ON THE CENTER OF THE RING OF INVARIANT DIFFERENTIAL OPERATORS ON SEMISIMPLE GROUPS OVER FIELDS OF POSITIVE CHARACTERISTIC

BY

HONGFEI TIAN

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2017

Urbana, Illinois

Doctoral Committee:

Professor Maarten Bergvelt, Chair
Professor William J. Haboush, Director of Research
Professor Alexander Yong
Professor Thomas Nevins

Abstract

In this thesis we prove the existence of Jordan Decomposition in $\mathcal{D}_{G/\mathbf{k}}$, the ring of invariant differential operators on a semisimple algebraic group over a field of positive characteristic, and its corollaries. In particular, we define the semisimple center of $\mathcal{D}_{G/\mathbf{k}}$, denoted by $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}})$, as the set of semisimple elements of its center. Then we show that if G is connected, the semisimple center $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}})$ contains $\mathcal{Z}_s(\mathcal{D}^{(\nu)}_{G/\mathbf{k}})$ for any positive integer ν, where $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$ is the ring of invariant differential operators on a Frobenius kernel derived from G.

To my parents, for their love and support.

Acknowledgments

Let me begin by offering my sincere gratitude to my advisor, William J. Haboush, for not only sharing with me his substantial knowledge of advanced mathematics, but also being a supportive life mentor. I wouldn't have been able to finish this dissertation without his constant support.

Besides, I also wish to show my gratitude to Professors Maarten Bergvelt, Alexander Yong, and Thomas Nevins for serving on my thesis committee and providing comments. I am grateful towards them for their kindness, for fruitful conversations, and for their contribution to my mathematical vision.

Furthermore, I want to thank my friends from the department of mathematics, who shared pain and gain with me during this unforgettable time.

Finally, I would like to thank my family. No matter what difficulty I meet, they always stand behind me and give me the best encouragement.

Table of Contents

List of Symbols . . . . **vi**

Introduction **1**

Chapter 1 Algebraic Groups **6**
- 1.1 Preliminary Category Theory 6
- 1.2 Group Schemes and Algebraic Groups 9
- 1.3 Representations 13

Chapter 2 Invariant Differential Operators **16**
- 2.1 Hopf Algebra Structure 16
- 2.2 Examples 20
- 2.3 Modules and Enveloping Algebras 26

Chapter 3 Frobenius Kernels **30**
- 3.1 The Frobenius Morphism 30
- 3.2 The Structure of $\mathcal{D}^{(\nu)}$ 31

Chapter 4 Semisimple Center **38**
- 4.1 Existence of Jordan Decomposition 38
- 4.2 A Theorem on the Semisimple Center of $\mathcal{D}^{(\nu)}$ 42
- 4.3 Harish-Chandra Centers 44

Chapter 5 Verma Modules **46**
- 5.1 Introduction to Verma Modules 46
- 5.2 Submodules of a Verma Module 47

Chapter 6 Integrals and Infinitesimal Verma Modules **50**
- 6.1 Integral of a Hopf Algebra 50
- 6.2 Central Operator Constructions 52
- 6.3 Infinitesimal Verma Modules 54

References **57**

Index **60**

List of Symbols

Without otherwise mentioning, the following symbols are usually used to denote objects as follows.

$\mathfrak{C}$	a (small) category
$\mathrm{obj}(\mathfrak{C})$	the set of objects of $\mathfrak{C}$
$\mathfrak{Sch}$	the category of schemes
p	a positive prime number
$\mathbb{F}_p$	the prime field of p elements
$\mathbf{k}$	a field
$\mathbb{C}$	the field of complex numbers
V^*	the linear dual space of a vector space V
δ_{st}	the Kronecker symbol
G	an algebraic group or group scheme over $\mathbf{k}$
$\mathbf{k}[G]$	the coordinate ring of G
G_a	$\operatorname{Spec}\mathbf{k}[x]$, the additive group
G_m	$\operatorname{Spec}\mathbf{k}[t,t^{-1}]$, the multiplicative group
e	the identity element in G
G°	the connected component of G containing e
$\mathfrak{m}_e$	the maximal ideal of $\mathbf{k}[G]$ corresponding to e
$\mathcal{D}_{G/\mathbf{k}}$	the ring of invariant differential operators over G
m^*	the comultiplication of $\mathcal{D}_{G/\mathbf{k}}$
ε	the counit map of $\mathcal{D}_{G/\mathbf{k}}$

$\mathbf{s}$	the antipode map of $\mathcal{D}_{G/\mathbf{k}}$
$\mathcal{D}^{\{n\}}$	$\{\sigma \in \mathcal{D}_{G/\mathbf{k}} \mid \sigma(\mathfrak{m}_e^{n+1}) = 0\}$, a subspace of $\mathcal{D}_{G/\mathbf{k}}$
$\mathcal{D}^{\{n\}+}$	$\{\sigma \in \mathcal{D}^n \mid \sigma(1) = 0\}$, the augmentation ideal of $\mathcal{D}^{\{n\}}$
$B^{\pm}$	a pair of opposite Borel subgroups of G
$U^{\pm}$	the unipotent radicals of $B^{\pm}$
T	$B^+ \cap B^-$, the maximal torus contained in them
$\mathfrak{g}$	the Lie algebra of G
$U(\mathfrak{g})$	the universal enveloping algebra of $\mathfrak{g}$
$\mathfrak{h}$	a Cartan subalgebra of L
Φ	the set of roots with respect to T
α	a root in Φ
$\alpha^{\vee}$	the coroot associated to α
Δ	the simple roots in Φ with respect to B^+; the comultiplication of $\mathbf{k}[G]$
ℓ	usually the number of simple roots in Δ, also the dimension of $\mathfrak{h}$
α_i	a simple root in Δ, $i = 1, 2, \cdots, \ell$
ω_i	a fundamental dominant weight, $i = 1, 2, \cdots, \ell$
$\Phi^{\pm}$	the positive and negative roots with respect to Δ (or B^+)
m	usually the number of positive roots in Φ^+
β_j	a positive root in Φ^+, $j = 1, 2, \cdots, m$
ρ	$\frac{1}{2}(\beta_1 + \cdots + \beta_m) = \omega_1 + \cdots + \omega_\ell$
$\mathcal{W}$	the Weyl group of G with respect to T
G_α	the centralizer of the subtorus $(\operatorname{Ker}\alpha)^0$ of T
u_α	the isomorphism from G_a into G such that $tu_\alpha(b)t^{-1} = u_\alpha(\alpha(t)b)$, $t \in T$
U_α	the image of u_α in G (also in G_α)
x_α	the coordinate function on U_α, $\mathbf{k}[U_\alpha] \simeq \mathbf{k}[x_\alpha]$
$X_\alpha^{[s]}$	the differential operator in $\mathcal{D}_{U_\alpha/\mathbf{k}}$ such that $X_\alpha^{[s]}(x_\alpha^t) = \delta_{st}$
Y_α	$X_{-\alpha}$, $\alpha \in \Phi^+$

H_α	$[X_\alpha, Y_\alpha]$
ν	a positive integer usually appears in the power p^ν
G_ν	the ν-th twisted group scheme of G
$F^{(\nu)}$	the ν-th Frobenius morphism
$G^{(\nu)}$	$\operatorname{Ker} F^{(\nu)}$
$\mathfrak{m}_e^{\{\nu\}}$	the ideal generated by the p^ν-th power of the elements of $\mathfrak{m}_e$
$\mathcal{D}^{(\nu)}$	$\mathcal{D}_{G^{(\nu)}/\mathbf{k}}$, the invariant differential operators over $G^{(\nu)}$
$[n]!$	the Cartier factorial of n
$\binom{n}{m}_p$	p-binomial coefficient
$\binom{n}{i,j,k}_p$	p-trinomial coefficient
$\mathbb{X}$	the character group of a torus
$\mathbf{a}$	a tuple of non-negative integers $(a_m, \ldots, a_1)$
$\mathbf{X}(\mathbf{a})$	the product $X_m^{[a_m]} \cdots X_1^{[a_1]}$
$\mathbf{c}$	a tuple of non-negative integers $(c_1, \ldots, c_\ell)$
$\binom{\mathbf{H}}{\mathbf{c}}$	the product $\binom{H_1}{c_1} \cdots \binom{H_\ell}{c_\ell}$
$\lvert\mathbf{a}\rvert$	$\sum_{i=1}^m a_i$
$\mathcal{Z}_s(\mathcal{D})$	the semisimple center of $\mathcal{D}$
λ	a weight, or a character
$\mathbf{k}_\lambda$	the one dimensional G-representation with action given by λ
$Z(\lambda)$	the Verma module over G of highest weight λ
$\Pi(V)$	the set of weights occur in a G-module V

Introduction

In this thesis we study the center of the ring of invariant differential operators on a semisimple algebraic group over a field of positive characteristic. This has long been an object of great interest to representation theorists. It is well-known that over a field of characteristic 0 the representation theory of a connected algebraic group G is very well reflected by the representation theory of its Lie algebra $\mathfrak{g}$ ([25]). Any representation of G gives rise to a representation of $\mathfrak{g}$. Then the notions of "submodule", "fixed point", or "module homomorphism" yield the same result whether applied to G-modules or to $\mathfrak{g}$-modules. This is no longer true in characteristic $p > 0$. Any G-module still leads to a $\mathfrak{g}$-module in a natural way, but now there may be $\mathfrak{g}$-submodules that are not G-submodules, or $\mathfrak{g}$-homomorphisms that are not G-homomorphisms, etc ([19]). It is, however, still possible to save some of the advantages of the linearization process (of going from G to $\mathfrak{g}$) by looking not only at $\mathfrak{g}$, but at the algebra $\mathcal{D}_{G/\mathbf{k}}$ of all invariant differential operators on G. (See § 2.1 for definition). It can also be defined as the ring of distributions on G with support in the origin ([19], I, § 7.1), or as special deviations ([9], II, 4, 5.2). It can be shown that all these definitions are equivalent ([9], II, 4, 5.7). In characteristic 0 there is not more information contained in $\mathcal{D}_{G/\mathbf{k}}$ than in $\mathfrak{g}$, as in this case $\mathcal{D}_{G/\mathbf{k}}$ is isomorphic to $U(\mathfrak{g})$, the universal enveloping algebra of $\mathfrak{g}$. This changes in prime characteristic and there $\mathcal{D}_{G/\mathbf{k}}$ will do everything that $\mathfrak{g}$ does not do ([19], I, § 7.14-7.17).

The dominant approach to the representation theory of G has been through quantized enveloping algebras ([1], [18], [22]), or by means of category theoretic methods ([6]). One unintended side effect of this work is that much of the basic algebra of $\mathcal{D}_{G/\mathbf{k}}$ remains unexamined. Inspired by the great success of Harish-Chandra's Theorem in characteristic 0, which characterizes the center of the universal enveloping algebra of $\mathfrak{g}$ ([29], § 4.10), we are trying to establish an analogue of this theory for the center of $\mathcal{D}_{G/\mathbf{k}}$ in positive characteristic. V. Kac and B. Weisfeiler described the center of $\mathcal{D}_{G/\mathbf{k}}^{(1)}$ (see § 1.3 for definition) using coadjoint actions ([20]). In his Marie-Paule Malliavin Seminar paper ([12]), W. Haboush calculated the integral of $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$ (see § 1.3 and § 4.1 for definitions) and used this to construct certain central differential operators that can not be generated from the Harish-Chandra center (§ 6.2).

Let $\mathcal{W}$ be the Weyl group, and $\mathbb{X}$ be the set of weights on G. The classical Harish-Chandra's Theorem described the center of $U(\mathfrak{g})$ as the set of $\mathcal{W}$-invariant weights in the sense that two weights λ and μ are "linked" if $\lambda + \rho$ and $\mu + \rho$ are $\mathcal{W}$-conjugate, where ρ is the half sum of all positive roots. The ultimate result of this research would be an analogous version of this phenomenon in the context of positive characteristic. One possible way is to find a generalized Weyl group $\widetilde{\mathcal{W}}$, a generalize set of weights $\widehat{\mathbb{X}}_p$, and identify the center of $\mathcal{D}_{G/\mathbf{k}}$ as a set of $\widetilde{\mathcal{W}}$-invariant functions on $\widehat{\mathbb{X}}_p$. Such a function f should satisfy that for any $w \in \widetilde{\mathcal{W}}$ and $\lambda \in \widehat{\mathbb{X}}_p$, there is $f(w(\lambda + \rho)) = f(\lambda + \rho)$.

One breakthrough on this journey, which is also the main result of this thesis, is a Jordan decomposition theorem for elements of the ring $\mathcal{D}_{G/\mathbf{k}}$, a phenomenon completely unlike anything true in characteristic zero. This gives us the chance of defining the notion of "semisimple center", $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}})$. This object is very interesting as we have observed its compatibility with the filtration on $\mathcal{D}_{G/\mathbf{k}}$ given by kernel of Frobenius (4.2.3). This greatly inspired us to construct a natural lifting from the semisimple center of $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$ to the semisimple center of $\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)}$, and to use induction on the Kac-Weisfeiler's base case of $\nu = 1$. The question of finding the correct lifting is still open, and is of our future interest. Along the Jordan decomposition, this thesis assembles a small collection of partial results we have developed along the way.

In order to be more self-explanatory, we start Chapter 1 by introducing the categorical approach of definitions. In this way only a minimal level of prerequisite is required. The notion of group schemes and algebraic groups are defined in section 1.2. We then briefly review the most basic representations that one can find in any algebraic group theory textbook.

Our main object of interest, the ring of invariant differential operators on G, is discussed in the second chapter. Let $\mathbf{k}[G]^*$ be the linear dual of the coordinate ring of G. We define the ring $\mathcal{D}_{G/\mathbf{k}}$ as the subspace of $\mathbf{k}[G]^*$ containing those operators that vanish on some power of the maximal ideal $\mathfrak{m}_e$, the one corresponds to the group identity of G. That is, $\sigma \in \mathcal{D}_{G/\mathbf{k}}$ if $\sigma(\mathfrak{m}_e)^n = 0$ for some integer $n > 0$. Right after the definition, we explored its Hopf structure. We showed that it is a well-defined cocommutative Hopf algebra with fruitful module structures around. In section 2.2, two fundamental examples, G_a and G_m, are calculated in details. The notations and results developed here are intensively referred in the sequel.

Chapter 3 is on the topic of Frobenius kernels. The Frobenius map is a special endomorphism that lives only in the world of prime characteristic. By considering the correct form of Frobenius maps in our case, we obtain a series of interesting infinitesimal group schemes, $G^{(\nu)}$, derived from G. In section 3.2, the structure theory of $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$, the ring of invariant differential operators on $G^{(\nu)}$, is introduced. We can see that each of them is a finite dimensional Hopf algebra. They form a direct system with $\mathcal{D}_{G/\mathbf{k}}$ as the limit. We give a clear characterization of these operators when G is a torus in terms of locally constant functions on the group algebra of characters on G. Then we explain a "PBW basis theorem" for $\mathcal{D}_{G/\mathbf{k}}$. The basis is also called a "Kostant's $\mathbb{Z}$-form". The definitions and results in the first three chapters are more or less contained in [9], [12], [19], [29], and [33].

In Chapter 4 we state and prove the main result, Jordan decomposition theorem of $\mathcal{D}_{G/\mathbf{k}}$. We show that Jordan decomposition is very well defined in $\mathcal{D}_{G/\mathbf{k}}$. It then allow us to use the term "semisimple" and "nilpotent" in this ring, and therefore we can define the semisimple center. To prove this property, we consider the filtration given by the Frobenius kernels. Since each of them is finite dimensional, there is the usual Jordan decomposition on it. To generalize it to the whole ring, it suffices to show that $\mathcal{D}_{G/\mathbf{k}}$ is a free module over each $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$. We give this proof in section 4.1. It doesn't require too much argument since we have already figured out their bases in the previous chapter.

In section 4.2 we state and prove our second result. It is an interesting corollary of the Jordan decomposition, and the proof we provide is also very short and elegant. Consider the set of semisimple elements in the center of $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$, denoted by $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu)})$. It forms a subalgebra and we call it the semisimple center. As $\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)}$ contains and is much larger than $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$, we show that $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)})$ also contains $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu)})$, provided that G is a connected group. This result inspired us to construct a "lifting" from $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu)})$ to $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)})$, and many effort has been put on this direction. This can be an explict map from $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$ to $\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)}$ that, if restricted to the semisimple center, is surjectively onto the semisimple center of the upper level. On the another hand, We can also try to directly construct elements in $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu+1)})$ in terms of elements in $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(\nu)})$. We are still searching for the right construction. Once such construction is done, we can inductively construct every semisimple central element of $\mathcal{D}_{G/\mathbf{k}}$ in terms of those in $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}}^{(1)})$. The structure of the center of $\mathcal{D}_{G/\mathbf{k}}^{(1)}$ has been well studied by many people. For instance, Kac and Weisfeiler provide a good characterization in [20]. Experts of Crystalline differential operators may also be interested in the relation between the "Harish-Chandra center" and semisimple center. We briefly discuss this in section 4.3.

