j{}^{\gamma_j - 1} \cdots X_m{}^{\gamma_m} \in R.$$

And hence,

$$(X_1{}^{\gamma_1} \cdots X_j{}^{\gamma_j} \cdots X_m{}^{\gamma_m}) \frac{\partial}{\partial X_j} = \left(X_1{}^{\gamma_1} \cdots X_j{}^{\gamma_j - 1} \cdots X_m{}^{\gamma_m}\right) X_j \frac{\partial}{\partial X_j}.$$

Thus, the monomial obtained from the solution $\underline{\gamma} = (\gamma_1, \ldots, \gamma_m)$ is an $R$-multiple of $X_j \dfrac{\partial}{\partial X_j}$.

**Case 2:** $\gamma_j = 0$:

Then by Lemma (23),

$$\alpha_1\gamma_1 + \ldots + \alpha_{j-1}\gamma_{j-1} + \alpha_{j+1}\gamma_{j+1} + \ldots + \alpha_m\gamma_m \equiv \alpha_j \pmod{n}$$

has exactly $n^{m-2}$ number of in-congruent solutions modulo $n$.

(recall: $d_j = \gcd(\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_m, n) = 1$ ).

Thus, for each $j$, we have $1 + n^{m-2}$ number of solutions for $\underline{\beta}$; and these solutions generate all other solutions for the corresponding $\underline{\beta}$. Hence, the solution set for the system of equations (3.6) is generated by $m(1 + n^{m-2})$ number of solutions. Note that any other solution will be an $R$-linear combination of these solutions.

Therefore

$$\mu(\text{Der } R) \leq m(1 + n^{m-2}).$$

□

## 3.3 Generating Set for the Module of Derivations

The following algorithm gives an explicit generating set for Der $R$.

**Input:**

- $m, n \in \mathbb{N}$
- $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$, with $1 \leq \alpha_i < n$ and $\gcd(\alpha_1, \ldots, \alpha_m, n) = 1$ and $d_j = 1$ for $1 \leq j \leq m$
- $\omega \in \mathbb{C}$, a primitive $n^{\text{th}}$ root of unity.

**Notations:** $G \cong \left\langle \begin{bmatrix} \omega^{\alpha_1} & 0 & \dots & 0 \\ 0 & \omega^{\alpha_2} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \omega^{\alpha_m} \end{bmatrix} \right\rangle < GL(m, \mathbf{k})$, with $o(G) = n$.

$R = \mathbf{k}[X_1, \dots, X_m]^G$.

**Output:** A generating set of Der $R$.

Initialize the set $M \leftarrow 0$.

**for** $j = 1$ to $m$. **do**

Solve the following congruence for $\underline{\gamma} = (\gamma_1, \dots, \gamma_m)$:

$$\alpha_1\gamma_1 + \dots + \alpha_m\gamma_m \equiv \alpha_j \pmod{n},$$

Compute $S_j = \{\underline{\gamma} \ : \ \underline{\alpha}\underline{\gamma} \equiv \alpha_j \pmod{n}\}$

Set $M := M \bigcup \left\{ \underline{X}^{\underline{\gamma}} \dfrac{\partial}{\partial X_j} : \underline{\gamma} \in S_j \right\}$

**end for**

**return** $M$

From the proof of Theorem 25, it follows that the module generated by the set $M$, obtained at the end of the above algorithm, is equal to Der $R$. A generating set for Der $R$ smaller than $M$ can be obtained by computing the reduced Gröbner basis for $M$ (with respect to some monomial ordering).

## 3.4 Example

The following version of Nakayama's Lemma for graded rings is important in calculating a (homogeneous) minimal generating set.

**Lemma 26.** *If $M$ is a finitely-generated positively graded module over a graded ring $R$ and the images of elements $m_1, \ldots, m_n$ of $M$ in $M/R_+M$ generate $M/R_+M$ as an $R/R_+$-module, then $m_1, \ldots, m_n$ also generate $M$ as an $R$-module.*

**Example 1:**

In the following example, we compute an explicit generating set for Der $R$:

Let $\omega$ be a 20-th primitive root of unity. Consider

$$G = \left\langle \begin{bmatrix} \omega^3 & 0 & 0 \\ 0 & \omega^7 & 0 \\ 0 & 0 & \omega^{13} \end{bmatrix} \right\rangle,$$