From Chapter 5 we focus on the Verma modules and infinitesimal Verma modules (also called "baby Verma modules") over G. Analogous to the Verma modules defined by universal enveloping algebras in characteristic 0, we also have the notion of Verma modules in characteristic p defined as $\mathcal{D}_{G/\mathbf{k}} \otimes_{\mathcal{D}_{B/\mathbf{k}}} \mathbf{k}_\lambda$, where B is a chosen Borel subgroup and $\mathbf{k}_\lambda$ is the 1-dimensional module of weight λ. It consists of weights of the form $\lambda - \sum_{i=1}^{\ell} k_i\alpha_i$, $k_i \in \mathbb{Z}^+$, where α_i's are simple roots. Among these weights some are maximal, in the sense that they vanish under the action of $\mathcal{D}_{U^+/\mathbf{k}}$. They correspond to the submodules. Take a simple monomial $Y_{\alpha_i}^{[t]}$ in $\mathcal{D}_{U^-/\mathbf{k}}$. Its action on a maximal vector v_λ gives a vector of weight $\lambda - t\alpha_i$. We answer the following quesion in section 5.2: what property of t implies maximality of

$\lambda - t\alpha_i$ in terms of λ and α_i?

In Chapter 6 we introduce another important object related to the center, the integral of a Hopf algebra. The Fundamental Theorem of Hopf Module shows that for a finite dimensional Hopf algebra H, its linear dual, H^*, is a free rank one H-module. A basis vector is called an integral (also called "norm form") in H^*. Apply this theorem to our case, we can explicitly write out the integral of each $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$. These objects are of great interest because we can use them to construct central operators directly (§ 6.2). This is another possible direction of tackling the entire problem, since it suffices to show that this construction covers all the central operators. Unfortunately this is not obvious at all. As a side result, we explore in section 6.3 of some kinds of submodules we can generate using integrals. We show that some constructions turn out to be baby Vermal modules with certain maximal weights.

Chapter 1

Algebraic Groups

In this first chapter we review some definitions and basic facts pertaining to group schemes. We adopt the categorical approach that widely used in modern algebraic group theory books, such as [19] and [32]. Readers are assumed to have basic knowledge on category theory, algebraic geometry, and representation theory at level of [2], [14], [16], [17], or [25]. Notations and conventions are mainly following Jantzen in [19].

1.1 Preliminary Category Theory

Definition 1.1.1. Let $\mathfrak{C}$ be a category. A *final object* $*$ in $\mathfrak{C}$ is an object such that for any $X \in \text{obj}(\mathfrak{C})$, there is a unique morphism $t_X : X \to *$ such that for every morphism $f : X \to Y$ in $\mathfrak{C}$, the following diagram commutes.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & {\scriptstyle t_X}\searrow \quad \swarrow{\scriptstyle t_Y} & \\ & * & \end{array} \tag{1.1.1}$$

A *product* $X_1 \times X_2$ of objects X_1 and X_2 in $\mathfrak{C}$ is an object Y with two morphisms $p_1 : Y \to X_1$, and $p_2 : Y \to X_2$, such that for any object Z and any pair of morphisms $f_1 : Z \to X_1$, $f_2 : Z \to X_2$ there exists a unique morphism $f : Z \to Y$ such that the following diagram commutes.

$$\begin{array}{ccccc} & & Z & & \\ & \swarrow^{f_1} & \downarrow f & \searrow^{f_2} & \\ X_1 & \xleftarrow{p_1} & Y & \xrightarrow{p_2} & X_2 \end{array} \tag{1.1.2}$$

The definition of the product amounts to say that the map

$$\mathrm{Hom}(Z, Y) \to \mathrm{Hom}(Y, X_1) \times \mathrm{Hom}(Y, X_2)$$

sending f to the pair $(p_1 \circ f, p_2 \circ f)$ is an isomorphism of functors for any Z. Note that by Yoneda's Lemma, any product $X_1 \times X_2$ of X_1 and X_2 in $\mathfrak{C}$ is unique up to isomorphism.

Definition 1.1.2. Suppose $\mathfrak{C}$ is a category with product and final object $*$. A *group* in $\mathfrak{C}$ is an object G with morphisms $\mu : G \times G \to G$, $s : G \to G$, and $e : * \to G$, such that the following diagrams commute.

$$\begin{CD} G\times G\times G @>{\mu\times \mathrm{id}}>> G\times G \\ @V{\mathrm{id}\times\mu}VV @VV{\mu}V \\ G\times G @>{\mu}>> G \end{CD} \tag{1.1.3}$$

$$\begin{CD} *\times G @>{e\times\mathrm{id}}>> G\times G \\ @A{(t_G,\mathrm{id})}AA @VV{\mu}V \\ G @>{\mathrm{id}}>> G \\ @V{(\mathrm{id},t_G)}VV @AA{\mu}A \\ G\times * @>{\mathrm{id}\times e}>> G\times G \end{CD} \tag{1.1.4}$$

$$\begin{array}{ccccc} G\times G & \xrightarrow{s\times\mathrm{id}} & G\times G & \xrightarrow{\mu} & G \\ \uparrow{\scriptstyle\Delta} & & & & \uparrow{\scriptstyle e} \\ G & & \xrightarrow{\quad t_G \quad} & & * \\ \downarrow{\scriptstyle\Delta} & & & & \downarrow{\scriptstyle e} \\ G\times G & \xrightarrow{\mathrm{id}\times s} & G\times G & \xrightarrow{\mu} & G \end{array} \tag{1.1.5}$$

In diagiam 1.1.5 above, the map Δ is the diagonal map that sends g to (g, g).

Example 1.1.3. A group in the category of groups is an Abelian group.

Final object and product exist in the category of groups, namely, the trivial group and the direct product of groups. In order to have the three diagrams commute, the maps μ, s, and e must be the group multiplication, antipode, and inclusion of identity of G respectively. But antipode is not a group homomorphism unless G is Abelian.

Proposition 1.1.4. *An object G is a group in a category $\mathfrak{C}$ if and only if for any object $T \in \mathrm{obj}(\mathfrak{C})$ there is a multiplication μ_T on $\mathrm{Hom}(T, G)$ such that $\mathrm{Hom}(T, G)$ is a group and the assignment $T \mapsto \mathrm{Hom}(T, G)$ is a functor from $\mathfrak{C}$ to the category of groups.*

Proof. Suppose G is a group in $\mathfrak{C}$, and $T \in \mathrm{obj}(\mathfrak{C})$, we give a group structure on $\mathrm{Hom}(T, G)$ as follows. Let u and v be elements of $\mathrm{Hom}(T, G)$. Define $uv = \mu \circ (u, v)$, $e_T = e \circ t_T$, and $u^{-1} = s \circ u$.

$$uv : T \xrightarrow{(u,v)} G \times G \xrightarrow{\mu} G, \tag{1.1.6}$$

$$e_T : T \xrightarrow{t_T} * \xrightarrow{e} G, \tag{1.1.7}$$

$$u^{-1} : T \xrightarrow{u} G \xrightarrow{s} G. \tag{1.1.8}$$

It is straightforward to check that these constructions give a group structure on $\mathrm{Hom}(T, G)$ and the map $T \mapsto \mathrm{Hom}(T, G)$ is functorial.

Now if G is a group object in $\mathfrak{C}$, then by definition, $\mathrm{Hom}(G \times G, G)$ is a group. Define $\mu = p_1 \cdot p_2$, where p_1 and p_2 are the canonical projections in $\mathrm{Hom}(G \times G, G)$. Let $e \in \mathrm{Hom}(*, G)$ be the identity element of the group, and $s = (\mathrm{id})^{-1} \in \mathrm{Hom}(G, G)$, where $\mathrm{id} \in \mathrm{Hom}(G, G)$ is the identity morphism from G to G. Then μ, e, and s satisfy the commutative relations defined in Definition 1.1.2. Hence G is a group in $\mathfrak{C}$. $\square$

1.2 Group Schemes and Algebraic Groups

Definition 1.2.1. Let S be a fixed scheme, and $\mathfrak{Sch}(S)$ be the category of schemes over S. A *group scheme over* S is a group in $\mathfrak{Sch}(S)$.

From now on, unless explicitly stated otherwise, $\mathbf{k}$ will denote an algebraically closed field or a perfect field, $S = \mathrm{Spec}(\mathbf{k})$, and $\mathfrak{C} = \mathfrak{Sch}(S)$.

Definition 1.2.2. An (*linear*) *algebraic group* is a reduced affine group scheme over some $\mathbf{k}$.

Let $A = \mathbf{k}[G]$ be the coordinate ring of G, then $G = \mathrm{Spec}(A)$. The scheme morphisms

$$\mu : G \times_{\mathbf{k}} G \to G, \tag{1.2.1}$$

$$e : G \to \mathrm{Spec}(\mathbf{k}), \tag{1.2.2}$$

$$s : G \to G \tag{1.2.3}$$

induce the algebra morphisms,

$$\Delta : A \to A \otimes_{\mathbf{k}} A, \tag{1.2.4}$$

$$\varepsilon : A \to \mathbf{k}, \tag{1.2.5}$$

$$\mathbf{s} : A \to A. \tag{1.2.6}$$

They are usually called comultiplication, counit, and antipode of A in literatures. Suppose $f \in A$, and $\Delta(f) = \sum_i f_i \otimes f_i'$, for some f_i and f_i' in A, it is easy to check that for any

g and h in G,

$$f(gh) = \sum_i f_i(g) f'_i(h), \tag{1.2.7}$$

$$\varepsilon(f) = f(e), \tag{1.2.8}$$

$$(\mathbf{s}(f))(g) = f(g^{-1}). \tag{1.2.9}$$

Note that we are also using e to denote the element $e(\mathrm{Spec}(\mathbf{k}))$ in the group G. According to the group axioms of G, we have the following corresponding axioms of the algebra morphisms Δ, ε and $\mathbf{s}$.

$$\begin{CD} A @>\mu>> A \otimes_{\mathbf{k}} A \\ @V\Delta VV @VV\Delta\otimes\mathrm{id}V \\ A \otimes_{\mathbf{k}} A @>\mathrm{id}\otimes\Delta>> A \otimes_{\mathbf{k}} A \otimes_{\mathbf{k}} A \end{CD} \tag{1.2.10}$$

$$\begin{CD} \mathbf{k} \otimes A @<e\times\mathrm{id}<< A \otimes A \\ @VVV @AA\Delta A \\ A @<\mathrm{id}<< A \\ @AAA @VV\Delta V \\ A \otimes \mathbf{k} @<\mathrm{id}\times e<< A \otimes A \end{CD} \tag{1.2.11}$$

$$\begin{CD} A \otimes A @<\mathbf{s}\otimes\mathrm{id}<< A \otimes A @<\Delta<< A \\ @A\Delta AA @. @VVeV \\ A @<<< {} @<<< \mathbf{k} \\ @V\Delta VV @. @AAeA \\ A \otimes A @<\mathrm{id}\otimes\mathbf{s}<< A \otimes A @<\Delta<< A \end{CD} \tag{1.2.12}$$

Thus A is a coassociative coalgebra.

Example 1.2.3. $G_a = \mathrm{Spec}(\mathbf{k}[x])$.

$\Delta(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$, $\mathbf{s}(x) = -x$.

Example 1.2.4. $G_m = \mathrm{Spec}(\mathbf{k}[t, t^{-1}])$.

$\Delta(t) = t \otimes t$, $\varepsilon(t) = 1$, $\mathbf{s}(t) = t^{-1}$.

Example 1.2.5. $\mathrm{GL}(n, \mathbf{k})$.

Let δ be the determinant function on M_n, the set of $n \times n$ matrices. The *general linear group* $\mathrm{GL}(n, \mathbf{k})$ is the principal open set $\{X \in M_n \mid \delta(X) \neq 0\}$, with matrix multiplication as group operation.

We have $A = \mathbf{k}[x_{ij}, \delta^{-1}]_{1 \leq i,j \leq n}$. Now Δ, ε, and $\mathbf{s}$ are given by

$$\Delta(x_{ij}) = \textstyle\sum_{l=1}^{n} x_{il} \otimes x_{lj}, \tag{1.2.13}$$

$$\varepsilon(x_{ij}) = \delta_{ij}, \tag{1.2.14}$$

$$\mathbf{s}(x_{ij}) = \frac{C_{ij}}{\delta}, \tag{1.2.15}$$

where δ_{ij} is the Kronecker symbol and C_{ij} is the (i, j)-entry of the adjugate matrix. Note that we have $\Delta(\delta) = \delta \otimes \delta$, $\varepsilon(\delta) = 1$, and $\mathbf{s}(\delta) = \delta^{-1}$.

Example 1.2.6. $\mathrm{SL}(n, \mathbf{k})$.

$\mathrm{SL}(n, \mathbf{k})$ is the closed subgroup of $\mathrm{GL}(n, \mathbf{k})$ consisting of all the matrices with determinant 1. Thus $\mathbf{k}[\mathrm{SL}(n, \mathbf{k})] = \mathbf{k}[x_{ij}]_{1 \leq i,j \leq n}/(\delta - 1)$. The maps Δ and $\mathbf{s}$ are induced, on passing to the quotient, by those of $\mathbf{k}[\mathrm{GL}(n, \mathbf{k})]$.

Example 1.2.7. α_{p^ν} and μ_{p^ν}.

Let $\mathrm{char}(\mathbf{k}) = p$. Define $\alpha_{p^\nu} = \mathrm{Spec}(\mathbf{k}[x])/(x^{p^\nu})$ and $\mu_{p^\nu} = \mathrm{Spec}(\mathbf{k}[t, t^{-1}])/(t^{p^\nu} - 1)$. The maps Δ, ε, and $\mathbf{s}$ are defined the same as those maps of G_a and G_m respectively. These two groups occur naturally in thinking about representations in prime characteristics.

Jantzen defines groups schemes in terms of the notion of group functors ([19], I, § 2.3). This interpretation is also handy for our purposes. By Proposition 1.1.4, this definition is the same as ours.

Suppose A and B are $\mathbf{k}$-algebras. There is a natural isomorphism

$$\mathrm{Hom}(\mathrm{Spec}(B), \mathrm{Spec}(A)) \cong \mathrm{Hom}(A, B).$$

If $G = \mathrm{Spec}(A)$ is an algebraic group, we introduce the notation $G(B) = \mathrm{Hom}(A, B)$. Now we give a group structure on $G(B)$. Suppose Δ_A, ε_A, and $\mathbf{s}_A$ are the algebra maps associated to A. For $\varphi, \psi \in G(B)$, define the product $\varphi\psi = m_B \circ (\varphi \otimes \psi) \circ \Delta_A$, group identity $e = \mathrm{id}_{\mathbf{k}} \circ \varepsilon_A$ and inverse $\varphi^{-1} = \varphi \circ \mathbf{s}_A$, where $\mathrm{id}_{\mathbf{k}}$ is the inclusion of $\mathbf{k}$ into B. One can easily check that these constructions define a group structure on $G(B)$. Thus in this way G can be thought as a functor from the category of $\mathbf{k}$-algebras to the category of groups (the socalled *group functor*).

Let $G = \mathrm{GL}(n, \mathbf{k})$, then $A = \mathbf{k}[x_{ij}]_\delta$. An element $\varphi \in G(B) = \mathrm{Hom}(\mathbf{k}[x_{ij}]_\delta, B)$ is determined by the image of x_{ij}'s in B. Note that $\det(\varphi(x_{ij})) = \varphi(\delta)$, which is an invertible element in B. Hence φ is in one to one correspondence of the set of $n \times n$ invertible matrices over B.

Suppose $b = (b_{ij})$, $c = (c_{ij})$ are matrices over B. $\varphi_b, \varphi_c \in \mathrm{GL}(n, \mathbf{k})(B)$. $\varphi_b(x_{ij}) = b_{ij}$ and $\varphi_c(x_{ij}) = c_{ij}$. $1 \le i, j \le n$. We now compute the product $\varphi_b\varphi_c$.

$$\begin{aligned}
\varphi_b\varphi_c(x_{ij}) &= (m \circ (\varphi_b \otimes \varphi_c) \circ \Delta)(x_{ij}) \\
&= m((\varphi_b \otimes \varphi_c)(\sum_{l=1}^{n} x_{il} \otimes x_{lj})) \\
&= m(\sum_{l=1}^{n} b_{il} \otimes c_{lj}) \\
&= \sum_{l=1}^{n} b_{il} c_{lj} \qquad (1.2.16)
\end{aligned}$$

Thus we have $\varphi_b\varphi_c = \varphi_{bc}$. This shows the group structure on $\mathrm{GL}(n, \mathbf{k})(B)$ is the same as $\mathrm{GL}(n, B)$.

1.3 Representations

Definition 1.3.1. Let $G = \mathrm{Spec}(A) \in \mathfrak{C}$ be an affine algebraic group over $\mathbf{k}$, and V be a vector space over $\mathbf{k}$. A *rational representation* of G in V is a map $\alpha : V \to V \otimes_{\mathbf{k}} A$, such that the following two diagram commute.

$$\begin{CD} V @>{\alpha}>> V \otimes_{\mathbf{k}} A \\ @V{\alpha}VV @VV{\mathrm{id} \otimes \Delta}V \\ V \otimes_{\mathbf{k}} A @>{\alpha \otimes \mathrm{id}}>> V \otimes_{\mathbf{k}} A \otimes_{\mathbf{k}} A \end{CD} \tag{1.3.1}$$

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & V \otimes_{\mathbf{k}} A \\ & {\scriptstyle \mathrm{id}} \searrow \quad \swarrow {\scriptstyle \mathrm{id} \otimes \varepsilon} & \\ & V & \end{array} \tag{1.3.2}$$

Suppose $\mathbf{k}$ is algebraically closed. For $g \in G$, define the action $g.v = \mathrm{id} \otimes (\alpha(v))$. Then the above two commutative diagrams are exactly the same conditions that one uses to define the representation of an ordinary group. Namely, $g.(h.v) = (gh).v$ and $e.v = v$ for $g, h, e \in G$ and $v \in V$.