By Theorem 25 we can see that

$$\mu(\operatorname{Der} R) \leq 3 + 3 \cdot 20^{3-2} = 63.$$

Using computer algebra systems SAGE [Sag16] and SINGULAR [DGPS18], we find a generating set for Der $R$:

$$\begin{aligned} \mathcal{B} = \Bigg\{ & X_3\frac{\partial}{\partial X_3}, \quad X_2\frac{\partial}{\partial X_2}, X_1\frac{\partial}{\partial X_1}, \\ & {X_1}^2X_2\frac{\partial}{\partial X_3}, \; X_1{X_3}^8\frac{\partial}{\partial X_2}, {X_1}^3{X_3}^6\frac{\partial}{\partial X_2}, \\ & {X_1}^5{X_3}^4\frac{\partial}{\partial X_2}, {X_1}^7{X_3}^2\frac{\partial}{\partial X_2}, {X_2}^9\frac{\partial}{\partial X_1}, \\ & {X_1}^9\frac{\partial}{\partial X_2}, \quad {X_3}^{11}\frac{\partial}{\partial X_1}, X_1{X_2}^{10}\frac{\partial}{\partial X_3}, \\ & {X_1}^{11}\frac{\partial}{\partial X_3}, \quad {X_3}^{19}\frac{\partial}{\partial X_2}, {X_2}^{19}\frac{\partial}{\partial X_3} \Bigg\} \end{aligned}$$

It can be easily seen that no proper subset of $\mathcal{B}$ can generate $\operatorname{Der} R$. Thus $\mathcal{B}$ is a minimal generating set for $\operatorname{Der} R$ (by Nakayama's lemma for graded rings).

Hence $\mu(\operatorname{Der} R) = 15 \leq 63$.

**Example 2:**

Let $\omega$ be a 30-th primitive root of unity, we consider

$$G = \left\langle \begin{bmatrix} \omega^2 & 0 & 0 \\ 0 & \omega^3 & 0 \\ 0 & 0 & \omega^5 \end{bmatrix} \right\rangle,$$

(Note that for each $i$, $\gcd(\alpha_i, n) > 1$. However $\sigma$ satisfies the conditions as mentioned earlier.)

By Theorem 25 we can see that

$$\mu(\operatorname{Der} R) \leq 3 + 3 \cdot 30^{3-2} = 93.$$

Using computer algebra systems SAGE [Sag16] and SINGULAR [DGPS18], we find a generating set for

$$\mathcal{B} = \left\{ \begin{array}{lll} X_1\frac{\partial}{\partial X_1}, & X_2\frac{\partial}{\partial X_2}, & X_3\frac{\partial}{\partial X_3}, \\ X_1X_2\frac{\partial}{\partial X_3}, & {X_2}^4{X_3}^4\frac{\partial}{\partial X_1}, & {X_2}^9X_3\frac{\partial}{\partial X_1}, \\ {X_1}^4{X_3}^5\frac{\partial}{\partial X_2}, & {X_1}^9{X_3}^3\frac{\partial}{\partial X_2}, & {X_1}^{14}X_3\frac{\partial}{\partial X_2} \end{array} \right\}$$

It can be easily seen that no proper subset of $\mathcal{B}$ can generate $\operatorname{Der} R$. Thus $\mathcal{B}$ is a minimal generating set for $\operatorname{Der} R$ (by Nakayama's lemma for graded rings).

Hence $\mu(\operatorname{Der} R) = 9 \leq 93$.

## 3.5 Remarks

In case of $m = 2$, the equality is attained (and is independent of $n$). In [GW08], it is proved that, for a finite cyclic subgroup of $GL(2, \mathbf{k})$, $\mu(\operatorname{Der} R) = 4$. In this case the bound is independent of $n$, the order of the group.

In view of Theorem 25, the following natural question can be asked:

**Question.** *Let $G < GL(m, \mathbf{k})$ be a finite subgroup acting on $\mathbf{k}[X_1, \ldots, X_m]$. Let $R$ be the ring of invariants. Then does there exist a (universal) bound for the minimum number of generators of* $\operatorname{Der} R$*?*