Suppose V is finite dimensional with basis $\{v_1, v_2, \cdots, v_n\}$. For every $j \in \{1, 2, \cdots, n\}$, we can write

$$\alpha(v_j) = \sum_{i=1}^{n} v_i \otimes f_{ij}, \quad f_{ij} \in A. \tag{1.3.3}$$

Hence

$$\begin{aligned} (\mathrm{id} \otimes \Delta) \circ \alpha(v_j) &= (\mathrm{id} \otimes \Delta) \left(\sum_{i=1}^{n} v_i \otimes f_{ij} \right) \\ &= \sum_{i=1}^{n} v_i \otimes \Delta(f_{ij}). \end{aligned} \tag{1.3.4}$$

$$\begin{aligned}(\alpha \otimes \mathrm{id}) \circ \alpha(v_j) &= (\alpha \otimes \mathrm{id}) \left(\sum_{l=1}^{n} v_l \otimes f_{lj} \right) \\ &= \sum_{l=1}^{n} \alpha(v_l) \otimes f_{lj} \\ &= \sum_{i,l=1}^{n} v_i \otimes f_{il} \otimes f_{lj}. \end{aligned} \tag{1.3.5}$$

Then the first commutative diagram gives that

$$\sum_{i=1}^{n} v_i \otimes \Delta(f_{ij}) = \sum_{i,l=1}^{n} v_i \otimes f_{il} \otimes f_{lj}. \tag{1.3.6}$$

Therefore

$$\Delta(f_{ij}) = \sum_{l=1}^{n} f_{il} \otimes f_{lj} \tag{1.3.7}$$

Similarly, by the second commutative diagram, we have

$$\begin{aligned} v_j &= (\mathrm{id} \otimes \varepsilon)(\alpha(v_j)) \\ &= \sum_{i=1}^{n} v_i \otimes \varepsilon(f_{ij}). \end{aligned} \tag{1.3.8}$$

Hence we have

$$\varepsilon(f_{ij}) = \delta_{ij}. \tag{1.3.9}$$

Consider the map $\varphi : G \to \mathrm{GL}_{\mathbf{k}}(V)$, from the algebraic group G to the set of nonsingular linear transformations of V, sending $g \in G$ to the matrix $(f_{ij}(g))$ under basis v_i. Then the relations 1.3.7 and 1.3.9 show that φ is a group homomorphism.

Example 1.3.2. Standard Representation of $\mathrm{GL}(n, \mathbf{k})$.

$A = \mathbf{k}[x_{11}, \cdots, x_{nn}]_\delta$. Let V be an n-dimensional vector space with the standard basis

$\{e_i\}$. Then $\alpha(e_j) = \sum_{i=1}^{n} e_i \otimes x_{ij}$ is a rational representation of G in V.

Example 1.3.3. Right Translation Representation.

For a fixed element g in an algebraic group G, consider the action of G on itself by right translation. $g : G \to G$, $x \mapsto xg$, $x \in G$. The corresponding algebra homomorphism on the coordinate ring A is given by $r_g : A \to A$, with $r_g(f)(x) = f(xg)$, $f \in A$, $x \in G$. Hence r gives a representation of G in $\mathrm{GL}(A)$. One can easily check that if $\Delta(f) = \sum_{i=1}^{n} f_i \otimes f'_i$, then $r_g(f) = \sum_{i=1}^{n} f'_i(g) f_i$.

The left translation representation is defined in the parallel way. For $g \in G$, define $l_g(f)(x) = f(g^{-1}x)$. We leave the details of this case to readers.

The following assertions are fundamental in algebraic group theory.

Lemma 1.3.4. *Let r_g be the right translation representation of G. For any $f \in A$, there exists a finite dimensional subrepresentation V containing f.*

Theorem 1.3.5. *Every affine algebraic group G is a closed subgroup scheme of* $\mathrm{GL}(n, \mathbf{k})$ *for some n.*

Detailed proofs and discussions can be found at [25].

Chapter 2

Invariant Differential Operators

In this chapter we introduce our main object of interest, the ring of invariant differential operators. It was studied by Demazure and Gabriel in [9], and then thoroughly discussed by Jantzen in [19]. Besides, [27], [29], and [33] are also helpful references.

2.1 Hopf Algebra Structure

Let G be an algebraic group. We first introduce the notation $\mathcal{D}^\circ = \mathbf{k}[G]^* = \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G], \mathbf{k})$, the linear dual of $\mathbf{k}[G]$. We simply write $\mathcal{D}^\circ$ if G and $\mathbf{k}$ are clear. Apparently $\mathcal{D}^\circ$ is a $\mathbf{k}$-vector space. It has an associative algebra structure and the multiplication can be defined as follows. Let

$$\Delta : \mathbf{k}[G] \to \mathbf{k}[G] \otimes \mathbf{k}[G]$$

be the comultiplication of the coalgebra $\mathbf{k}[G]$. Given σ, $\tau \in \mathcal{D}^\circ$, define their product by $\sigma\tau = (\sigma \otimes \tau) \circ \Delta$. That is, as the following composition shows,

$$\sigma\tau : \mathbf{k}[G] \xrightarrow{\Delta} \mathbf{k}[G] \otimes \mathbf{k}[G] \xrightarrow{\sigma\otimes\tau} \mathbf{k},$$

so that for any $f \in \mathbf{k}[G]$, if write $\Delta(f) = \sum f_i' \otimes f_i''$, then

$$\sigma\tau(f) = \sum \sigma(f_i')\tau(f_i''). \tag{2.1.1}$$

The associativity follows from the coassociativity of the comultiplication Δ. (cf. 1.2.10).

Let e be the identity element of G. The multiplicative identity in $\mathcal{D}^\circ$ is the operator 1. It operates on any $f \in \mathbf{k}[G]$ as the evaluation at e.

$$1(f) = f(e). \tag{2.1.2}$$

This makes $\mathcal{D}^\circ$ an associative algebra with unit.

The algebra $\mathcal{D}^\circ$ contains an important subalgebra, which can be interpreted as the ring of invariant differential operators on G, which we define as follows.

Definition 2.1.1. Let $\mathbf{k}$ be a field and G be an algebraic group over $\mathbf{k}$. Let e denote the identity element of G, and $\mathfrak{m}_e$ the maximal ideal of $\mathbf{k}[G]$ corresponding to e. The *ring of invariant differential operators* on G, denoted by $\mathcal{D}_{G/\mathbf{k}}$ (also $\mathcal{D}$ for simplicity), are the elements of $\mathcal{D}^\circ$, which vanish on some power of $\mathfrak{m}_e$:

$$\mathcal{D}_{G/\mathbf{k}} = \{\sigma \in \mathcal{D}^\circ \mid \sigma(\mathfrak{m}_e^n) = 0, \text{ for some integer } n > 0\}.$$

In the literature, it is also called the "*hyperalgebra*" of G ([27]), or the "*distributions*" on G with support at e ([9], [19]).

It is not directly obvious from this definition that $\mathcal{D}$ is a subalgebra of $\mathcal{D}^\circ$. To see this, we need the following lemma.

Lemma 2.1.2. *Suppose G is an algebraic group and H is a closed subscheme of G defined by the ideal I, i.e., we have a short exact sequence*

$$0 \longrightarrow I \longrightarrow \mathbf{k}[G] \longrightarrow \mathbf{k}[H] \longrightarrow 0\,.$$

Then H is a subgroup of G if and only if $\Delta(I) \subset I \otimes \mathbf{k}[G] + \mathbf{k}[G] \otimes I$.

Proof. Consider the diagram

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
I & \dashrightarrow & I \otimes \mathbf{k}[G] + \mathbf{k}[G] \otimes I \\
\downarrow & & \downarrow \\
\mathbf{k}[G] & \xrightarrow{\Delta} & \mathbf{k}[G] \otimes \mathbf{k}[G] \\
\downarrow & & \downarrow \\
\mathbf{k}[H] & \xrightarrow{\Delta} & \mathbf{k}[H] \otimes \mathbf{k}[H] \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

The columns are exact. H is a subgroup of G if and only if the lower square is commute. Hence their is an induced injection from I to $I \otimes \mathbf{k}[G] + \mathbf{k}[G] \otimes I$. □

Consider the trivial subgroup $\{e\}$ of G. It is defined by $\mathfrak{m}_e$. So by the above lemma, $\Delta(\mathfrak{m}_e) \subset \mathfrak{m}_e \otimes \mathbf{k}[G] + \mathbf{k}[G] \otimes \mathfrak{m}_e$. Therefore $\Delta(\mathfrak{m}_e^n) \subset \sum_{r=0}^{n} \mathfrak{m}_e^r \otimes \mathfrak{m}_e^{n-r}$ for any positive integer n. Now we have

Proposition 2.1.3. *$\mathcal{D}$ is a subalgebra of $\mathcal{D}^\circ$.*

Proof. The fact that $e \in \mathcal{D}$ is trivial. Suppose σ, $\tau \in \mathcal{D}$, then there exist r and s such that $\sigma(\mathfrak{m}_e^r) = 0$ and $\tau(\mathfrak{m}_e^s) = 0$. Hence

$$\begin{aligned}
\sigma\tau(\mathfrak{m}_e^{r+s}) &= (\sigma \otimes \tau) \circ \Delta(\mathfrak{m}_e^{r+s}) \\
&\subset (\sigma \otimes \tau) \left(\sum_t \mathfrak{m}_e^t \otimes \mathfrak{m}_e^{r+s-t} \right). \qquad (2.1.3)
\end{aligned}$$

This value is 0 because every term in the summation would either have $t \geq r$ or $r+s-t \geq s$. This shows that $\mathcal{D}$ is closed under the multiplication, therefore is a subalgebra. □

By abuse of notations, define a map $1 : \mathcal{D} \to \mathbf{k}$ be setting $1(\sigma) = \sigma(1)$ where the latter 1 is the constant polynomial in $\mathbf{k}[G]$. Since for $1 \in \mathbf{k}[G]$, $\Delta(1) = 1 \otimes 1$, we have for σ, $\tau \in \mathcal{D}$

$$\begin{aligned} 1(\sigma\tau) &= \sigma\tau(1) = (\sigma \otimes \tau)(1 \otimes 1) \\ &= \sigma(1)\tau(1) = 1(\sigma)1(\tau). \end{aligned} \tag{2.1.4}$$

Hence 1 is an algebra homomorphism. We can also define $s : \mathcal{D} \to \mathcal{D}$ be setting $s(\sigma) = \sigma \circ \mathbf{s}$, where $\mathbf{s} : \mathbf{k}[G] \to \mathbf{k}[G]$ is the coalgebra antipode of $\mathbf{k}[G]$ defined in 1.2.12, such that $\mathbf{s}(f)(g) = f(g^{-1})$ for any $f \in \mathbf{k}[G]$ and $g \in G$. Then suppose $\Delta(f) = \sum_i f_i' \otimes f_i''$, and thus $\Delta(\mathbf{s}(f)) = \sum_i \mathbf{s}(f_i'') \otimes \mathbf{s}(f_i')$, therefore

$$\begin{aligned} s(\sigma\tau) &= \sigma\tau(\mathbf{s}(f)) = (\sigma \otimes \tau)(\Delta(\mathbf{s}(f))) \\ &= (\sigma \otimes \tau)\left(\sum_i \mathbf{s}(f_i'') \otimes \mathbf{s}(f_i')\right) \\ &= \sum_i \tau(\mathbf{s}(f_i'))\sigma(\mathbf{s}(f_i'')) \\ &= (s(\tau) \otimes s(\sigma))(\Delta(f)) = (s(\tau)s(\sigma))(f). \end{aligned} \tag{2.1.5}$$

Hence s is an antihomomorphism and obviously $s^2 = \mathrm{id}$. This shows that $\mathcal{D}$ is an algebra with *augmentation* and *involution*.

In addition to being an associative algebra, $\mathcal{D}$ also has a cocommutative coalgebra structure. Consider for any positive integer n the set

$$\mathcal{D}^{\{n\}} = \{\sigma \in \mathcal{D} \mid \sigma(\mathfrak{m}_e^{n+1}) = 0\} = \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G]/\mathfrak{m}_e^{n+1}, \mathbf{k}). \tag{2.1.6}$$

Then we have $\mathcal{D} = \varinjlim \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G]/\mathfrak{m}_e^{n+1}, \mathbf{k}) = \varinjlim \mathcal{D}^{\{n\}}$. Consider the map of finite dimensional vector spaces given by multiplication

$$\mathbf{k}[G]/\mathfrak{m}_e^n \otimes \mathbf{k}[G]/\mathfrak{m}_e^n \xrightarrow{m} \mathbf{k}[G]/\mathfrak{m}_e^n.$$

Dualizing,

$$\mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G]/\mathfrak{m}_e^n, \mathbf{k}) \to \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G]/\mathfrak{m}_e^n, \mathbf{k}) \otimes \mathrm{Hom}_{\mathbf{k}}(\mathbf{k}[G]/\mathfrak{m}_e^n, \mathbf{k}).$$

i.e.,

$$\mathcal{D}^{\{n-1\}} \xrightarrow{m^*} \mathcal{D}^{\{n-1\}} \otimes \mathcal{D}^{\{n-1\}}.$$

Hence the dual of the multiplication on the algebra gives a comultiplication of differential operators. This makes each $\mathcal{D}^{\{n\}}$, together with their union $\mathcal{D}$, a coalgebra. If $\sigma \in \mathcal{D}$, we can then write

$$m^*(\sigma) = \sum_i \sigma_i' \otimes \sigma_i''. \tag{2.1.7}$$

This implies that for any f and g in $\mathbf{k}[G]$,

$$m^*(\sigma)(f \otimes g) = \sigma(fg) = \sum_i \sigma_i'(f)\sigma_i''(g). \tag{2.1.8}$$

With all the information above, it is then just routine to check the following proposition.

Proposition 2.1.4. *The data $(\Delta, e; m^*, \varepsilon, s)$ make $\mathcal{D}$ a cocommutative Hopf algebra with antipode and augmentation.* □

Detailed proofs can be found in [28].

2.2 Examples

In this section we calculate the structure of $\mathcal{D}_{G/\mathbf{k}}$ for $G = G_a$ and G_m. Let us look at firstly the additive group $G_a = \mathrm{Spec}(\mathbf{k}[t])$, with $\mathrm{char}(\mathbf{k}) = 0$. The identity ideal $\mathfrak{m}_e = (t)$, and $\mathbf{k}[t]/\mathfrak{m}_e^{n+1}$ has the residue classes $1, t, \ldots, t^n$ as a set of basis. For each $m = 0, 1, \ldots, n$, define notation $X^{[m]} \in \mathbf{k}[t]^*$ through

$$X^{[m]}(t^n) = \delta_{mn}. \tag{2.2.1}$$

Here δ_{mn} is the Kronecker symbol. Then one can check that $\mathcal{D}$ is a $\mathbf{k}$-vector space with basis $\{X^{[m]}\}_{m\geq 0}$ and each $\mathcal{D}^{\{r\}}$ has basis $\{X^{[m]}\}_{0\leq m\leq r}$. The multiplication is given by

$$X^{[m]}X^{[n]} = \binom{m+n}{m} X^{[m+n]}. \tag{2.2.2}$$

In particular,

$$(X^{[1]})^n = \binom{2}{1}\binom{3}{1}\cdots\binom{n}{1} X^{[n]} = n! X^{[n]} \tag{2.2.3}$$

or $X^{[n]} = \frac{1}{n!}(X^{[1]})^n$. So $\mathcal{D}_{G_a/\mathbb{C}}$ is isomorphic to $\mathbb{C}[X^{[1]}]$.

If $\mathrm{char}(\mathbf{k}) = p$, the above multiplication formula remains valid for m and $n < p$. For $n = p$ we immediately have

$$(X^{[1]})^p = p! X^{[p]} = 0. \tag{2.2.4}$$

This means $X^{[p]}$ can no longer be generated by $X^{[1]}$. Similar phenomena happen to $X^{[p^\nu]}$ for every integer $\nu \geq 1$.