# Part II

# Chapter 4

# Module of Derivations of Certain Quotient Rings

## 4.1 Introduction

Let $\mathbf{k}$ be an algebraically closed field of characteristic zero. Let $f$ be a polynomial in $\mathbf{k}[X_1, \ldots, X_n]$. For the ring $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, the module of Kähler differentials $(\Omega_{R/k})$ has the following free presentation:

$$R \xrightarrow{\phi} R^n \to \Omega_{R/k} \to 0$$

where the map $\phi$ is represented by the Jacobian matrix $J = [\frac{\partial f}{\partial X_1} \ldots \frac{\partial f}{\partial X_n}]$. Now by applying $\mathrm{Hom}(-, R)$ functor to the above sequence, we get the following left-exact sequence:

$$0 \longrightarrow \mathrm{Hom}(\Omega_{R/k}, R) \longrightarrow \mathrm{Hom}(R^n, R) \xrightarrow{\psi} \mathrm{Hom}(R, R),$$

where $\psi$ is the map represented by the transpose of $J$. Thus we get $\ker\psi \cong \mathrm{Hom}(\Omega_{R/k}, R) \cong \mathrm{Der}\, R$. It is easy to see that $\ker\psi = \mathrm{syz}_R\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$. Thus to find $\mathrm{Der}\, R$ is equivalent to find $\mathrm{syz}_R\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$.

## 4.2 Computation of Syzygy Module

As mentioned in the introduction, computing $\mathrm{Der}\, R$ is equivalent to compute certain syzygy module. In this section, we discuss a method for computing syzygy module. We recall the notations from [KR00, §2.3].

**Definition** (Syzygy / syzygy module)**.** *Let $R$ be a ring, $M$ an $R$-module, and $\mathscr{G} = (g_1, \ldots, g_s)$ a tuple of elements of $M$.*

*a. A syzygy of $\mathscr{G}$ is a tuple $(f_1, \ldots, f_s) \in R^s$ such that $f_1g_1 + \ldots + f_sg_s = 0$.*

*b. The set of all syzygies of $\mathscr{G}$ forms an $R$-module which we call the (first) syzygy module of $\mathscr{G}$ and we denote it by $\mathrm{syz}_R(\mathscr{G})$ or by $\mathrm{syz}_R(g_1, \ldots, g_s)$.*

**Definition** ($\sigma$-degree, $\sigma$-leading form)**.** *Let $m$ be a non-zero element of a $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$-graded module, and let $m = \sum_{\mu \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle} m_\mu$ be the decomposition of $m$ into its homogeneous components. The term*

$$\max_\sigma \{\mu \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle | m_\mu \neq 0\}$$

*is called $\sigma$-degree of $m$, and the homogeneous component of $m$ of this degree is called $\sigma$-leading form of $m$.*

The following result provides a method to compute $\sigma$-degree and $\sigma$-leading form:

**Lemma 27** ([KR00, Proposition 2.3.5]). *Let $f_1, \ldots, f_s \in P$, and $\mathbf{m} = \sum_{j=1}^{s} f_j \epsilon_j \in P^s$ be a non-zero element in the free module.*

*Let*

$$\deg_{\sigma,\mathscr{G}}(\mathbf{m}) := \max_{\sigma} \{LT_\sigma(f_i g_i) | 1 \leq j \leq s,\ f_j g_j \neq 0\}$$

*and*

$$LF_{\sigma,\mathscr{G}}(\mathbf{m}) := \sum_{j=1}^{s} \overline{f_j} \epsilon_j$$

*where:*

$$\overline{f_j} = \begin{cases} 0 & \text{if } f_j = 0 \text{ or } LT_\sigma(f_j g_j) <_\sigma \deg_{\sigma,\mathscr{G}}(\mathbf{m}) \\ c_j t_j & \text{if } LT_\sigma(f_j g_j) = \deg_{\sigma,\mathscr{G}}(\mathbf{m}) \text{ such that} \\ & LM_\sigma(f_j g_j) = c_j t_j LM_\sigma(g_j) \end{cases}$$

**Definition** (Lifting of an element). *An element $m \in P^s$ is called a lifting of an element $\overline{m} \in P^s$ if we have $LF_{\sigma,\mathscr{G}}(m) = \overline{m}$.*

The following proposition provides a tool to compute the $\sigma$-degree and the $\sigma$-leading form of an element of a module. In section 5.3, we use this result to compute a generating set of Der $R$.

**Theorem 28** ([KR00, Proposition 2.3.7]). *For a monomial ordering $\sigma$ we have $LM_\sigma(g_j) = c_j t_j e_{\gamma_j}$, where $c_j \in \mathbf{k}$, $t_j \in \mathbb{T}^n$ and $\gamma_j \in 1, \ldots, r$. For all $1 \leq i, j \leq s$ we define $t_{ij} = \frac{\operatorname{lcm}(t_i, t_j)}{t_i}$. Then, we have:*

**a.** *For $1 \leq i < j \leq s$ and $\gamma_i = \gamma_j$, the element*

$$\Sigma_{ij} = \frac{1}{c_i} t_{ij} \epsilon_i - \frac{1}{c_j} t_{j,i} \epsilon_j \in P^s$$

*is a syzygy of $LM_\sigma(\mathscr{G})$ and is homogeneous of $\sigma$-degree $\deg_{\sigma,\mathscr{G}}(\Sigma_{ij}) = \operatorname{lcm}(t_i, t_j) e_{\gamma_i}$*

**b.** $\text{syz}(LM_\sigma(\mathscr{G})) = \langle \Sigma ij : 1 \leq i < j \leq s,\ \gamma_i = \gamma_j \rangle$.

The following theorem provides a method to compute a generating set for the syzygy module using lifts of a generating set of syzygies of leading monomials.

**Theorem 29** ([KR00, Proposition 2.3.11])**.** *Let* $\{\overline{m_1}, \ldots, \overline{m_t}\}$ *be a homogeneous system of generators for the module* $\text{syz}(LM(\mathscr{G}))$ *and let* $m_1, \ldots, m_t \in \text{syz}(\mathscr{G})$ *be elements such that* $LF(m_i) = \overline{m_i}$ *for* $1 \leq i \leq t$*, then* $\{m_1, \ldots, m_t\}$ *is a system of generators of* $\text{syz}(\mathscr{G})$.

## 4.3 Computation of Der $R$

**Theorem 30.** *For* $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1 \rangle}$*, where* $f$ *is a homogeneous polynomial of degree* $m$*;* $\mu(\text{Der}\, R) \leq \binom{n}{2}$*, and* $\text{Der}\, R$ *is generated by the regular generators.*

*Proof.* From the discussion above, we know that $\text{Der}\, R \cong \text{syz}_R\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$. In order to compute the syzygy module $\text{syz}_R\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$, we will first compute $\text{syz}_{\mathbf{k}[\underline{X}]}\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n},\ f+1\right)$; then we will take the projection of the first $n$ components of the generators of this Syzygy module onto $R^n$.

Now, let $\mathscr{G} = \left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n},\ f+1\right)$. With respect to local lexicographic ordering $\sigma$, we get the leading terms of $G$ as follows:

$$\text{LT}_\sigma(\mathscr{G}) = \left(\text{LT}_\sigma\left(\frac{\partial f}{\partial X_1}\right), \ldots, \text{LT}_\sigma\left(\frac{\partial f}{\partial X_n}\right), 1\right).$$

According to the Theorem 28 of the previous section a homogeneous(with respect to $\deg_{\sigma,\mathscr{G}}$) generating set for $\text{syz}_{\mathbf{k}[\underline{X}]}(\text{LT}_\sigma(\mathscr{G}))$ is given by the following

$\Sigma_{i,j}$'s:

$$\Sigma_{1,2} = \left(\mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_2}\right), -\mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_1}\right), 0, \ldots, 0\right)$$
$$\vdots$$
$$\Sigma_{n-1,n} = \left(0, \ldots, \mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_n}\right), -\mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_{n-1}}\right), 0\right)$$

and,

$$\Sigma_{1,n+1} = \left(1, 0, \ldots, 0, -\mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_1}\right)\right)$$
$$\vdots$$
$$\Sigma_{n,n+1} = \left(0, 0, \ldots, 1, -\mathrm{LT}_\sigma\left(\frac{\partial f}{\partial X_n}\right)\right)$$

Lifting these generators to $\mathrm{syz}_{\mathbf{k}[\underline{X}]}(\mathscr{G})$, we get $\widetilde{\Sigma_{i,j}}$'s:

$$\widetilde{\Sigma_{1,2}} = \left(\frac{\partial f}{\partial X_2}, -\frac{\partial f}{\partial X_1}, 0, \ldots, 0\right)$$
$$\vdots$$
$$\widetilde{\Sigma_{n-1,n}} = \left(0, \ldots, 0, \frac{\partial f}{\partial X_n}, -\frac{\partial f}{\partial X_{n-1}}, 0\right)$$

and,

$$\widetilde{\Sigma_{1,n+1}} = \left(f + 1, 0, \ldots, 0, -\frac{\partial f}{\partial X_1}\right)$$
$$\vdots$$
$$\widetilde{\Sigma_{n,n+1}} = \left(0, 0, \ldots, f + 1, -\frac{\partial f}{\partial X_n}\right)$$

By the theorem 29 we can say that $\{\widetilde{\Sigma_{i,j}} : 1 \leq i < j \leq n+1\}$ forms a generating set for $\mathrm{syz}_{\mathbf{k}[\underline{X}]}(\mathscr{G})$.