Now recall the theorem of Lucas. For non-negative integers m and n and a prime number p, the following congruence relation holds:

$$\binom{m}{n} \equiv \prod_{\nu=0}^{q} \binom{m_\nu}{n_\nu} \pmod{p}, \tag{2.2.5}$$

where $m = \sum_{\nu=0}^{q} m_\nu p^\nu$ and $n = \sum_{\nu=0}^{q} n_\nu p^\nu$ are p-adic expansions of m and n respectively. This uses the convention that $\binom{m}{n} = 0$ if $m < n$. Therefore in characteristic p, we can define the p-binomial coefficients $\binom{m}{n}_p$ by

$$\binom{m}{n}_p = \prod_{\nu=0}^{q} \binom{m_\nu}{n_\nu}. \tag{2.2.6}$$

Notice that if an integer $n = n' + n_\nu p^\nu$ with $0 \leq n' < p^\nu$ and $0 < n_\nu < p$, using the notation defined above, we have

$$\binom{n}{n'}_p = \binom{n' + n_\nu p^\nu}{n'}_p = \binom{n'}{n'}_p \binom{n_\nu}{0} = 1. \tag{2.2.7}$$

Hence

$$X^{[n]} = \binom{n}{n'}_p X^{[n]} = X^{[n']} X^{[n_\nu p^\nu]} = \frac{1}{n_\nu!} X^{[n']} (X^{[p^\nu]})^{n_\nu}. \tag{2.2.8}$$

Therefore if n has p-adic expansion $n = \sum_{\nu=0}^{q} n_\nu p^\nu$, we have inductively

$$X^{[n]} = \frac{1}{[n]!} \prod_{\nu=0}^{q} (X^{[p^\nu]})^{n_\nu}, \tag{2.2.9}$$

where $[n]! = \prod_{\nu=0}^{q} n_\nu!$ is the Cartier factorial of n. So $\mathcal{D}_{G_a/\mathbf{k}}$ is generated as $\mathbf{k}$-algebra by $\{1, X^{[p^\nu]}\}_{\nu \geq 0}$. For the coalgebra structure, we have for the generators

$$m^*(X^{[p^\nu]}) = \sum_{i=0}^{p^\nu} X^{[i]} \otimes X^{[p^\nu - i]}, \tag{2.2.10}$$

and $\varepsilon(X^{[p^\nu]}) = 0$, $\mathbf{s}(X^{[p^\nu]}) = (-1)^{p^\nu} X^{[p^\nu]}$. It is then also true that for any $n > 0$,

$$m^*(X^{[n]}) = \sum_{i=0}^{n} X^{[i]} \otimes X^{[n-i]}. \tag{2.2.11}$$

Let us now consider the multiplicative group $G = G_m = \mathrm{Spec}(\mathbf{k}[t, t^{-1}])$, firstly in characteristic 0. The identity ideal $\mathfrak{m}_e$ is generated by $t - 1$. Writing $z = t - 1$, the residue classes of 1, z, …, z^n form a basis of $\mathbf{k}[G_m]/\mathfrak{m}_e^{n+1}$. Let $H^{[m]}$ be the unique operator such that

$$H^{[m]}(z^n) = \delta_{mn}. \tag{2.2.12}$$

Then by the binomial development of $t^n = (z+1)^n$ one gets

$$H^{[m]}(t^n) = \binom{n}{m}. \tag{2.2.13}$$

The set of all $H^{[m]}$ with $m \geq 0$ form a basis of $\mathcal{D}$ and those with $m \leq r$ form a basis of $\mathcal{D}^{\{r\}}$. The multiplication is given by

$$H^{[n]}H^{[m]} = \sum_{i=0}^{\min(n,m)} \binom{n+m-i}{n-i, m-i, i} H^{[n+m-i]}, \tag{2.2.14}$$

where

$$\binom{n+m-i}{n-i, m-i, i} = \frac{(n+m-i)!}{(n-i)!(m-i)!i!}, \tag{2.2.15}$$

is the trinomial coefficient. As a special case we get

$$H^{[1]}H^{[n-1]} = nH^{[n]} + (n-1)H^{[n-1]}, \tag{2.2.16}$$

hence

$$(H^{[1]} - (n-1))H^{[n-1]} = nH^{[n]} \tag{2.2.17}$$

and inductively

$$n!H^{[n]} = H^{[1]}(H^{[1]} - 1) \cdots (H^{[1]} - n + 1) \tag{2.2.18}$$

or

$$H^{[n]} = \binom{H^{[1]}}{n}. \tag{2.2.19}$$

Therefore $\mathcal{D}_{G_m/\mathbb{C}}$ is isomorphic to $\mathbb{C}[H^{[1]}]$.

Now consider the case of $\mathrm{char}(\mathbf{k}) = p$. Then

$$H^{[1]}H^{[p-1]} = pH^{[p]} + (p-1)H^{[p-1]} = (p-1)H^{[p-1]}, \tag{2.2.20}$$

so similarly each $H^{[p^\nu]}$ can no longer be generated by $H^{[1]}$. To properly use the notation of trinomial coefficients, we make a generalization of Lucas' Theorem as follows.

Lemma 2.2.1. *For non-negative integers n, r, s, $t = n - r - s$ and a prime number p, the* *following congruence relation holds:*

$$\binom{n}{r,s,t} \equiv \prod_{\nu=0}^{q} \binom{n_\nu}{r_\nu, s_\nu, t_\nu} \pmod{p}, \tag{2.2.21}$$

where n_ν, r_ν, s_ν, and t_ν are the p-adic digits of n, r, s, and t respectively. This uses the convention that $\binom{n}{r,s,t} = 0$ if n is less than either one of r, s and t.

Proof. For $n = p$ and $0 \le r, s, t < p$, the numerator of

$$\binom{p}{r,s,t} = \frac{p!}{r!s!t!} \tag{2.2.22}$$

is divisible by p but the denominator is not. Hence p divides $\binom{p}{r,s,t}$. In terms of generating functions, this means that

$$(x+y+z)^p \equiv x^p + y^p + z^p \pmod{p}. \tag{2.2.23}$$

Continuing by induction, we have for every non-negative interger ν that

$$(x+y+z)^{p^\nu} \equiv x^{p^\nu} + y^{p^\nu} + z^{p^\nu} \pmod{p}. \tag{2.2.24}$$

Now let n be general and suppose that $n = \sum_{\nu=0}^{q} n_\nu p^\nu$ for some non-negative integer q and integers n_ν for each ν so that $0 \le n_\nu < p$. Then notice that

$$(x+y+1)^n = \sum_{\substack{r,s,t \\ r+s+t=n}} \binom{n}{r,s,t} x^r y^s. \tag{2.2.25}$$

On the other hand,

$$\begin{aligned}(x+y+1)^n &= \prod_{\nu=0}^{q}((x+y+1)^{p^\nu})^{n_\nu} \equiv \prod_{\nu=0}^{q}(x^{p^\nu}+y^{p^\nu}+1)^{n_\nu} \\ &= \prod_{\nu=0}^{q}\left(\sum_{\substack{r_\nu,s_\nu,t_\nu \\ r_\nu+s_\nu+t_\nu=n_\nu}} \binom{n_\nu}{r_\nu, s_\nu, t_\nu} x^{r_\nu p^\nu} y^{s_\nu p^\nu}\right) \\ &= \sum_{\substack{r,s,t \\ r+s+t=n}} \left(\prod_{\nu=0}^{q}\binom{n_\nu}{r_\nu, s_\nu, t_\nu}\right) x^r y^s \pmod p, \end{aligned} \tag{2.2.26}$$

where in the final product, r_ν, s_ν, and t_ν are the ν-th p-adic digits of r, s and t respectively. This proves the lemma. □

Using Lemma 2.2.1, we can now define the p-trinomial coefficients as

$$\binom{n}{r, s, t}_p = \prod_{\nu=0}^{q}\binom{n_\nu}{r_\nu, s_\nu, t_\nu}, \tag{2.2.27}$$

and it is then meaningful to write

$$H^{[n]}H^{[m]} = \sum_{i=0}^{\min(n,m)} \binom{n+m-i}{n-i, m-i, i}_p H^{[n+m-i]}. \tag{2.2.28}$$

For an integer $n = n' + n_\nu p^\nu$ with $0 \le n' < p^\nu$ and $0 < n_\nu < p$, we have

$$\begin{aligned} H^{[n']}H^{[n_\nu p^\nu]} &= \sum_{i=0}^{n'} \binom{n-i}{n'-i, n_\nu p^\nu - i, i}_p H^{[n-i]} \\ &= \binom{n}{n', n_\nu p^\nu, 0}_p H^{[n]} + \sum_{i=0}^{n'} \binom{n-i}{n'-i, n_\nu p^\nu - i, i}_p H^{[n-i]}. \end{aligned} \tag{2.2.29}$$

Since

$$\binom{n}{n', n_\nu p^\nu, 0}_p = \binom{n'}{n', 0, 0}_p \binom{n_\nu}{0, n_\nu, 0} = 1 \tag{2.2.30}$$

and for $1 \le i \le n'$,

$$\binom{n-i}{n'-i, n_\nu p^\nu - i, i}_p = \binom{n'-i+n_\nu p^\nu}{n'-i, (p^\nu - i) + (n_\nu - 1)p^\nu, i}_p$$
$$= \binom{n'-i}{n'-i, p^\nu - i, i - p^\nu}_p \binom{n_\nu}{0, n_\nu - 1, 1} = 0. \tag{2.2.31}$$

This proves

$$H^{[n]} = H^{[n']} H^{[n_\nu p^\nu]} = H^{[n']} \binom{H^{[p^\nu]}}{n_\nu}, \tag{2.2.32}$$

and inductively

$$H^{[n]} = \prod_{\nu=0}^{q} \binom{H^{[p^\nu]}}{n_\nu}. \tag{2.2.33}$$

So $\mathcal{D}_{G_m/\mathbf{k}}$ is generated as $\mathbf{k}$-algebra by $\{1, H^{[p^\nu]}\}_{\nu \ge 0}$. For the coalgebra structure, we have

$$m^*(H^{[n]}) = \sum_{r+s \le n} H^{[r]} \otimes H^{[s]}. \tag{2.2.34}$$

2.3 Modules and Enveloping Algebras

There are various module structures on $\mathcal{D}$. For each $f \in \mathbf{k}[G]$ and $\sigma \in \mathcal{D}$ we define the action $f \cdot \sigma \in \mathcal{D}$ through

$$(f \cdot \sigma)(g) = \sigma(fg) \tag{2.3.1}$$

for all $g \in \mathbf{k}[G]$. In this way $\mathcal{D}$ is a right $\mathbf{k}[G]$-module. Obviously $\mathcal{D}$ also has module structures over itself by left and right multiplications. In addition to these two, it also has a $\mathcal{D}$-module structure induced by the conjugation action of G on itself. For σ and τ in $\mathcal{D}$, the action is

$$\sigma \circ \tau = \sum_i \sigma_i' \tau s(\sigma_i''), \tag{2.3.2}$$

where σ_i' and σ_i'' are in the same way defined as 2.1.7 in the comultiplication.

An element τ is called *invariant* under the action $\circ$ if for any σ,

$$\sigma \circ \tau = \varepsilon(\sigma)\tau. \tag{2.3.3}$$

The notion of invariant is such defined because if V is any representation of G, then $v \in V$ is a G-invariant, in the sense of $g.v = v$ for any $g \in G$, if and only if it is invariant for the $\mathcal{D}$ action in the sense of $\sigma.v = \varepsilon(\sigma)v$ for any $\sigma \in \mathcal{D}$.

Also if in addition $\delta \in \mathcal{D}$, we have

$$\sigma \circ (\tau\delta) = \sum_i (\sigma_i' \circ \tau)(\sigma_i'' \circ \delta). \tag{2.3.4}$$

For this property, we say that the action $\circ$ *measures* $\mathcal{D}$ to itself. This action is particularly useful when talking about the center of $\mathcal{D}$, because an element τ is in the center of $\mathcal{D}$ if and only if it is invariant under this action. (cf Lemma 4.2.2).

Any G-module (or G-representation) V is naturally a $\mathcal{D}$-module. Let

$$\begin{aligned} \Delta_V : V &\to V \otimes \mathbf{k}[G] \\ v &\mapsto \sum_i v_i \otimes f_i \end{aligned}$$

be the comodule map. Then the action of $\sigma \in \mathcal{D}$ on V is given by

$$V \xrightarrow{\Delta_V} V \otimes \mathbf{k}[G] \xrightarrow{\mathrm{id}_V \otimes \sigma} V \otimes \mathbf{k} \cong V, \tag{2.3.5}$$

i.e., $\sigma.v = \sum \sigma(f_i)v_i$. Any G-submodule of V is also a $\mathcal{D}$-submodule of V (cf. [19], I, §7.11(4)).

Consider the subalgebras $\mathcal{D}^{\{n\}}$ defined in 2.1.6. Clearly they give a filtration of $\mathcal{D}$ with

$$\mathcal{D}^{\{0\}} \subset \mathcal{D}^{\{1\}} \subset \cdots \subset \mathcal{D}^{\{n\}} \subset \cdots, \tag{2.3.6}$$

and more interestingly,

$$\mathcal{D}^{\{n\}}\mathcal{D}^{\{m\}} \subset \mathcal{D}^{\{n+m\}}. \tag{2.3.7}$$

(cf. [19] §7.7). If $\sigma \in \mathcal{D}^{\{n\}}$ and $\tau \in \mathcal{D}^{\{m\}}$, then

$$[\sigma, \tau] = \sigma\tau - \tau\sigma \in \mathcal{D}^{\{n+m-1\}}. \tag{2.3.8}$$

So $\mathcal{D}$ is a filtered associative algebra over $\mathbf{k}$ such that its associated graded algebra is commutative. Notice that

$$\mathcal{D}^{\{0\}} \cong \mathbf{k}^* \cong \mathbf{k}, \tag{2.3.9}$$

and for any n,

$$\mathcal{D}^{\{n\}} \cong \mathbf{k} \oplus \mathcal{D}^{\{n\}+}, \tag{2.3.10}$$

where $\mathcal{D}^{\{n\}+} = \{\sigma \in \mathcal{D}^{\{n\}} \mid \sigma(1) = 0\}$. In particular, $\mathcal{D}^{\{1\}+} \cong (\mathfrak{m}_e/\mathfrak{m}_e^2)^*$ as $\mathbf{k}$-vector spaces, and the fact that $[\mathcal{D}^{\{n\}+}, \mathcal{D}^{\{m\}+}] \subset \mathcal{D}^{\{n+m-1\}+}$ implies that $\mathcal{D}^{\{1\}+}$ is nothing but the Lie algebra of G.

Let $\mathfrak{g}$ be the Lie algebra of G, and $U(\mathfrak{g})$ its universal enveloping algebra. In characteristic 0, $U(\mathfrak{g})$ is isomorphic to $\mathcal{D}$, but in characteristic p the situation is quite different and $\mathcal{D}$ is a much larger algebra. Let $U^{[p]}(\mathfrak{g})$ denote the restricted enveloping algebra of $\mathfrak{g}$. One can show that there is an injective homomorphism $U^{[p]}(\mathfrak{g}) \to \mathcal{D}$ (cf. [9], II, §7).

We end this section by explaining why we call $\mathcal{D}$ the ring of invariant differential operators. There is a notion of differential operators on a scheme (cf. [9], II, §4, 5.3). In the case of an algebraic group G they can be described as follows ([9], II, §4, 5.7): Each $f \in \mathbf{k}[G]$ defines $\mathrm{ad}(f) : \mathrm{End}(\mathbf{k}[G]) \to \mathrm{End}(\mathbf{k}[G])$ through $(\mathrm{ad}(f)\phi)(f_1) = f\phi(f_1) - \phi(ff_1)$. In other words, $\mathrm{ad}(f)(\phi)$ is the commutator of the left multiplication by f and of ϕ. Then a differential operator on X of order $\leq n$ is some $\sigma \in \mathrm{End}(\mathbf{k}[G])$ with $\mathrm{ad}(f_0)\,\mathrm{ad}(f_1)\cdots\mathrm{ad}(f_n)\sigma = 0$ for all $f_0, f_1, \ldots, f_n \in \mathbf{k}[G]$. A differential operator on G is then defined as a differential operator of order $\leq n$ for some positive interger n. They form a subalgebra of $\mathrm{End}(\mathbf{k}[G])$.

Consider the action G on itself by left (resp. right) translation, then we get an action of any $\sigma \in \mathcal{D}$ as a differential operator on G that commutes with the action of G by multiplication on the other side. This construction turns out to yield an isomorphism of $\mathcal{D}$ onto the algebra of all differential operators on G that are right (resp. left) invariant (i.e., that commute with the action of G by right (resp. left) translation), cf. [9], II, §4, 6.5.

Chapter 3

Frobenius Kernels

In this chapter we give the definitions and elementary properties of *Frobenius kernels*. They are infinitesimal algebraic groups. We compute the structure of the ring of invariant differential operators on these groups. For more discussions in this area, [19] and [12] are good references.

3.1 The Frobenius Morphism

Let $\mathbf{k}$ be an algebraically closed field of characteristic p throughout and let G be a $\mathbf{k}$-group scheme. For each $\mathbf{k}$-algebra A and integer m we define $A^{(m)}$ as the $\mathbf{k}$-algebra that coincides with A as a ring with scalar $b \in \mathbf{k}$ acts as $b^{p^{-m}}$ does on A. One obviously has $A^{(0)} = A$ and

$$(A^{(m)})^{(n)} = A^{(m+n)} \tag{3.1.1}$$

for all $m, n \in \mathbb{Z}$. For each integer $\nu \geq 0$ the map

$$\gamma^{(\nu)} : A^{(m)} \to A^{(m-\nu)}, \quad f \mapsto f^{p^\nu} \tag{3.1.2}$$

is a homomorphism of $\mathbf{k}$-algebras. Now define for each ν a new group scheme G_ν by setting $G_\nu(A) = G(A^{(-\nu)})$ for all $\mathbf{k}$-algebras A, and define a morphism $F^{(\nu)} : G \to G_\nu$ through

$$F^{(\nu)}(A) = G(\gamma^{(\nu)}) : G(A) \to G(A^{(-\nu)}) = G_\nu(A) \tag{3.1.3}$$

for all A. We call $F^{(\nu)}$ the ν-th *Frobenius morphism* on G. Its kernel $G^{(\nu)} = \mathrm{Ker}(F^{(\nu)})$ is a normal subgroup scheme of G that is called the ν-th *Frobenius kernel* of G.