The projection of first $n$-components of the first $\binom{n}{2}$ generators $\widetilde{\Sigma_{i,j}}$, $1 \leq i <$

$j \leq n$, onto $R^n$, are following $\widehat{\Sigma_{i,j}}$'s:

$$\widehat{\Sigma_{1,2}} = \left(\frac{\partial f}{\partial X_2}, -\frac{\partial f}{\partial X_1}, 0, \ldots, 0\right)$$
$$\vdots$$
$$\widehat{\Sigma_{n-1,n}} = \left(0, \ldots, 0, \frac{\partial f}{\partial X_n}, -\frac{\partial f}{\partial X_{n-1}}\right)$$

The projection of the first $n$ components onto $R^n$, of the rest of the $\widehat{\Sigma_{i,j}}$ gives $\mathbf{0}$.

Thus a generating set for $\mathrm{syz}_R(\mathscr{G})$ is given by

$$\{\widehat{\Sigma_{i,j}} \in R^n : 1 \leq i < j \leq n\}$$

i.e. Der $R$ is generated by the regular generators:

$$\left\{\left(\frac{\partial f}{\partial X_2}, -\frac{\partial f}{\partial X_1}, 0, \ldots, 0\right), \ldots, \left(0, \ldots, 0, \frac{\partial f}{\partial X_n}, -\frac{\partial f}{\partial X_{n-1}}\right)\right\}$$

Hence, $\mu(\mathrm{Der}\, R) \leq \binom{n}{2}$ □

# Chapter 5

# An Alternative Approach Using the Theory of Projective Modules

## 5.1 Introduction

In this chapter we study the module of derivations of the smooth hypersurface, given by $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, where $f \in \langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\rangle \subset \mathbf{k}[X_1, \ldots, X_n]$. As a special case, when $f+1$ is irreducible, the result coincides with the special case of Bavula's result [Bav10, Theorem 1.1] applied to a principal prime ideal. The proof given here uses computations of a syzygy module using a result of unimodular rows, to get an explicit generating set for $\operatorname{Der} R$.

For a smooth hypersurface $R$ of dimension $n-1$, using a result by A. A.

Suslin [Sus77], it can be shown that Der $R$ is free of rank $n-1$.

## 5.2 Some Useful Results

In this section, we recall some well-known results which are used in the proof of the main result.

**Definition.** *Let $A$ be a commutative ring with unity. For $r \geq 1$ we say $(a_1, \ldots, a_r) \in A^r$ is unimodular of length $r$ if there exists $b_i \in A$ for $1 \leq i \leq r$ such that,*

$$\sum_{i=1}^{r} b_i a_i = 1$$

*We denote the set of all unimodular vectors of length $r$ over the ring $A$ by* $\mathrm{Um_r(A)}$.

**Lemma 31.** *Let $v = (v_1, \ldots, v_r) \in \mathrm{Um_r(A)}$, and $f : A^r \to A$ be an $A$-linear map given by $e_i \longmapsto v_i$, where $\{e_i\}_{i=1}^r$ is the canonical basis for $A^r$. Then* $\ker(f)$ *is generated by the set,*

$$\{v_j e_i - v_i e_j | 1 \leq i < j \leq r\}$$

*Proof.* Since, $v \in \mathrm{Um_r(A)}$, there exists $w_1, w_2, \ldots, w_r \in A$ such that,

$$\sum_{i=1}^{r} v_i w_i = 1$$

We define, the following two $A$-linear maps,

$$g : A \longrightarrow A^r \text{ by } g(1) = \sum_{i=1}^{r} w_i e_i$$

and,

$$\theta : A^r \longrightarrow \ker(f) \text{ by } \theta(x) = x - gf(x)$$

We note that $\theta$ is identity on $\ker(f)$, hence $\theta$ is surjective. Thus, $\ker(f)$ is generated by $\{\theta(e_i)\}_{i=1}^r$. Now,

$$\begin{aligned}\theta(e_i) &= e_i - gf(e_i)\\ &= e_i - g(v_i)\\ &= \sum_{j=1}^{r} v_j w_j e_i - \sum_{j=1}^{r} v_i w_j e_j\\ &= \sum_{j=1}^{r} w_j(v_j e_i - v_i e_j)\end{aligned}$$

Now, since $(v_j e_i - v_i e_j) \in \ker(f)$ for $1 \leq i < j \leq r$, our assertion follows. □

**Lemma 32.** *For* $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, *such that* $f \in \langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\rangle$, $\operatorname{Der} R$ *is stably free* $R$ *module of rank* $n-1$.

*Proof.* As discussed in section 4.1, we have the following exact sequence:

$$0 \longrightarrow \operatorname{Der} R \longrightarrow R^n \xrightarrow{J} R \tag{5.1}$$

Again, we see that:

$$f\ (= -1 \text{ in } R)\ \in \langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\rangle$$

hence,

$$J = \left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) \in \operatorname{Um}_n(R)$$

there exists $g_1, \ldots, g_n \in R$ such that $\sum_{i=1}^n \frac{\partial f}{\partial X_i} g_i = 1$. Hence, the sequence (5.1) is right exact:

$$0 \longrightarrow \operatorname{Der} R \longrightarrow R^n \xrightarrow{J} R \longrightarrow 0$$

Also, we have the map $\xi : R \to R^n$ given by $1 \longmapsto (g_1, \ldots, g_n)$. Hence the above sequence splits and Der $R \oplus R \cong R^n$. Thus Der $R$ is stably free of rank $n-1$. □

**Remark 6.** *It is known that, if $A$ is an affine algebra of dimension $d$ over an algebraically closed field, then each stably free module whose rank is greater than or equal to $d$ is free [Sus77]. Thus, in view of the above lemma we see that* Der $R$ *is free of rank $n-1$.*

The next lemma is used in the proof of Theorem 37 .

**Lemma 33.** *Given a homogeneous polynomial $f$ of degree $m$ in $\mathbf{k}[X, Y, Z]$, there exists an automorphism of $\mathbf{k}[X, Y, Z]$, say $\tau$, such that at least one of the three pure powers ($X^m$, $Y^m$ or $Z^m$) does not appear in $\tau(f)$.*

*Proof.* Assuming $f$ has all the three pure powers, $f$ can be written as:

$$f(X, Y, Z) = c_0X^m + c_1X^{m-1}Y + \ldots + c_{m-1}XY^{m-1} + c_mY^m + Zh(X, Y, Z),$$

where $h$ is a homogeneous polynomial of degree $m-1$.

For $\alpha \in \mathbf{k}$, consider the transformation $\tau$ given by

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \mapsto \begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}.$$

Thus,

$$\begin{aligned} \tau(f) =& f(X + \alpha Y, Y, Z) \\ =& c_0(X + \alpha Y)^m + c_1(X + \alpha Y)^{m-1}Y + \ldots \\ &+ c_{m-1}(X + \alpha Y)Y^{m-1} + c_mY^m + Zg(X + \alpha Y, Y, Z). \end{aligned}$$

Note that the coefficient of $Y^m$ in the above equation is:

$$c_0\alpha^m + c_1\alpha^{m-1} + \ldots + c_{m-1}\alpha + c_m$$

Since, $\mathbf{k}$ is algebraically closed, choose $\alpha$ to be a root of

$$c_0t^m + c_1t^{m-1} + \ldots + c_{m-1}t + c_m \ \in \mathbf{k}[t].$$

Thus the coefficient of $Y^m$ in $\tau(f)$ is 0. □

## 5.3 Computation of Der $R$

**Definition** (Regular derivations)**.** *Let* $S = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle g\rangle}$. *For* $1 \leq i < j \leq n$, *derivations* $\Delta_{ij}$ *of the form* $\Delta_{ij} = \dfrac{\partial g}{\partial X_j}\dfrac{\partial}{\partial X_i} - \dfrac{\partial g}{\partial X_i}\dfrac{\partial}{\partial X_j}$ *are called regular derivations of* $S$.

**Theorem 34.** *For* $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, *such that* $f \in \left\langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \right\rangle$, Der $R$ *is generated by the regular derivations.*

*Proof.* From the discussion above, we know that

$$\text{Der}\, R \cong \text{syz}_R\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right).$$

We note that,

$$\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) \in \text{Um}_n(R)$$

Hence, using Lemma 31, we can say that, Der $R$ is generated by,

$$\left\{\frac{\partial f}{\partial X_j}\frac{\partial}{\partial X_i} - \frac{\partial f}{\partial X_i}\frac{\partial}{\partial X_j} | 1 \leq i < j \leq n\right\}$$

□

**Corollary 35.** *If $R = \mathbf{k}[X_1, \ldots, X_n]/\langle f + 1\rangle$ and $f$ is quasi-homogeneous of degree $m \geq 1$, then* $\operatorname{Der} R$ *is generated by the regular derivations.*