If $\mathbf{k} = \mathbb{F}_p$ and if G is defined over $\mathbb{F}_p$, then we can identify each G_ν with G and interpret $F^{(\nu)}$ as the ν-th power of some Frobenius endomorphism $F : G \to G$. This is true for example for $G = G_a$ and $G = G_m$. In both cases $F^*(t) = t^p$. Therefore $G_a^{(\nu)}$ is the group scheme such that $G_a^{(\nu)}(A) = \{f \in A \mid f^{p^\nu} = 0\}$, and $G_m^{(\nu)}$ is that $G_m^{(\nu)}(A) = \{f \in A \mid f^{p^\nu} = 1\}$. In general, write $\mathfrak{m}_e^{\{\nu\}}$ for the ideal generated by the p^ν-th power of elements of $\mathfrak{m}_e$. Then $G^{(\nu)} = \mathrm{Spec}(\mathbf{k}[G]/\mathfrak{m}_e^{\{\nu\}})$. We have an ascending chain

$$G^{(1)} \subset G^{(2)} \subset G^{(3)} \subset \cdots \tag{3.1.4}$$

of normal subgroup schemes of G. The Lie algebra of $G^{(\nu)}$ is the same as the Lie algebra of G, and the representation theory of $G^{(1)}$ is equivalent to that of $\mathfrak{g}$ as a restricted Lie algebra.

The ideals, $\mathfrak{m}_e^{\{\nu\}}$, are a cofinal system of ideals for the $\mathfrak{m}_e$-adic topology. Write $\mathcal{D}^{(\nu)}$ for $\mathcal{D}_{G^{(\nu)}/\mathbf{k}}$ and we then have $\mathcal{D} = \varinjlim_\nu \mathcal{D}^{(\nu)}$. Since $\mathfrak{m}_e^{\{\nu\}}$ are Hopf ideals, each $\mathcal{D}^{(\nu)}$ is a finite dimensional Hopf algebra. For the $\mathbf{k}[G]$-module structure on $\mathcal{D}$ defined in 2.1, $\mathcal{D}^{(\nu)}$ is a $\mathbf{k}[G]$-submodule for each ν.

The proofs of these assertions and many more details about Frobenius morphisms and Frobenius kernels can be found in [19], I, §9.

3.2 The Structure of $\mathcal{D}^{(\nu)}$

Now we are ready to develop the structure theory of $\mathcal{D}^{(\nu)}$. We mainly follow Haboush's work in [12]. Throughout $\mathbf{k}$ will be an algebraically closed field of characteristic p and G will be a semisimple, simply connected, connected algebraic group over $\mathbf{k}$. Then, B is a fixed Borel subgroup, T is a maximal torus contained in it, U is its unipotent radical and B^- and U^- are the Borel subgroup opposite to it with respect to T and the unipotent radical of B^-, respectively. Let Φ, respectively Φ^+ be the roots of T and those positive with respect to B.

Fix a particular order on the positive roots, Φ^+, for convenience. Suppose there are m positive roots. Choose an ordering $\alpha_1, \ldots, \alpha_m$ so that for any k the set of roots α_k, α_{k+1}, $\ldots$, α_m form an ideal in the root system. Recall that a set, $S \subseteq \Phi^+$, is an ideal if whenever $\alpha \in S$, $\beta \in \Phi^+$, then $\alpha + \beta \in \Phi^+$ implies that $\alpha + \beta \in S$. We can arrange this so that $\{\alpha_1, \ldots, \alpha_\ell\} = \Delta$ is the set of simple positive roots.

For any $\alpha \in \Phi$ let U_α be the corresponding root subgroup and let the map $x_\alpha : \mathbf{k} \to G$ be the corresponding parametrization, i.e., the homomorphism such that $tx_\alpha(b)t^{-1} = x_\alpha(\alpha(t)b)$, for $t \in T$ and $b \in \mathbf{k}$. The image of $x_\alpha(\mathbf{k})$ is U_α.

By taking the tangent map and expanding to higher degrees, the parametrization x_α induces an injection $\mathrm{d}x_\alpha : \mathcal{D}_{G_a/\mathbf{k}} \to \mathcal{D}_{G/\mathbf{k}}$. We write $X_\alpha^{[n]}$ for $\mathrm{d}x_\alpha(X^{[n]})$. Relative to the chosen order of positive roots, write $X_i^{[n]}$ for $X_{\alpha_i}^{[n]}$ and $Y_i^{[n]}$ for $X_{-\alpha_i}^{[n]}$. Let boldface symbols $\mathbf{a}, \mathbf{b}$, etc. refer to vectors of the corresponding variables. Then $\mathbf{X}(\mathbf{a})$ denotes $X_m^{[a_m]} X_{m-1}^{[a_{m-1}]} \cdots X_1^{[a_1]}$ and $\mathbf{Y}(\mathbf{b})$ denotes $Y_1^{[b_1]} Y_2^{[b_2]} \cdots Y_m^{[b_m]}$. For an integer n, let the boldface symbol $\mathbf{n}$ denote the m-dimensional vector $(n, \ldots, n)$ in which every entry is the number n. We write $\mathbf{a} < \mathbf{n}$ if $a_i < n$ for every $i = 1, \ldots, m$. With these notations, we have $\mathcal{D}_{U/\mathbf{k}}^{(\nu)}$ and $\mathcal{D}_{U^-/\mathbf{k}}^{(\nu)}$ are the $\mathbf{k}$-vector spaces with basis $\{\mathbf{X}(\mathbf{a})\}_{\mathbf{0} \le \mathbf{a} < \mathbf{p}^\nu}$ and $\{\mathbf{Y}(\mathbf{b})\}_{\mathbf{0} \le \mathbf{b} < \mathbf{p}^\nu}$ respectively.

Now we consider the elements of $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$. Let $\mathbb{X} = \mathbb{X}(T)$ denote the group of characters of T. Then the coordinate ring of T is the group algebra $\mathbf{k}[\mathbb{X}]$. For a character $\lambda \in \mathbb{X}$ we write t^λ when it is viewed as a function on T. Then the identity ideal $\mathfrak{m}_e$ of T is generated by $t^\lambda - 1$, and $\mathfrak{m}_e^{\{p^\nu\}}$ is the ideal generated by $(t^\lambda - 1)^{p^\nu} = t^{p^\nu \lambda} - 1$. So the kernel of ν-th Frobenius is $\operatorname{Spec} \mathbf{k}[\mathbb{X}/p^\nu \mathbb{X}]$. Hence $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$, as the linear dual of this, is the $\mathbf{k}$-valued functions on $\mathbb{X}/p^\nu\mathbb{X}$. In other words, it is the set of all $\mathbf{k}$-valued functions on $\mathbb{X}$ that are locally constant on every $p^\nu\mathbb{X}$-coset. This implies the following observation on the structure of $\mathcal{D}_{T/\mathbf{k}}$. Let $\widehat{\mathbb{Z}}_p$ denote the set of all p-adic integers equipped with the p-adic topology, and let $\mathbf{k}$ be viewed as a discrete topological space. Then we have

Proposition 3.2.1. *The ring $\mathcal{D}_{T/\mathbf{k}}$ is isomorphic to the ring of continuous functions on*

$\widehat{\mathbb{Z}}_p \otimes \mathbb{X}$ *with values in* $\mathbf{k}$.

Proof. Suppose σ, $\tau \in \mathcal{D}^{(\nu)}_{T/\mathbf{k}}$. Notice that under the comultiplication of $\mathbf{k}[T]$, $\Delta(t) = t \otimes t$. So we have

$$(\sigma\tau)(t^\lambda) = (\sigma \otimes \tau)(t^\lambda \otimes t^\lambda) = \sigma(t^\lambda)\tau(t^\lambda). \tag{3.2.1}$$

Hence the multiplication of $\mathcal{D}^{(\nu)}_{T/\mathbf{k}}$ can be identified with pointwise multiplication in the ring of functions on $\mathbb{X}/p^\nu\mathbb{X}$.

Let LC stand for locally constant and $\mathrm{LC}^\nu(\mathbb{X}, \mathbf{k})$ denote the ring of all functions on $\mathbb{X}$ that are locally constant on every $p^\nu\mathbb{X}$-coset. Then as rings, we have

$$\begin{aligned} \mathcal{D}_{T/\mathbf{k}} &= \varinjlim \mathcal{D}^{(\nu)}_{T/\mathbf{k}} \cong \varinjlim \mathrm{LC}^\nu(\mathbb{X}, \mathbf{k}) \\ &\cong \mathrm{LC}(\varprojlim \mathbb{X}/p^\nu\mathbb{X}, \mathbf{k}) = \mathrm{LC}(\widehat{\mathbb{Z}}_p \otimes \mathbb{X}, \mathbf{k}). \end{aligned} \tag{3.2.2}$$

To finish the proof, it suffices to show that under the given topology, locally constant functions on $\widehat{\mathbb{Z}}_p \otimes \mathbb{X}$ are exactly continuous functions. Since any p-adic coset is closed in $\widehat{\mathbb{Z}}_p \otimes \mathbb{X}$ and its complement is a finite union of same closed cosets, each coset is both open and closed. $\widehat{\mathbb{Z}}_p \otimes \mathbb{X}$ is a totally disconnected space. So given a locally constant function, since $\mathbf{k}$ is discrete, the inverse image of any subset of $\mathbf{k}$ is a union of p-adic cosets, which is open. Thus this function is continuous. Conversely for a continuous function, its preimage of any point must be open, thus it is a union of p-adic cosets. Hence the function is locally constant. □

The object $\widehat{\mathbb{Z}}_p \otimes \mathbb{X}$ is sometimes written as $\widehat{\mathbb{X}}_p$ for short, and called the *generalized weights* of T. More discussions on $\widehat{\mathbb{X}}_p$ can be found in [12] §2.

Back to $\mathcal{D}^{(\nu)}_{T/\mathbf{k}}$, we would like to find a convenient set of basis for later use. Apparently, just pick all the characteristic functions of cosets of $p^\nu\mathbb{X}$ would give a set of basis. Let $\delta^{(\nu)}_\lambda$ denote the characteristic function of $\lambda = \lambda_0 + p^\nu\mathbb{X}$, which takes value 1 on the coset of λ_0 and 0 on the others. The set of all functions $\delta^{(\nu)}_\lambda$ is linearly independent and certainly a basis for $\mathcal{D}^{(\nu)}_{T/\mathbf{k}}$. The following discussion aims to explicitly interpret $\delta^{(\nu)}_\lambda$ in terms of those

X's, **Y**'s, and **H**'s.

Let $\omega_1, \omega_2, \ldots, \omega_\ell$ be the fundamental dominant weights corresponding to our choice of roots. Then for any integral weight λ, there exist integers q_i, all non-negative or all non-positive, such that $\lambda = \sum_{i=1}^{\ell} q_i \omega_i$. Let $\alpha_1^\vee, \alpha_2^\vee, \ldots, \alpha_\ell^\vee$ denote the corresponding coroots in the sense that $\alpha_i^\vee(\omega_j) = \delta_{ij}$. They are $\mathbb{Z}$-valued functions on $\mathbb{X}$, the full weight lattice, such that $\alpha_i^\vee(\lambda) = q_i$. Write H_i for $\alpha_i^\vee$ and $H_i^{[n]}$ for the element of the linear dual of $\mathbf{k}[T]$ defined by

$$H_i^{[n]}(t^\lambda) = \binom{\alpha_i^\vee(\lambda)}{n}_p. \tag{3.2.3}$$

One can check that these notations are consistent with those we used in § 2.2, which is the case of $\ell = 1$.

We now would like to interpret the characteristic function $\delta_\lambda^{(\nu)}$ in terms of the H_i's and give another set of basis for $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$. Suppose $\lambda = \sum_{i=i}^{\ell} q_i \omega_i$. Consider the following expression

$$\delta = \prod_{i=1}^{\ell} \left(\sum_{j=0}^{p^\nu - 1} (-1)^j \binom{H_i - q_i}{j}_p \right). \tag{3.2.4}$$

We want to show that δ is equal to the characteristic function $\delta_\lambda^{(\nu)}$. It is convenient to introduce firstly the following computational properties of the binomial sum involved.

Lemma 3.2.2. *Let q be an integer, and $f(x)$ be a function on $\mathbb{Z}$ defined by*

$$f(x) = \sum_{j=0}^{p^\nu - 1} (-1)^j \binom{x-q}{j}_p,$$

then

1. *f depends only on the residue classes of x and q in $\mathbb{Z}/p^\nu\mathbb{Z}$;*

2. *$f(q) = 1$;*

3. *$f(x) = 0$ for any $x \neq q$.*

Proof. By the definition of p-binomial coefficient, (1) is clear since j is less than p^ν always. (2) is also straightforward since

$$f(q) = \sum_{j=0}^{p^\nu - 1} (-1)^j \binom{0}{j}_p = (-1)^0 \binom{0}{0} = 1. \tag{3.2.5}$$

To see (3), let $x \neq q$, then

$$f(x) = \sum_{j=0}^{p^\nu - 1} (-1)^j \binom{x-q}{j}_p = (1-1)^{x-q} = 0. \tag{3.2.6}$$

□

Proposition 3.2.3. $\delta = \delta_\lambda^{(\nu)}$.

Proof. For any $\eta \in \mathbb{X}$,

$$\begin{aligned} \delta(p^\nu \eta) &= \prod_{i=1}^{\ell} \left(\sum_{j=0}^{p^\nu - 1} (-1)^j \binom{p^\nu \alpha_i^\vee(\eta) - q_i}{j}_p \right) \\ &= \prod_{i=1}^{\ell} \left(\sum_{j=0}^{p^\nu - 1} (-1)^j \binom{p^\nu - q_i}{j}_p \right) \\ &= \prod_{i=1}^{\ell} (1-1)^{p^\nu - q_i} = 0. \end{aligned} \tag{3.2.7}$$

This shows that δ is constant on cosets of $p^\nu \mathbb{X}$, therefore is a well defined operator in $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$. Then by Lemma 3.2.2,

$$\delta(\lambda) = \prod_{i=1}^{\ell} \left(\sum_{j=0}^{p^\nu - 1} (-1)^j \binom{0}{j}_p \right) = 1, \tag{3.2.8}$$

and for any $\eta \neq \lambda$, without loss of generality, say $\alpha_1^\vee(\eta) \neq q_1$, then

$$\begin{aligned}\delta(\eta) &= \left(\sum_{j=0}^{p^\nu-1}(-1)^j\binom{\alpha_1^\vee(\eta)-q_i}{j}_p\right)\prod_{i=2}^{\ell}\left(\sum_{j=0}^{p^\nu-1}(-1)^j\binom{\alpha_1^\vee(\eta)-q_i}{j}_p\right)\\ &= (1-1)^{\alpha_1^\vee(\eta)-q_i}\prod_{i=2}^{\ell}\left(\sum_{j=0}^{p^\nu-1}(-1)^j\binom{\alpha_1^\vee(\eta)-q_i}{j}_p\right) = 0. \qquad (3.2.9)\end{aligned}$$

□

Hence δ is the characteristic function $\delta_\lambda^{(\nu)}$. Therefore

$$\begin{aligned}\delta_\lambda^{(\nu)} &= \prod_{i=1}^{\ell}\left(\sum_{j=0}^{p^\nu-1}(-1)^j\binom{H_i-q_i}{j}_p\right)\\ &= \prod_{i=1}^{\ell}\left(\sum_{j=0}^{p^\nu-1}(-1)^j\sum_{c_i=0}^{j}\binom{H_i}{c_i}_p\binom{-q_i}{j-c_i}_p\right)\\ &= \prod_{i=1}^{\ell}\left(\sum_{c_i=0}^{p^\nu-1}\sum_{j=c_i}^{p^\nu-1}(-1)^j\binom{H_i}{c_i}_p\binom{-q_i}{j-c_i}_p\right)\\ &= \sum_{c_1,c_2,\dots,c_\ell=0}^{p^\nu-1}\left(r_{c_1,c_2,\dots,c_\ell}\prod_{i=1}^{\ell}\binom{H_i}{c_i}_p\right), \qquad (3.2.10)\end{aligned}$$

where the constants

$$r_{c_1,c_2,\dots,c_\ell} = \prod_{i=1}^{\ell}\left(\sum_{j=0}^{p^\nu-1}(-1)^j\binom{-q_i}{j}_p\right). \qquad (3.2.11)$$

This shows that each characteristic function $\delta_\lambda^{(\nu)}$ is a linear combination of monomials $\binom{H_1}{c_1}\binom{H_2}{c_2}\cdots\binom{H_\ell}{c_\ell}$ with each $c_i < p^\nu$. Using vector notation, $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$ has a basis $\{\binom{\mathbf{H}}{\mathbf{c}}\}_{\mathbf{0}\leq\mathbf{b}<\mathbf{p}^\nu}$.

To put things together, we need one more observation. Let H and M be subgroups of G, and $H \cup M = \{e\}$. Suppose the map sending the pair (h, m) to $h \cdot m$ is étale at e, then there is an isomorphism of vector spaces $\mathcal{D}_{H/\mathbf{k}} \otimes \mathcal{D}_{M/\mathbf{k}} \cong \mathcal{D}_{G/\mathbf{k}}$. This is worked out in § 1.2 and § 1.3 of [12]. Hence we have

Proposition 3.2.4. *$\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$ has a $\mathbf{k}$-basis consisting of monomials of the form $\mathbf{X}(\mathbf{a})\binom{\mathbf{H}}{\mathbf{c}}\mathbf{Y}(\mathbf{b})$, where $\mathbf{0} \leq \mathbf{a}, \mathbf{b}, \mathbf{c} < \mathbf{p}^\nu$.* □

This shows that $\mathcal{D}_{G/\mathbf{k}}$ is isomorphic to the Kostant $\mathbb{Z}$-form over $\mathbf{k}$, reduced by p.