*Proof.* If $f$ is quasi-homogeneous, then there exists $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$, such that

$$\alpha_1 X_1 \frac{\partial f}{\partial X_1} + \ldots + \alpha_n X_n \frac{\partial f}{\partial X_n} = mf.$$

Thus $f \in \langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \rangle$. □

**Corollary 36.** *For $R = \frac{\mathbf{k}[X_1,\ldots,X_n]}{\langle f+1\rangle}$, such that $f \in \sqrt{\langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \rangle}$,* $\operatorname{Der} R$ *is generated by the regular derivations.*

*Proof.* We note that, for $m \in \mathbb{N}$, $f^m$ is a unit in $R$. Thus

$$\left( \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \right) \in \operatorname{Um}_n(R)$$

Hence our assertion follows. □

# Chapter 6

# Computing a Minimal Generating Set for Der $R$ for a Special Case

## 6.1 Introduction

In this chapter we study the special case when $n = 3$ and $f$ is quasi-homogeneous, i.e. $R = \frac{\mathbf{k}[X,Y,Z]}{\langle f+1\rangle}$. In this case, we give an explicit construction of a minimal generating set for Der $R$, consisting of two derivations.

As discussed above, we see that for a quasi-homogeneous polynomial $f \in \mathbf{k}[X, Y, Z]$, Der $\left(\frac{\mathbf{k}[X,Y,Z]}{\langle f+1\rangle}\right)$ is generated by the regular derivations $\Delta_1, \Delta_2, \Delta_3$, where $\Delta_1 = (0, -\frac{\partial f}{\partial Z}, \frac{\partial f}{\partial Y})$, $\Delta_2 = (-\frac{\partial f}{\partial Z}, 0, \frac{\partial f}{\partial X})$ and $\Delta_3 = (-\frac{\partial f}{\partial Y}, \frac{\partial f}{\partial X}, 0)$. As $R$ is a smooth hypersurface, Der $R$ is a free $\mathbf{k}[\underline{X}]$-module of rank 2.

In order to prove the following result for quasi-homogeneous case it suffices to prove the result when $f \in \mathbf{k}[X, Y, Z]$ is homogeneous of degree $m$. Also, in view of Lemma 33, we will assume (without loss of generality) that, $Z^m$ does not appear in $f$.

The computation of a minimal generating set of $\operatorname{Der} R$ is described in the next section.

## 6.2 Main Result

**Theorem 37.** *For $R = \frac{\mathbf{k}[X,Y,Z]}{\langle f+1\rangle}$, where $f$ is a homogeneous polynomial, minimal generating set for $\operatorname{Der} R$ can be computed explicitly.*

*Proof.* As discussed above, the module of derivations $\operatorname{Der} R$ is free of rank 2 and $\operatorname{Der}(R) = \langle \Delta_1, \Delta_2, \Delta_3 \rangle$.

Hence, the set $\{\Delta_1, \Delta_2, \Delta_3\}$ is $R$-linearly dependent. More precisely,

$$\frac{\partial f}{\partial X}\Delta_1 - \frac{\partial f}{\partial Y}\Delta_2 + \frac{\partial f}{\partial Z}\Delta_3 = 0.$$

Note that if one of the partial derivatives is a unit in $R$, say $\frac{\partial f}{\partial X}$; then $\Delta_1$ can be written as an $R$-linear combination of $\Delta_2$ and $\Delta_3$. Thus $\operatorname{Der}(R) = \langle \Delta_2, \Delta_3 \rangle$.

Consider the general case, where all the three partial derivatives are non-unit in $R$.

**Claim:** There exists an $R$-automorphism of $R^3$, which takes $(\Delta_1, \Delta_2, \Delta_3) \mapsto$

$(\eta_1, \eta_2, \eta_3)$ such that there exists an $R$-linear relation of $\eta_i$'s, with at least one of the coefficients of $\eta_i$'s a unit in $R$.

That is to find an invertible $3 \times 3$ matrix over $R$, say $A$, such that

$$\begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix}$$

and there exists $g_1, g_2, g_3 \in R$, such that at least one of them is a unit and $g_1\eta_1 + g_2\eta_2 + g_3\eta_3 = 0$.