Chapter 4

Semisimple Center

As before, let $\mathbf{k}$ be an algebraically closed field of characteristic p, and G be an arbitrary affine group scheme over $\mathbf{k}$. We prove in the first section the existence of Jordan decomposition in the ring $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$. Jordan decomposition is important of the study of algebraic groups. Much literature can be found at [15], [16], [21], [24], and [30]. On the ring of invariant differential operators Jordan decomposition does not exist in characteristic 0. But in characteristic p, due to the finiteness of Frobenius kernels, we are able to generalize the Jordan decomposition to it. This suggests the concept of the semisimple center of the ring $\mathcal{D}_{G/\mathbf{k}}$ and its subalgebras $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$, which inspired our development of the characteristic p Harish-Chandra theory. This is a promising direction of research in representation theory, as interesting results appear immediately. We give in §4.2 a short elegant proof of a theorem on the semisimple center of $\mathcal{D}_{G/\mathbf{k}}$ when G is connected.

4.1 Existence of Jordan Decomposition

We shall say that an element $\sigma \in \mathcal{D}$ is *semisimple* (respectively *nilpotent*) if, under left multiplication, it acts semisimply (respectively nilpotently) on $\mathcal{D}$.

Proposition 4.1.1. *Let G be an affine group scheme over $\mathbf{k}$ and let $\sigma \in \mathcal{D}_{G/\mathbf{k}}$. Then:*

1. *there are polynomials, $f(x)$ and $g(x)$, so that $f(\sigma)$ is semisimple, $g(\sigma)$ is nilpotent and $\sigma = f(\sigma) + g(\sigma)$.*

2. *$f(\sigma) = \sigma_s$ and $g(\sigma) = \sigma_n$ are unique with respect to the properties that their sum is σ,*

that they commute and that σ_s acts semisimply on all representations and that σ_n is nilpotent.

3. *σ_s and σ_n are the semisimple and nilpotent parts of σ under right multiplication as well.*

Proof. Since $\mathcal{D} = \bigcup_{\nu \geq 0} \mathcal{D}^{(\nu)}$, there exists ν such that $\sigma \in \mathcal{D}^{(\nu)}$, which is a finite dimensional space. Let L_σ denote the left multiplication by σ. It is a linear map on $\mathcal{D}^{(\nu)}$, thus we have

$$L_\sigma = (L_\sigma)_s + (L_\sigma)_n, \tag{4.1.1}$$

the standard Jordan decomposition of L_σ, and there exist polynomials f and g such that

$$(L_\sigma)_s = f(L_\sigma) \tag{4.1.2}$$

and

$$(L_\sigma)_n = g(L_\sigma) \tag{4.1.3}$$

are the semisimple part and nilpotent part respectively. Let $\sigma_s = f(\sigma)$ and $\sigma_n = g(\sigma)$. Now we show that σ_s and σ_n give a decomposition of σ that satisfies the properties described in (1) and (2).

Let $\mathrm{Hom}_{-\mathcal{D}^{(\nu)}}(-,-)$ denote the functor of right $\mathcal{D}^{(\nu)}$-module maps. Then $\mathrm{Hom}_{-\mathcal{D}^{(\nu)}}(\mathcal{D}^{(\nu)}, \mathcal{D}^{(\nu)})$ contains L_δ for any $\delta \in \mathcal{D}^{(\nu)}$, and it is a left $\mathcal{D}^{(\nu)}$-module via action $(\delta \cdot \varphi)(\mu) = \delta\varphi(\mu)$, for any δ, $\mu \in \mathcal{D}^{(\nu)}$ and $\varphi \in \mathrm{Hom}_{-\mathcal{D}^{(\nu)}}(\mathcal{D}^{(\nu)}, \mathcal{D}^{(\nu)})$. Consider the map

$$\theta : \mathcal{D}^{(\nu)} \to \mathrm{Hom}_{-\mathcal{D}^{(\nu)}}(\mathcal{D}^{(\nu)}, \mathcal{D}^{(\nu)}) \tag{4.1.4}$$

sending $\sigma \in \mathcal{D}^{(\nu)}$ to L_σ. It is straightforward to check that θ is an isomorphism of left

$\mathcal{D}^{(\nu)}$-modules. Indeed, for δ, μ, and $\tau \in \mathcal{D}^{(\nu)}$,

$$\begin{aligned}\theta(\delta\mu)(\tau) &= L_{\delta\mu}(\tau) = \delta\mu\tau \\ &= \delta L_{\mu}(\tau) = \delta(\theta(\mu)(\tau)) \\ &= (\delta \cdot \theta(\mu))(\tau),\end{aligned} \tag{4.1.5}$$

and the map $\theta^{-1} : \varphi \mapsto \varphi(1)$ gives the inverse. Therefore we have

$$\begin{aligned}\sigma &= \theta^{-1}(L_\sigma) = \theta^{-1}(f(L_\sigma) + g(L_\sigma)) \\ &= f(\theta^{-1}(L_\sigma)) + g(\theta^{-1}(L_\sigma)) \\ &= f(\sigma) + g(\sigma) = \sigma_s + \sigma_n.\end{aligned} \tag{4.1.6}$$

It is clear that σ_n is nilpotent since $(L_\sigma)_n = \theta(\sigma_n)$ is nilpotent. To see that σ_s is semisimple, consider its minimal polynomial $m(x)$. Obviously $m(x)$ is also the minimal polynomial of $(L_\sigma)_s$. Recall that a linear transformation is semisimple if and only if its minimal polynomial has no multiple roots. Since $(L_\sigma)_s$ is semisimple, $m(x)$ has no multiple root. Thus σ_s is semisimple. The uniqueness properties stated in (2) can also be proved this way, using the isomorphism θ.

By now we have set up the Jordan decomposition for $\mathcal{D}^{(\nu)}$. Notice that σ_s (respectively σ_n) acts semisimply (respectively nilpotently) on every free left $\mathcal{D}^{(\nu)}$-module. Thus to show that they are in the same way acting on $\mathcal{D}$, it suffices to show that $\mathcal{D}$ is a free left $\mathcal{D}^{(\nu)}$-module for every ν. We prove this assertion in Lemma 4.1.2.

To see that the semisimple and nilpotent parts are the same for the right multiplication, let $\mathrm{Hom}_{\mathcal{D}^{(\nu)}-}(\mathcal{D}^{(\nu)}, \mathcal{D}^{(\nu)})$ be the set of all left $\mathcal{D}^{(\nu)}$-module maps from $\mathcal{D}^{(\nu)}$ to itself. Then it is a right $\mathcal{D}^{(\nu)}$-module and the map

$$\eta : \mathcal{D}^{(\nu)} \to \mathrm{Hom}_{\mathcal{D}^{(\nu)}-}(\mathcal{D}^{(\nu)}, \mathcal{D}^{(\nu)}) \tag{4.1.7}$$

that sending σ to R_σ is a right $\mathcal{D}^{(\nu)}$-module isomorphism, where R_σ is the right multiplication by σ. Decomposing R_σ inside $\mathcal{D}^{(\nu)}$ gives another pair of polynomials $f'(x)$ and $g'(x)$ such that $\sigma = f'(\sigma) + g'(\sigma)$ is also a Jordan decomposition of σ. Therefore by the uniqueness property we must have $f = f'$ and $g = g'$. □

To finish the proof of Proposition 4.1.1, we need the following lemma:

Lemma 4.1.2. *Under left multiplication, $\mathcal{D}$ is a free left $\mathcal{D}^{(\nu)}$-module for every non-negative integer ν.*

Proof. The proof of this assertion will be carried out in two steps. Given any ν fixed, we write $\mathcal{D} \cong \mathcal{D}^{(\nu)} \otimes M$ as $\mathbf{k}$-vector spaces, for some vector space M, and then show that the actions by $\mathcal{D}^{(\nu)}$ via left multiplication on both sides are the same, i.e, they are isomorphic as left $\mathcal{D}^{(\nu)}$-modules.

Let M be the subspace of $\mathcal{D}$ spanned by monomials $\mathbf{X}(p^\nu \mathbf{a})\binom{\mathbf{H}}{p^\nu \mathbf{c}}\mathbf{Y}(p^\nu \mathbf{b})$, where $p^\nu \mathbf{a}$ denote the tuple $(p^\nu a_m, \ldots, p^\nu a_1)$, and $p^\nu \mathbf{b}$ and $p^\nu \mathbf{c}$ are of the similar meaning in their own ways. Now we show that any monomial $\sigma = \mathbf{X}(\mathbf{a})\binom{\mathbf{H}}{\mathbf{c}}\mathbf{Y}(\mathbf{b}) \in \mathcal{D}$ can be written as a finite sum $\sum_i \sigma_i' \sigma_{\nu i}$ with σ_i''s in $\mathcal{D}^{(\nu)}$ and $\sigma_{\nu i}$'s in M. Therefore we can construct an isomorphism $\pi : \mathcal{D} \to \mathcal{D}^{(\nu)} \otimes M$ by setting $\pi(\sigma) = \sum_i \sigma_i' \otimes \sigma_{\nu i}$.

For $\mathbf{a} = (a_m, \ldots, a_1)$, define $|\mathbf{a}| = \sum_{i=1}^m a_i$. $|\mathbf{b}|$ and $|\mathbf{c}|$ are similarly defined. Define the degree of σ as $\deg(\sigma) = |\mathbf{a}| + |\mathbf{c}| + |\mathbf{b}|$, then $\sigma \in \mathcal{D}^{\{\deg(\sigma)\}}$. We prove the first step by inducing on $\deg(\sigma)$. Initial cases are obvious, since $\sigma \in \mathcal{D}^{(\nu)}$ when $\deg(\sigma) < p^\nu$. For a larger degree monomial, write $\mathbf{a} = \mathbf{a}' + p^\nu \mathbf{a}_\nu$, where $\mathbf{a}'$ is a tuple with entries are all less than p^ν. Write $\mathbf{b}$ and $\mathbf{c}$ in the same way. Note that under the $\mathcal{D}^{\{n\}}$ filtration, the associated graded algebra of $\mathcal{D}$ is commutative. That means we are allowed to rearrange symbols in the top degree terms only affecting lower degree terms. Hence

$$\begin{aligned}\sigma &= \mathbf{X}(\mathbf{a})\binom{\mathbf{H}}{\mathbf{c}}\mathbf{Y}(\mathbf{b}) \\ &= \mathbf{X}(\mathbf{a}')\binom{\mathbf{H}}{\mathbf{c}'}\mathbf{Y}(\mathbf{b}') \cdot \mathbf{X}(p^\nu \mathbf{a}_\nu)\binom{\mathbf{H}}{p^\nu \mathbf{c}_\nu}\mathbf{Y}(p^\nu \mathbf{b}_\nu) + f(\mathbf{X}, \mathbf{H}, \mathbf{Y}), \qquad (4.1.8)\end{aligned}$$

where f is a polynomial with $\deg(f) < \deg(\sigma)$. By the inductive hypotheses on each term of f, we have written σ in the desired form.

Now we show that π is an isomorphism of $\mathcal{D}^{(\nu)}$-modules. That is, for any $\delta \in \mathcal{D}^{(\nu)}$,

$$\pi(\delta\sigma) = (\delta \otimes 1).\pi(\sigma) = \sum_i \delta\sigma_i \otimes \sigma_{\nu i}. \tag{4.1.9}$$

Write $\pi(\sigma) = \sigma' \otimes \sigma_\nu + \pi(f)$, where $\sigma' = \mathbf{X}(\mathbf{a}')\binom{\mathbf{H}}{\mathbf{c}'}\mathbf{Y}(\mathbf{b}')$ and $\sigma_\nu = \mathbf{X}(p^\nu \mathbf{a}_\nu)$ $\binom{\mathbf{H}}{p^\nu \mathbf{c}_\nu}\mathbf{Y}(p^\nu \mathbf{b}_\nu)$. Then it suffices to show that

$$\pi(\delta\sigma) = \delta\sigma' \otimes \sigma_\nu + (\delta \otimes 1).\pi(f). \tag{4.1.10}$$

By inducing on $\deg(\sigma)$, we can assume the assertion is true for all the terms in f since $\deg(f) < \deg(\sigma)$. That is $\pi(\delta f) = (\delta \otimes 1).\pi(f)$. Hence it leaves to show that

$$\delta\sigma' \otimes \sigma_\nu = \pi(\delta\sigma) - \pi(\delta f) = \pi(\delta(\sigma - f)) = \pi(\delta\sigma'\sigma_\nu). \tag{4.1.11}$$

This is obvious because both δ and σ' are in $\mathcal{D}^{(\nu)}$, which is a subalgebra. $\square$

4.2 A Theorem on the Semisimple Center of $\mathcal{D}^{(\nu)}$

Definition 4.2.1. If A is a $\mathbf{k}$-algebra, the *semisimple center* of A, written $\mathcal{Z}_s(A)$, consists of those elements of the center of A which act semisimply on A via left multiplication.

Because the sum and product of commuting semisimple elements are semisimple, the semisimple center of an algebra is a subring of the center.

Recall the definition in §1.1 that an element μ of $\mathcal{D}$ is called invariant under the conjugating action if $\sigma \circ \mu = \varepsilon(\sigma)\mu$ for every $\sigma \in \mathcal{D}$.

Lemma 4.2.2. *An element of $\mathcal{D}$ is central if and only if it is fixed under the conjugating action $\circ$ of $\mathcal{D}$ on itself.*

Proof. The only-if part is trivial, since if $\mu \in \mathcal{D}$ is central, for any $\sigma \in \mathcal{D}$,

$$\sigma \circ \mu = \sum_i \sigma_i' \mu \mathbf{s}(\sigma_i'') = \sum_i \sigma_i' \mathbf{s}(\sigma_i'') \mu = \varepsilon(\sigma)\mu. \tag{4.2.1}$$

For the if part, let μ be an invariant of the conjugating action: $\sigma \circ \mu = \varepsilon(\sigma)\mu$ for any σ. For notation convenience let's suppose

$$(\mathrm{id} \otimes m^*)(m^*(\sigma)) = \sum \sigma_i' \otimes \sigma_i'' \otimes \sigma_i'''. \tag{4.2.2}$$

We then have

$$\begin{aligned} \sigma\mu &= \sum \sigma_i' \varepsilon(\sigma_i'')\mu = \sum \sigma_i' \mu \varepsilon(\sigma_i'') \\ &= \sum \sigma_i' \mu \mathbf{s}(\sigma_i'')\sigma_i''' = \sum (\sigma_i' \circ \mu)\sigma_i'' \\ &= \sum \varepsilon(\sigma_i')\mu\sigma_i'' = \sum \mu\varepsilon(\sigma_i')\sigma_i'' = \mu\sigma. \end{aligned} \tag{4.2.3}$$

This proves the lemma. □

Proposition 4.2.3. *If G is connected, then $\mathcal{Z}_s(\mathcal{D}) \cap \mathcal{D}^{(\nu)} = \mathcal{Z}_s(\mathcal{D}^{(\nu)})$, $\nu \geq 0$.*

Proof. It is clear that $\mathcal{Z}_s(\mathcal{D}) \cap \mathcal{D}^{(\nu)} \subseteq \mathcal{Z}_s(\mathcal{D}^{(\nu)})$. To establish the converse inclusion, consider the spectrum of the ring $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$. The commutative algebra $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ is finite dimensional since it is contained in $\mathcal{D}^{(\nu)}$. Therefore its spectrum $\mathrm{Spec}(\mathcal{Z}_s(\mathcal{D}^{(\nu)}))$ is of dimension 0 and every prime ideal in $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ is maximal. Since it contains only semisimple elements, the radical of $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ is trivial. By the Chinese Remainder Theorem, $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ is isomorphic to the product of finite many copies of $\mathbf{k}$. Therefore its spectrum is a finite discrete set of points.

Now consider the action of G on $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ by conjugation. It naturally induces an action on $\mathrm{Spec}(\mathcal{Z}_s(\mathcal{D}^{(\nu)}))$. This is an action of a connected algebraic group on a discrete reduced spectrum and it is hence trivial. That is, under the conjugating action, G acts trivially on the elements of $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$. Hence every element in $\mathcal{Z}_s(\mathcal{D}^{(\nu)})$ is $\mathcal{D}$-invariant under the conjugating action $\circ$. Now by Lemma 4.2.2 they are central in $\mathcal{D}$. This establishes the converse inclusion and proves the assertion. □

Propsition 4.2.3 implies that the semisimple center of $\mathcal{D}^{(\nu)}$ is contained in the semisimple center of $\mathcal{D}^{(\nu+1)}$, which is a very strong result. This inspires us to describe higher level semisimple centers in terms of the lower level ones, so that inductive methods could be applied.

4.3 Harish-Chandra Centers

In this section we review the knowledge of the Harish-Chandra centers, and aim to compare with the semisimple center we are studying.