Now,

$$\frac{\partial f}{\partial X}\Delta_1 - \frac{\partial f}{\partial Y}\Delta_2 + \frac{\partial f}{\partial Z}\Delta_3 = 0$$

implies:

$$\begin{aligned} \frac{\partial f}{\partial X}(a_{11}\eta_1 + a_{12}\eta_2 + a_{13}\eta_3) - \frac{\partial f}{\partial Y}(a_{21}\eta_1 + a_{22}\eta_2 + a_{23}\eta_3) \\ + \frac{\partial f}{\partial Z}(a_{31}\eta_1 + a_{32}\eta_2 + a_{33}\eta_3) = 0 \end{aligned}$$

i.e.,

$$\begin{aligned} \left(a_{11}\frac{\partial f}{\partial X} - a_{21}\frac{\partial f}{\partial Y} + a_{31}\frac{\partial f}{\partial Z}\right)\eta_1 + \left(a_{12}\frac{\partial f}{\partial X} - a_{22}\frac{\partial f}{\partial Y} + a_{32}\frac{\partial f}{\partial Z}\right)\eta_2 \\ + \left(a_{13}\frac{\partial f}{\partial X} - a_{23}\frac{\partial f}{\partial Y} + a_{33}\frac{\partial f}{\partial Z}\right)\eta_3 = 0 \end{aligned}$$

As $f$ is a homogeneous polynomial in $\mathbf{k}[X, Y, Z]$, we know that $X\frac{\partial f}{\partial X} + Y\frac{\partial f}{\partial Y} + Z\frac{\partial f}{\partial Z} = mf = -m$ in $R$.

Thus, choosing $a_{11} = X$, $a_{21} = -Y$ and $a_{31} = Z$ makes the coefficient of $\eta_1$ a unit in $R$. Thus it suffices to find a $3 \times 3$ invertible matrix over $R$ with the

first column:

$$\begin{bmatrix} X \\ -Y \\ Z \end{bmatrix}$$

Now, we can write $f = PX + Q \in \mathbf{k}[X, Y, Z]$, where $Q$ is a homogeneous polynomial in $\mathbf{k}[Y, Z]$ of degree $m$. We also note that, $Y$ divides $Q$ (since, $Z^m$ does not appear in $Q$ ).

Consider:

$$A = \begin{bmatrix} X & \frac{Q}{Y} & 0 \\ -Y & P & 0 \\ Z & 0 & 1 \end{bmatrix}$$

Thus $\det[A] = PX + Q = f$, a unit in $R$.

Also,

$$\begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} = A^{-1} \begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \end{bmatrix}$$

$$\text{i.e, } \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} = \begin{bmatrix} -P & \frac{Q}{Y} & 0 \\ -Y & -X & 0 \\ PZ & -\frac{QZ}{Y} & 1 \end{bmatrix} \begin{bmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \end{bmatrix}$$

Hence, a minimal generating set for Der $R$ can be given as,

$$\{\eta_2, \eta_3\} = \{-Y\Delta_1 - X\Delta_2, PZ\Delta_1 - \frac{QZ}{Y}\Delta_2 + \Delta_3\}$$

□

# Bibliography


[Bav10] V. V. Bavula. Generators and defining relations for the ring of differential operators on a smooth affine algebraic variety. *Algebr. Represent. Theory*, 13(2):159–187, 2010.

[Che55] Claude Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[Cox34] H. S. M. Coxeter. Discrete groups generated by reflections. *Ann. of Math. (2)*, 35(3):588–621, 1934.

[DGPS18] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4-1-1 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2018.

[DW18] Arindam Dey and Vinay Wagh. On the module of derivations of certain rings of invariants. *J. Ramanujan Math. Soc.*, 33(2):149–158, 2018.

[GW08] R. V. Gurjar and Vinay Wagh. On the number of generators of the module of derivations and multiplicity of certain rings. *J. Algebra*, 319(5):2030–2049, 2008.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

[NS02] Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.

[Sag16] SAGE mathematics software, 2016. `http://www.sagemath.org/`.

[Sai71] Kyoji Saito. Quasihomogene isolierte Singularitäten von Hyperflächen. *Invent. Math.*, 14:123–142, 1971.

[Ser68] Jean-Pierre Serre. Groupes finis d'automorphismes d'anneaux locaux réguliers. In *Colloque d'Algèbre (Paris, 1967), Exp. 8*, page 11. Secrétariat mathématique, Paris, 1968.

[ST54] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canadian J. Math.*, 6:274–304, 1954.

[Sus77] A. A. Suslin. Stably free modules. *Mat. Sb. (N.S.)*, 102(144)(4):537–550, 632, 1977.