Let $\mathfrak{g}$ be the Lie algebra of G and let $U(\mathfrak{g})$ be the universal enveloping algebra over $\mathfrak{g}$. When the field $\mathbf{k}$ is of prime characteristic, $\mathfrak{g}$ has the restricted Lie algebra structure with the "p-th power operation" $x^{[p]}$ on each element x. One can easily check that for any $x \in \mathfrak{g}$, $x^p - x^{[p]} \in U(\mathfrak{g})$ is in the center of $U(\mathfrak{g})$, where x^p is the tensor product of p x's in $U(\mathfrak{g})$. The map sending x to $x^p - x^{[p]}$ is p-linear ([2]) and the image is called the *Frobenius center*. Let's denote it by $\mathcal{Z}_{\mathrm{Fr}}$. As we have proved in Lemma 4.2.2, the set of all $\mathrm{ad}(G)$-invariant in $U(\mathfrak{g})$ is also contained in the center of $U(\mathfrak{g})$ and is called the *Harish-Chandra center*, denoted by $\mathcal{Z}_{\mathrm{HC}}$. Standard facts about the Harish-Chandra center can be found in [7] and [23]. In particular, the following proposition about the center of $U(\mathfrak{g})$ is proved in [23].

Proposition 4.3.1. *The center of $U(\mathfrak{g})$ is generated by $\mathcal{Z}_{\mathrm{Fr}}$ and $\mathcal{Z}_{\mathrm{HC}}$.* □

Consider the natural inclusion $\mathfrak{g} \hookrightarrow \mathcal{D}_{G/\mathbf{k}}$. It induces a map $\phi : U(\mathfrak{g}) \to \mathcal{D}_{G/\mathbf{k}}$. The image of this map is $\mathcal{D}^{(1)}_{G/\mathbf{k}}$, which is isomorphic to the restricted enveloping algebra over $\mathfrak{g}$. So ϕ is the map of $U(\mathfrak{g})$ to its quotient modulo the ideal generated by $\mathcal{Z}^+_{\mathrm{Fr}}$, where $\mathcal{Z}^+_{\mathrm{Fr}}$ is the ideal of polynomials in $\mathcal{Z}_{\mathrm{Fr}}$ with no constant term. This map sends the Harish-Chandra center $\mathcal{Z}_{\mathrm{HC}}$

into the center of $\mathcal{D}^{(1)}_{G/\mathbf{k}}$. Some natural questions can be asked from here, such as does the image of $\mathcal{Z}_{\mathrm{HC}}$ under ϕ lie in the semisimple center $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}})$? Or conversely does $\mathcal{Z}_s(\mathcal{D}_{G/\mathbf{k}})$ lie in $\phi(\mathcal{Z}_{\mathrm{HC}})$? We will answer these questions in Section 6.2.

Chapter 5

Verma Modules

In this chapter we review the knowledge of Verma modules over a semisimple algebraic group G in positive characteristic, and give the necessary and sufficient condition for certain integral weights to be maximal.

5.1 Introduction to Verma Modules

In representation theory, there are at least three standard methods of constructing an irreducible representation having a given dominant integral weight, namely Verma modules, Weyl modules, and the Borel-Weil theory. In this section we review the Verma module approach. Given any λ in $\widehat{\mathbb{X}}$, we can construct a representation $Z(\lambda)$ called a Verma module. It is named after Daya-Nand Verma, who explored these modules in detail ([31]), followed by more recent works by Bernstein, Gel'fand, Gel'fand ([3], [4], [5]), and Dixmier ([10]). In fact, λ can be any element of $\widehat{\mathbb{X}}$, not necessarily dominant or integral. Note that the Verma module $Z(\lambda)$ is always infinite dimensional, even if λ is dominant integral. But it eventually turns out that if λ is dominant integral, then $Z(\lambda)$ contains an invariant subspace $V(\lambda)$ such that the quotient space $Z(\lambda)/V(\lambda)$ is finite dimensional irreducible and has highest weight λ.

There are a number of different but equivalent ways to construct a Verma module ([13], §7.3.1, [15], §20.3, and [11]). Following Humphrey's induced module construction, let $\mathbf{k}_\lambda$ be the one dimensional module spanned by the maximal vector of weight λ. Then the Verma module $Z(\lambda)$ over G of highest weight λ can be constructed as $\mathcal{D}_{G/\mathbf{k}} \otimes_{\mathcal{D}_{B/\mathbf{k}}} \mathbf{k}_\lambda$. In characteristic 0, this is nothing but $U(\mathfrak{g}) \otimes_{U(\mathfrak{b})} \mathbf{k}_\lambda$. Here $\mathfrak{b}$ is the Lie algebra of the preselected Borel subgroup B, and $U(-)$ means the universal enveloping algebra.

Given λ dominant integral, the next question is to find submodules inside $Z(\lambda)$ that can play the role of $V(\lambda)$. This amouts to find those weights occurring in $Z(\lambda)$ that are vanished under the action of all the elements of $\mathcal{D}_{U+/\mathbf{k}}$, or in terms of the basis constructed in Chapter 1, the $X_\alpha^{[p^\nu]}$'s. In characteristic 0, the answer to this question is well-known and straightforward ([13], Proposition 7.23), but in characteristic p it is much more subtle. We give a simple result of this question in the next section.

5.2 Submodules of a Verma Module

The Verma module $Z(\lambda)$ over G of highest weight λ is the module $\mathcal{D}_{G/\mathbf{k}} \otimes_{\mathcal{D}_{B/\mathbf{k}}} \mathbf{k}_\lambda$, where $\mathbf{k}_\lambda$ is the one dimensional module with action given by the character. Then $\Pi(Z(\lambda))$, the weights occur in $Z(\lambda)$, consists of weights of the form $\lambda - \sum_{i=1}^{l} k_i\alpha_i$, $k_i \in \mathbb{Z}^+$. Let v_λ be a maximal vector of weight λ, and α_i a fixed simple root. Let ρ denote the half sum of all positive roots. Then note that $\alpha_i^\vee(\lambda+\rho) = \alpha_i^\vee(\lambda) + 1$. Write $\alpha_i^\vee(\lambda+\rho)$ p-adically as $\sum_{\nu \geq 0} a_\nu p^\nu$, where $0 \leq a_\nu \leq p-1$ are integers depend on λ and i. Consider $Y_{\alpha_i}^{[t]}.v_\lambda$, a vector of weight $\lambda - t\alpha_i$, $t \geq 0$. We have the following.

Proposition 5.2.1. *1. $Y_{\alpha_i}^{[t]}.v_\lambda$ is a maximal vector if and only if $t = \sum_{\nu=0}^{n} a_\nu p^\nu$ for some $n \geq 0$, i.e., $\alpha_i^\vee(\lambda+\rho) - t \equiv 0 \mod p^{n+1}$.*

2. $Z(\lambda)$ contains a submodule of weight μ such that $\alpha_i^\vee(\mu+\rho)$ has p-adic expansion $\sum_{\nu=0}^{n}(-a_\nu)p^\nu + \sum_{\nu \geq n+1} a_\nu p^\nu$.

Proof. (1) It suffices to show that $Y_{\alpha_i}^{[t]}.v_\lambda$ is killed by all $X_{\alpha_j}^{[p^\nu]}$ for all $\alpha_j \in \Delta$ and $\nu \geq 0$. If $j \neq i$, we already have $X_{\alpha_j}^{[p^\nu]} Y_{\alpha_i}^{[t]}.v_\lambda = 0$ for any ν since $X_{\alpha_j^{[p^\nu]}}$ commutes with $Y_{\alpha_i^{[t]}}$. When

$j=i$, white X_{α_i} and Y_{α_i} as X and Y for short, recall the commutation formula

$$X^{[s]}Y^{[t]} = \sum_{k=0}^{\min(s,\ t)} Y^{[t-k]}\binom{H-s-t+2k}{k}_p X^{[s-k]}. \tag{5.2.1}$$

Then for a fixed n we have

$$X^{[p^n]}Y^{[t]}.v_\lambda = \sum_{k=0}^{\min(p^n,\ t)} Y^{[t-k]}\binom{H-p^n-t+2k}{k}_p X^{[p^n-k]}.v_\lambda \tag{5.2.2}$$

The right hand side is obviously 0 for those n such that $p^n > t$. For $p^n \leq t$,

$$\begin{aligned} X^{[p^n]}Y^{[t]}.v_\lambda &= \sum_{k=0}^{p^n} Y^{[t-k]}\binom{H-p^n-t+2k}{k}_p X^{[p^n-k]}.v_\lambda \\ &= Y^{[t-p^n]}\binom{H+p^n-t}{p^n}_p .v_\lambda \\ &= \binom{\alpha_i^\vee(\lambda)+p^n-t}{p^n}_p Y^{[t-p^n]}.v_\lambda \end{aligned} \tag{5.2.3}$$

In order for this vector to be 0, the scalar $\binom{\alpha_i^\vee(\lambda)+p^n-t}{p^n}_p$ must be 0 in $\mathbf{k}$. Now if $t=\sum_{\nu=0}^{n} a_\nu p^\nu$, we have

$$\begin{aligned} \binom{\alpha_i^\vee(\lambda)+p^n-t}{p^n}_p &= \binom{p^n-1+\sum_{\nu\geq n+1} a_\nu p^\nu}{p^n}_p \\ &= \binom{p^n-1}{0}_p \binom{0}{1}\binom{\sum_{\nu\geq n+1} a_\nu p^\nu}{0}_p \\ &= 0 \end{aligned} \tag{5.2.4}$$

Supposed t is not a p-adic truncation of $\alpha_i^\vee(\lambda+\rho)$, then t is not of the form $\sum_{\nu=0}^{n} a_\nu p^\nu$ for any n. We now show that there exists a number k such that $\binom{\alpha_i^\vee(\lambda)+p^k-t}{p^k} \neq 0$. Write t p-adically as $\sum_{\nu\geq 0} t_\nu p^\nu$, and let k be the smallest number such that $a_k \neq t_k$. Without loss of generality, we can assume that $a_k > t_k$. Then

$$\begin{aligned}\binom{\alpha_i^\vee(\lambda)+p^k-t}{p^k}_p &= \binom{p^k-1+(a_k-t_k)p^k+\sum_{\nu\geq n+1}(a_\nu-t_\nu)p^\nu}{p^k}_p \\ &= \binom{p^k-1}{0}_p\binom{a_k-t_k}{1}\binom{\sum_{\nu\geq n+1}(a_\nu-t_\nu)p^\nu}{0}_p \\ &= a_k-t_k \neq 0 \end{aligned} \tag{5.2.5}$$

This proves (1). To see the assertion in (2), let $\mu = \lambda - t\alpha_i$ and apply $\alpha_i^\vee$ to $\mu+\rho$.

$$\begin{aligned}\alpha_i^\vee(\mu+\rho) &= \alpha_i^\vee(\lambda - t\alpha_i+\rho) \\ &= \alpha_i^\vee(\lambda+\rho)-2t \\ &= \sum_{\nu=0}^{n}(-a_\nu)p^\nu + \sum_{\nu\geq n+1} a_\nu p^\nu \end{aligned} \tag{5.2.6}$$

This finishes the proof of proposition. □

Chapter 6

Integrals and Infinitesimal Verma Modules

In this Chapter, assumptions are the same as in Chapter 5. The field $\mathbf{k}$ is algebraically closed and of characteristic p. Let G be a split semisimple, connected and simply-connected group scheme over $\mathbf{k}$. In the first section we will review the notion of integral of a Hopf algebra, introduced by Sweedler ([28]). We will then introduce the integrals of $\mathcal{D}^{(\nu)}$, which were calculated by Haboush in [12].

In the two sections that follow, we give each an application of integrals. In section 6.2 we answer the questions arised from the end of Chapter 4 by constructing particular central operators using integrals. In the last section, we introduce the induced module of $G^{(\nu)}$ by $B^{(\nu)}$. Those induced by the one dimensional module associated with a weight λ are called infinitesimal Verma modules, or "baby Verma modules" in some literature. We will use the integral of $\mathcal{D}^{(\nu)}_{U^+/\mathbf{k}}$ and the characteristic functions defined in section 1.4 to show that every infinitesimal Verma module over $\mathcal{D}^{(\nu)}$ is isomorphic to a left ideal of $\mathcal{D}^{(\nu)}$.

6.1 Integral of a Hopf Algebra

Let H be a finite dimensional augmented Hopf algebra over $\mathbf{k}$ with antipode. Recall that in this case H^*, its linear dual is also a Hopf algebra, and there is the "transpose module structure" on H^*, making H^* a right H-module. Namely if $\sigma \in H^*$, $f \in H$, one can define $\sigma.f$ by the equation

$$\langle \sigma.f \ , \ f' \rangle = \langle \sigma \ , \ ff' \rangle, \tag{6.1.1}$$

where $\langle \ , \ \rangle$ is the natural pairing between H and H^*.

Definition 6.1.1. Let H be a finite dimensional Hopf algebra over $\mathbf{k}$. An element $\omega \in H$ is called a *right integral* if for each $\sigma \in H^+$ (the augmentation ideal), $\omega\sigma = 0$. It will be called a *left integral* if $\sigma\omega = 0$ and a *two-sided integral* if it is both a left and right integral.

Theorem 6.1.2. *(Sweedler-Larson) Let H be a finite dimensional Hopf algebra over $\mathbf{k}$. Then*

1. *H^* contains a right integral ω, and any other right integral is a constant multiple of ω.*

2. *H^* is a free rank one H-module under the transpose module structure with ω as basis.*

A detailed proof of this theorem is presented in [28]. Notice that $\mathbf{k}[G^{(\nu)}]$ is a finite dimensional augmented Hopf algebra with antipode for every ν. Therefore by Sweedler's theorem, $\mathcal{D}^{(\nu)}$ contains a right integral. Recall the boldface notation for tuples we used in Chapter 1 and 2. Define operators

$$\Delta^{(\nu)} = \sum_{\mathbf{r} \leq \mathbf{p}^\nu - \mathbf{1}} (-1)^{|\mathbf{r}|} \binom{\mathbf{H}}{\mathbf{r}}, \tag{6.1.2}$$

and for any $\chi \in \mathbb{X}(\mathbb{T})$,

$$\Delta^{(\nu)}_\chi = \sum_{\mathbf{r} \leq \mathbf{p}^\nu - \mathbf{1}} (-1)^{|\mathbf{r}|} \binom{\mathbf{H} - \chi(\mathbf{H})}{\mathbf{r}}. \tag{6.1.3}$$

Also define

$$\omega^{(\nu)} = \mathbf{Y}(\mathbf{p}^\nu - \mathbf{1}) \Delta^{(\nu)}_{-2(p^\nu - 1)\rho} \mathbf{X}(\mathbf{p}^\nu - \mathbf{1}), \tag{6.1.4}$$

where ρ is again the half sum of all positive roots. Let U^+ be the unipotent radical of G corresponds to the choice of T. Then we have the following theorem.

Theorem 6.1.3. *(Haboush)*

1. *$\Delta^{(\nu)}$ is a two-sided integral of $\mathcal{D}^{(\nu)}_{T/\mathbf{k}}$.*

2. *$\mathbf{X}(\mathbf{p}^\nu - \mathbf{1})$ is a two-sided integral of $\mathcal{D}^{(\nu)}_{U+/\mathbf{k}}$.*

3. $\omega^{(\nu)}$ *is a two-sided integral of* $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$.

Proofs of these assertions and many more properties of $\omega^{(\nu)}$ can be found in [12].

6.2 Central Operator Constructions

In this section we will see that the two inclusion considered at the end of Chapter 4 are both false. For the first question, integrals provide natural counterexamples as follows.

Proposition 6.2.1. *The integrals* $\omega^{(\nu)}$ *are* $\mathrm{ad}(G)$*-invariant operators.* □

This assertion is proved in [12] as Corollary 6.9. Take $\mathrm{SL}(2,\mathbf{k})$ as example. Let α be the only positive root. We have $\omega^{(1)}$ defined as

$$Y_\alpha^{[p-1]}\Delta^{(1)}_{-(p-1)\alpha}X_\alpha^{[p-1]}.$$

It is in the image of the Harish-Chandra center under the quotient map, but obviously not semisimple, since it is nilpotent by definition.

To give a counterexample of the second statement, we need a semisimple central operator that is not in $\mathcal{D}^{(1)}_{G/\mathbf{k}}$. Before trying to construct this operator directly, an observation is in order. Let $S(\nu)$ denote the set of dominant weights of G which can be written in the form $\lambda = \sum_{i=1}^{\ell} a_i\omega_i$ where ω_i are the fundamental dominant weights and the a_i are intergers such that $0 \le a_i \le p^\nu - 1$. If $\lambda \in S(\nu)$, then $\lambda = \lambda_0 + p\lambda_1 + p^2\lambda_2 + \cdots + p^{\nu-1}\lambda_{\nu-1}$ with each $\lambda_i \in S(1)$. Then the Steinberg Tensor Product Theorem ([26]) asserts that there is the following isomorphism

$$I_\lambda \cong I_{\lambda_0} \otimes I_{\lambda_1}^{[p]} \otimes I_{\lambda_2}^{[p^2]} \otimes \cdots \otimes I_{\lambda_{\nu-1}}^{[p^{\nu-1}]}, \tag{6.2.1}$$

where I_λ denote the irreducible representation of highest weight λ, and $I_{\lambda_i}^{[p]}$ is the Frobenius twist module of I_{λ_i}. If r is any natural number, then for any fixed ν, r can be written uniquely as $r_0 + p^\nu r_1$ where $0 \le r_0 < p^\nu$ and r_1 is nonnegative. Then $\binom{H}{r} = \binom{H}{r_0}\binom{H}{p^\nu r_1}$. Now

$\binom{H}{r_0}$, being an element of $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$, acts on the tensor product $I_{\lambda_0} \otimes I_{p^\nu \lambda_1}$ strictly through its action on I_{λ_0}. In particular, any element of $\mathcal{D}^{(1)}_{G/\mathbf{k}}$ acts on $I_{p^\nu \lambda}$ as 0 provided that $\nu > 1$. In another words, an $\mathcal{D}^{(1)}_{G/\mathbf{k}}$ element would see no difference between the two weights $\lambda_0 \otimes \lambda_1^{[p]}$ and $\lambda_0 \otimes {\lambda'_1}^{[p]}$ with $\lambda_0 \in S(1)$ and $\lambda_1 \neq \lambda'_1$.

Therefore, it suffices to construct a semisimple central operator that acts on $I_{\lambda_0 \otimes \lambda_1^{[p]}}$ and $I_{\lambda_0 \otimes {\lambda'_1}^{[p]}}$ as different scalars for some choices of λ_0, λ_1 and λ'_1. According to the Jordan decomposition we have constructed before, a central operator and its semisimple part behave as exactly the same scalars when acting on irreducibles. Hence it suffices to find a central operator that provides the above property. Then its semisimple part would just be the counterexample we need. Such a central operator can be constructed as follows.

Let $A_{(\nu)} = \mathbf{k}[G]/\mathfrak{m}_e^{\{\nu\}}$, where $\mathfrak{m}_e^{\{\nu\}}$ is the ideal generated by the p-th power of elements of $\mathfrak{m}_e$. Recall that this is the algebra of the Frobenius twisted group scheme $G^{(\nu)}$ in § 3.1. It is also isomorphic to the linear dual of $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$. Write $\mathcal{Z}^{(\nu)}$ for $\mathcal{Z}(\mathcal{D}_{G/\mathbf{k}}) \cap \mathcal{D}^{(\nu)}_{G/\mathbf{k}}$. Note that this is not the center of $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$, but it is the set of ad(G)-invariants in $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$. Suppose $\sigma \in \mathcal{D}^{(\nu)}_{G/\mathbf{k}}$, then by Theorem 6.1.2 there is a unique $\bar{f} \in A_{(\nu)}$ such that $\sigma = \omega^{(\nu)}.\bar{f}$. It is proved in [12] Lemma 7.5 that if σ is in $\mathcal{Z}^{(\nu)}$, then $\bar{f}$ is an ad(G)-invariant in $A_{(\nu)}$. We call this $\bar{f}$ the function associated to σ in $\mathcal{D}^{(\nu)}_{G/\mathbf{k}}$.

One more definition is necessary. Let λ be any dominant integral weight. Then let $\mathcal{T}_\lambda$ denote the character function associated to I_λ. That is, if $g \in G(\mathbf{k})$, $\mathcal{T}_\lambda$ is defined by $\mathcal{T}_\lambda(g) = \mathrm{tr}_{I_\lambda}(g)$.

The most useful case of $\mathcal{T}_\lambda$ is that when λ is congruent to a Steinberg weight mod $p^\nu \widehat{\mathbb{X}}$. Recall that the ν-th Steinberg weight is defined as $(p^\nu - 1)\rho$, where ρ is the half sum of all positive roots. Let γ_ν denote the ν-th Steinberg weight, then the follow theorem is proved in [12] as Theorem 8.2.

Theorem 6.2.2. *Let $E^{(\nu)} = \omega^{(\nu)}.\mathcal{T}_{\gamma_\nu}$. Then there is a constant $c \neq 0$, such that*

$$E^{(\nu)}(\lambda) = \begin{cases} c & \text{if } \lambda - \gamma_\nu \in p^\nu \widehat{\mathbb{X}} \\ 0 & \text{otherwise} \end{cases}$$

□

Now we are ready to provide the counterexample. Consider $\gamma_1 = (p-1)\rho$, the first order Steinberg weight. Then $I_{\gamma_2} \cong I_{\gamma_1} \otimes I_{\gamma_1}^{[p]}$. Let $V = I_{\gamma_1} \otimes I_\sigma^{[p]}$, where σ is anything other than γ_1. Then we have $E^{(2)}$ acts on I_{γ_2} as a non-zero scalar and on V as 0. But as we discussed before, any operator in $\mathcal{D}^{(1)}_{G/\mathbf{k}}$ will act on I_{γ_2} and V in the same way as it acts on I_{γ_1}. This shows that $E^{(2)}$ is not in $\mathcal{D}^{(1)}_{G/\mathbf{k}}$. Since the trace function is ad(G)-invariant, $E^{(2)}$ is central. Hence its semisimple part gives an operator that is in the semisimple center of $\mathcal{D}_{G/\mathbf{k}}$ but not in $\mathcal{D}^{(1)}_{G/\mathbf{k}}$. Obviously any higher order $E^{(\nu)}$ can also do the same job.

6.3 Infinitesimal Verma Modules

Consider the isomorphism of schemes

$$U^{(\nu)+} \times B^{(\nu)} \xrightarrow{\sim} G^{(\nu)} \tag{6.3.1}$$

given by multiplication, which is compatible with the action of $U^{(\nu)+}$ by left multiplication and with the action of $B^{(\nu)}$ by right multiplication. So the isomorphisms of vector spaces

$$\mathbf{k}[G^{(\nu)}] \xrightarrow{\sim} \mathbf{k}[U^{(\nu)+}] \otimes \mathbf{k}[B^{(\nu)}] \tag{6.3.2}$$

and

$$\mathcal{D}^{(\nu)}_{U^+/\mathbf{k}} \otimes \mathcal{D}^{(\nu)}_{B/\mathbf{k}} \xrightarrow{\sim} \mathcal{D}^{(\nu)}_{G/\mathbf{k}} \tag{6.3.3}$$

are also compatible with the representations of $U^{(\nu)+}$ induced by these actions.

We have for any $B^{(\nu)}$-module M

$$\operatorname{coind}_{B^{(\nu)}}^{G^{(\nu)}} M = (\mathbf{k}[G^{(\nu)}] \otimes M)^{B^{(\nu)}} \cong \mathbf{k}[U^{(\nu)+}] \otimes (\mathbf{k}[B^{(\nu)}] \otimes M)^{B^{(\nu)}}, \tag{6.3.4}$$

and similarly,

$$\operatorname{ind}_{B^{(\nu)}}^{G^{(\nu)}} M = \mathcal{D}_{G/\mathbf{k}}^{(\nu)} \otimes_{\mathcal{D}_{B/\mathbf{k}}^{(\nu)}} M \cong \mathcal{D}_{U^+/\mathbf{k}}^{(\nu)} \otimes \mathcal{D}_{B/\mathbf{k}}^{(\nu)} \otimes_{\mathcal{D}_{B/\mathbf{k}}^{(\nu)}} M, \tag{6.3.5}$$

therefore

$$\operatorname{ind}_{B^{(\nu)}}^{G^{(\nu)}} M \cong \mathcal{D}_{U^+/\mathbf{k}}^{(\nu)} \otimes M.$$

We will focus on the induced module in this article. Notice that

$$\dim \mathbf{k}[U^{(\nu)}] = p^{\nu \dim U} = p^{r|\Phi^+|}. \tag{6.3.6}$$

This is also the dimension of $\mathbf{k}[U^{(\nu)+}]$, $\mathcal{D}_{U/\mathbf{k}}^{(\nu)}$, and $\mathcal{D}_{U^+/\mathbf{k}}^{(\nu)}$. So all the induced modules have dimension equal to

$$p^{r|\Phi^+|} \dim M. \tag{6.3.7}$$

Recall that any $\lambda \in \mathbb{X}(T)$ defines by restriction a character of $T^{(\nu)}$, which we again denote by λ. By extending its restriction to $T^{(\nu)}$ trivially on $U^{(\nu)}$ or $U^{(\nu)+}$, any $\lambda \in \mathbb{X}(T)$ defines a one dimensional module, denoted by $\mathbf{k}_\lambda$ for $B^{(\nu)}$ and $B^{(\nu)+}$. We can induce this module to $G^{(\nu)}$ and for simplicity denoted by

$$Z_\nu(\lambda) = \operatorname{ind}_{B^{(\nu)}}^{G^{(\nu)}} \mathbf{k}_\lambda. \tag{6.3.8}$$

Here our notation follows Jantzen in [19]. Also a number of useful observations on $Z_\nu(\lambda)$ can be found in II, 3.7 of this book. We quote one of them that to be used later in our proof.

Lemma 6.3.1. $Z_\nu(\lambda)^* \simeq Z_\nu(2(p^\nu - 1)\rho - \lambda)$. □

Recall that the integral of $\mathcal{D}_{U^+/\mathbf{k}}^{(\nu)}$ is $\mathbf{X}(\mathbf{p}^\nu - \mathbf{1})$. Let's denote this integral by ω_ν. Let

$\delta_\lambda^{(\nu)}$ be the characteristic function of the weight λ. Notice that if f is any element of $\mathcal{D}_{T/\mathbf{k}}^{(\nu)}$ viewed as a function on $\mathbb{X}/p^\nu\mathbb{X}$, then $f\delta_\lambda^{(\nu)} = f(\lambda)\delta_\lambda^{(\nu)}$. Consider the element $\delta_\lambda^{(\nu)}\omega_\nu$ in $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$. It generate two modules $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}\delta_\lambda^{(\nu)}\omega_\nu$ and $\delta_\lambda^{(\nu)}\omega_\nu\mathcal{D}_{G/\mathbf{k}}^{(\nu)}$. These are all viewed as left modules, the first via the natural left multiplication the second one via $\sigma \cdot u = u(s)(\sigma)$.

Proposition 6.3.2. *For any* $\lambda \in \mathbb{X}/p^\nu\mathbb{X}$,

1. $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}\delta_\lambda^{(\nu)}\omega_\nu \simeq Z_\nu(\lambda)$,
2. $\delta_\lambda^{(\nu)}\omega_\nu\mathcal{D}_{G/\mathbf{k}}^{(\nu)} \simeq Z_\nu(2(p^\nu - 1)\rho - \lambda) \simeq Z_\nu(\lambda)^*$.

Proof. To prove (1) notice that all elements, $\mathbf{X}(\mathbf{a})$, annihilate $\delta_\lambda^{(\nu)}\omega_\nu$. This is simply because

$$\mathbf{X}(\mathbf{a})\delta_\lambda^{(\nu)}\omega_\nu = h\mathbf{X}(\mathbf{a})\omega_\nu \tag{6.3.9}$$

for some element $h \in \mathcal{D}_{T/\mathbf{k}}^{(\nu)}$ and ω_ν annihilates the augmentation ideal of $\mathcal{D}_{U^+/\mathbf{k}}^{(\nu)}$. Now multiplying by $\mathbf{Y}(\mathbf{b})f$ for $f \in \mathcal{D}_{T/\mathbf{k}}^{(\nu)}$ yields

$$\mathbf{Y}(\mathbf{b})f\delta_\lambda^{(\nu)}\omega_\nu = f(\lambda)\mathbf{Y}(\mathbf{b})\delta_\lambda^{(\nu)}\omega_\nu. \tag{6.3.10}$$

Since $\delta_\lambda^{(\nu)}\omega_\nu$ is in $\mathcal{D}_{B+/\mathbf{k}}^{(\nu)}$, the elements, $\mathbf{Y}(\mathbf{b})\delta_\lambda^{(\nu)}\omega_\nu$, are all linearly independent. Hence the module $\mathcal{D}_{G/\mathbf{k}}^{(\nu)}\delta_\lambda^{(\nu)}\omega_\nu$ has highest weight λ and exactly the same lower weights of $Z_\nu(\lambda)$. Thus (1) follows.

Now notice that the total weight of $\mathbf{X}(\mathbf{p}^\nu - \mathbf{1})$ is $2(p^\nu - 1)\rho$. Hence,

$$\delta_\lambda^{(\nu)}\omega_\nu = \omega_\nu\delta_{\lambda-2(p^\nu-1)\rho}^{(\nu)}. \tag{6.3.11}$$

Combining this with the fact that the left structure on this module makes use of the involution and reasoning exactly as in the proof of (1) yields (2). □

References

[1] H. H. Andersen, J. C. Jantzen, W. Soergel, *Representations of quantum groups at a pth root of unity and of semisimple groups in characteristic p: independence of p*. Astérisque No. **220** (1994).

[2] A. Borel, *Linear algebraic groups. Second edition*, Graduate Texts in Mathematics, **126**. Springer-Verlag, New York, 1991.

[3] I. N. Bernstein, I. M. Gel'fand, S. I. Gel'fand, *Structure of representations generated by vectors of highest weight*, Funkcional. Anal. i Prilozen. **5**, no. 1, 1-9(1971).

[4] I. N. Bernstein, I. M. Gel'fand, S. I. Gel'fand, *Differential operators on the base affine space and a study of $\mathfrak{g}$-modules*, pp. 21-64 in: Lie Groups and their Representations, ed. I. M. Gel'fand, New York: Halsted, 1975.

[5] I. N. Bernstein, I. M. Gel'fand, S. I. Gel'fand, *A category of $\mathfrak{g}$-modules*, Funkcional. Anal. i Prilozen. **10**, no. 2, 1-8(1976).

[6] R. Bezrukavnikov, I. Mirkovic, *Representations of semisimple Lie algebras in prime characteristic and the noncommutative Springer resolution*, Ann. of Math. (2) 178 (2013), no. **3**, 835919.

[7] R. Bezrukavnikov, I. Mirkovic, D. Rumynin, *Localization of modules for a semisimple Lie algebra in prime characteristic*. arXiv preprint math/0205144 (2002).

[8] V. Carstensen, K. Erdmann, *On characteristic p Verma modules and subalgebras of the hyperalgebra*, DPhil. University of Oxford, 1994.

[9] M. Demazure, P. Gabriel, *Groupes Algebriques*, Tome I, North Holland Publishing Co., Amsterdam 1970.

[10] J. Dixmier, *Algebres Enveloppants*, Paris: Cauthier-Villars, 1974; English translation, *Enveloping Algebras*, Amsterdam: North-Holland, 1977.

[11] J. Franklin, *Homomorphisms between Verma modules in characteristic p*, Journal of Algebra, Volume **112**, Issue 1, January 1988, Pages 58-85.

[12] W. J. Haboush, *Central differential operators of split semisimple groups over filed of positive characteristic*, In: Sminaire dAlgbre Paul Dubreil et Marie-Paule Malliavin, Springer Lecture Notes in Mathematics **795**, pp 35-85.

[13] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, Graduate Texts in Mathematics, **222** (2nd ed.), Springer, 2015.

[14] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, **52**, Springer- Verlag, New York-Heidelberg, 1977.

[15] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics, **9**, Springer, 1972.

[16] J. E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, **21**, Springer-Verlag, New York-Heidelberg, 1975.

[17] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, **73**, Springer-Verlag, New York-Berlin, 1980.

[18] J. C. Jantzen, *Uber das Dekompositionsverhalten gewisser modularer Darstellungen hal beinfacher Gruppen und ihrer Lie-Algebren*, (German) J. Algebra **49** (1977).

[19] J. C. Jantzen, *Representations of algebraic groups*. Second edition, Mathematical Surveys and Monographs, **107** American Mathematical Society, Providence, RI, 2003.

[20] V. Kac, B. Weisfeiler, *Coadjoint action of a semi-simple algebraic group and the center of the enveloping algebra in characteristic p*, Andag. Math. **38** (1978) 136-151.

[21] S. Lang, *Algebra*, (Revised third ed.), Graduate Texts in Mathematics, **211**, New York: Springer-Verlag, 2002.

[22] G. Lusztig, *Introduction to quantum groups*. Reprint of the 1994 edition.

[23] I. Mirkovic, D. Rumynin, *Centers of reduced enveloping algebras*. Mathematische Zeitschrift 231.1 (1999): 123-132.

[24] J-P. Serre, *Lie algebras and Lie groups*, 1964 lectures given at Harvard University, Lecture notes in mathematics, **1500**, Springer-Verlag, 1992.

[25] T. A. Springer, *Linear algebraic groups*. Second edition, Progress in Mathematics, **9**. Birkhuser Boston, Inc., Boston, MA, 1998.

[26] R. Steinberg, *Represntations of Algebraic Groups*, Nagoya Math. J. **22** (1963) 33-56.

[27] J. B. Sullivan, *Representations of the hyperalgebra of an algebraic group*, Amer. J. Math. **100** (1978).

[28] M. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.

[29] M. Takeuchi, *Tangent coalgebras and hyperalgebras I*, Japan. J. Math. **42** (1974), 1-143.

[30] V. S. Varadarajan, *Lie groups, Lie algebras, and their representations*, Graduate Texts in Mathematics, **102**. Springer-Verlag, New York, 1984.

[31] D.-N. Verma, *Structure of certain induced representations of complex semi-simple Lie algebras*, Yale Univ., dissertation, 1966; cf Bull Amer. Math. Soc. **74**, 160-166(1968).

[32] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, **66**. Springer-Verlag, New York-Berlin, 1979.

[33] H. Yanagihara, *Theory of Hopf Algebras Attached to Group Schemes*, Lecture Notes in Math. **614**, Berlin etc. 1977.

Index

algebraic group, 9

augmentation, 19

distribution, 17

final object, 6

Frobenius center, 44

Frobenius kernel, 31

Frobenius morphism, 31

function associated to differential operators, 53

general linear group, 11

generalized weights, 33

group functor, 12

group in a category, 7

group scheme, 9

Harish-Chandra center, 44

hyperalgebra, 17

integral, 51

invariant differential operators, 17

invariant operator, 27

involution, 19

left integral, 51

measure, 27

nilpotent, 38

product, 6

rational representation, 13

right integral, 51

semisimple, 38

semisimple center, 42

Steinberg Tensor Product Theorem, 52

Steinberg weight, 53